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
# Contents

1 VMware vRealize Operations for Published Applications Installation and Administration 5

2 Introducing vRealize Operations for Published Applications 7
   vRealize Operations for Published Applications Architecture 8
   vRealize Operations for Published Applications Desktop Agent 8
   vRealize Operations for Published Applications Broker Agent 9
   vRealize Operations for Published Applications Adapter 9

3 System Requirements for vRealize Operations for Published Applications 11
   Product Compatibility for vRealize Operations for Published Applications 11
   Software Requirements for vRealize Operations for Published Applications 11

4 Installing and Configuring vRealize Operations for Published Applications 13
   Install and Configure vRealize Operations for Published Applications 13

5 Monitoring Your Citrix XenApp Environment 25
   Using the Citrix XenApp Dashboards 25
   Using the XA Reports 29

6 Managing RMI Communication in
   vRealize Operations for Published Applications 33
   RMI Services 33
   Default Ports for RMI Services 34
   Changing the Default RMI Service Ports 34

7 Changing the Default SSL/TLS Configuration in
   vRealize Operations for Published Applications 37
   Default SSL Protocols and Ciphers for vRealize Operations for Published Applications 37
   SSL/TLS Configuration Properties 38
   Change the Default SSL/TLS Configuration for Servers 38
   Change the Default SSL/TLS for Agents 39

8 Managing Authentication in vRealize Operations for Published Applications 41
   Understanding Authentication for Each Component 41

9 Certificate and Trust Store Files 43
   vRealize Operations for Published Applications Adapter Certificate and Trust Store Files 43
   Broker Agent Certificate and Trust Store Files 44
10 Replacing the Default Certificates 45
   Replace the Default Certificate for the vRealize Operations for Published Applications Adapter 45
   Replace the Default Certificate for the Broker Agent 47

11 Certificate Pairing 49

12 SSL/TLS and Authentication-Related Log Messages 51

13 Create a vRealize Operations Manager Support Bundle 53

14 Download vRealize Operations for Published Applications Broker Agent Log Files 55

15 Download vRealize Operations for Published Applications Desktop Agent Log Files 57

16 View Collector and vRealize Operations for Published Applications Adapter Log Files 59

17 Modify the Logging Level for vRealize Operations for Published Applications Adapter Log Files 61

Index 63
VMware vRealize Operations for Published Applications Installation and Administration

VMware vRealize Operations for Published Applications Installation and Administration provides information about how to monitor the performance of your Citrix XenApp environment in VMware vRealize™ Operations Manager™.

Intended Audience

This information is intended for users who monitor the performance of a Citrix XenApp environment in VMware vRealize Operations Manager and administrators who are responsible for maintaining and troubleshooting a Citrix XenApp environment.
Introducing vRealize Operations for Published Applications

vRealize Operations for Published Applications collects performance data from monitored software and hardware objects in your Citrix XenApp environment and provides predictive analysis and real-time information about problems in your Published Applications infrastructure.

vRealize Operations for Published Applications presents data through alerts, on configurable dashboards, and on predefined pages in vRealize Operations Manager.

IT administrators can use vRealize Operations for Published Applications to quickly obtain an overview of how the Citrix XenApp environment is behaving and view important metrics associated with that environment. Help desk specialists can view objects related to end user sessions, perform basic troubleshooting, and resolve user problems.

This chapter includes the following topics:

- “vRealize Operations for Published Applications Architecture,” on page 8
- “vRealize Operations for Published Applications Desktop Agent,” on page 8
- “vRealize Operations for Published Applications Broker Agent,” on page 9
- “vRealize Operations for Published Applications Adapter,” on page 9
vRealize Operations for Published Applications Architecture

The vRealize Operations for Published Applications components include the Published Applications adapter, broker agent, and desktop agents.

vRealize Operations for Published Applications Desktop Agent

The vRealize Operations for Published Applications desktop agent runs as service on the XA Controller server and on each XA Session host server.

The desktop agent monitors Citrix ICA sessions and applications launched in the Citrix ICA sessions by using standard functions and APIs of Windows OS. The desktop agent periodically collects the Citrix ICA sessions’ data on properties and performance, and sends the data to the adapter using a secure connection.

The desktop agent service is configured to restart automatically by default. You can change the default configuration by accessing services.msc, right-click Desktop Agent Service, and select Properties > Recovery.
vRealize Operations for Published Applications Broker Agent

The vRealize Operations for Published Applications broker agent runs on a vRealize Operations for Published Applications Controller server or on a dedicated machine, collects information from the XA Controller server, the XA Licensing server, and the XA Web Interface server, and sends that information to the Published Applications adapter.

When you configure a broker agent, you pair the broker agent with a Published Applications adapter instance.

vRealize Operations for Published Applications Adapter

The vRealize Operations for Published Applications adapter collects XenApp inventory information from the broker agent and collects metrics and performance data from desktop agents. The vRealize Operations for Published Applications adapter sends that information to vRealize Operations Manager. The information is displayed in preconfigured XenApp dashboards in the vRealize Operations Manager user interface.

The vRealize Operations for Published Applications adapter runs on a cluster node or remote collector node in vRealize Operations Manager. You can create a single vRealize Operations for Published Applications adapter instance to monitor multiple XenApp farms. During broker agent configuration, you pair the broker agent with a vRealize Operations for Published Applications adapter instance.

If you are monitoring multiple XenApp farms, you can pair the broker agent installed in each farm with the same vRealize Operations for Published Applications adapter instance as long as the total number of objects that the vRealize Operations for Published Applications adapter instance handles does not exceed 10,000. You can create more vRealize Operations for Published Applications adapter instances on different remote nodes to support large scale environments.

IMPORTANT Creating more than one vRealize Operations for Published Applications adapter instance for each cluster node or remote collector is not supported. Also, creating more than one vRealize Operations for Published Applications adapter instance for each farm is not supported.

If your vRealize Operations for Published Applications environment resembles one of the following configurations, VMware recommends that you create the vRealize Operations for Published Applications adapter instance on a remote collector node.

- **XenApp deployments with multiple farms**
  To improve scalability, create the vRealize Operations for Published Applications adapter instance on a remote collector node to offload processing from the vRealize Operations Manager cluster data nodes.

- **Remote datacenters**
  To minimize network traffic across WAN or other slow connections, install a remote collector node with a separate vRealize Operations for Published Applications adapter instance in remote datacenters. Pair each vRealize Operations for Published Applications adapter instance with the broker agent that is located in the same remote datacenter.
System Requirements for vRealize Operations for Published Applications

vRealize Operations for Published Applications has specific system requirements. Verify that your environment meets these system requirements before you install vRealize Operations for Published Applications.

This chapter includes the following topics:
- “Product Compatibility for vRealize Operations for Published Applications,” on page 11
- “Software Requirements for vRealize Operations for Published Applications,” on page 11

Product Compatibility for vRealize Operations for Published Applications

vRealize Operations for Published Applications is compatible with the following products.
- vCenter Server 5.5 and 6.0
- vRealize Operations Manager 6.0.2
- Citrix XenApp 6.5

Software Requirements for vRealize Operations for Published Applications

Each component of vRealize Operations for Published Applications has requirements for the software on the system where it is installed.

vRealize Operations for Published Applications Desktop Agent Software Requirements

You install the vRealize Operations for Published Applications desktop agent on all Citrix Delivery Controllers and Session Host servers.

vRealize Operations for Published Applications Broker Agent Software Requirements

You install the vRealize Operations for Published Applications broker agent on the Citrix Delivery Controller. Alternatively, you can install the vRealize Operations for Published Applications broker agent on a separate Windows machine.

The vRealize Operations for Published Applications broker agent has the following software requirements.
- Windows 7, Windows 2008R2, Windows 8, Windows 8.1
■ Microsoft .Net Framework 3.5

vRealize Operations for Published Applications Adapter Software Requirements

You install the vRealize Operations for Published Applications adapter on a vRealize Operations Manager server that is running.

The vRealize Operations for Published Applications adapter has the following software requirements.

■ VMware vRealize Operations Manager 6.0.2
Installing and Configuring vRealize Operations for Published Applications

Installing vRealize Operations for Published Applications involves downloading the installation files from the VMware product download page and installing and configuring software components on machines in your vRealize Operations for Published Applications environment.

Install and Configure vRealize Operations for Published Applications

You install and configure vRealize Operations for Published Applications software components on machines in your Published Applications and vRealize Operations Manager environments.

Prerequisites

- Verify that your environment meets product compatibility, hardware, and software requirements. See Chapter 3, “System Requirements for vRealize Operations for Published Applications,” on page 11.
- Verify that vRealize Operations Manager is deployed and running. If you need to upgrade vRealize Operations Manager, perform the upgrade before you install vRealize Operations for Published Applications.
- Download the vRealize Operations for Published Applications installation files from the product download page. See “Downloading the vRealize Operations for Published Applications Installation Files,” on page 14.
- Verify that you have a license key for the vRealize Operations for Published Applications solution.
- Verify that you have a license key for vRealize Operations Manager.
- Registered VMware users can download the vRealize Operations for Published Applications installation files from the product download page.
- You install the vRealize Operations for Published Applications solution from a PAK file in vRealize Operations Manager.
- After you install the vRealize Operations for Published Applications adapter, you disable the firewall service and open the default ports.
- After you install the vRealize Operations for Published Applications solution, you must add a vRealize Operations for Published Applications license key in the vRealize Operations Manager user interface. vRealize Operations for Published Applications is not functional until it is licensed.
- **Associate Published Applications Objects with Your vRealize Operations for Published Applications License Key** on page 17
  You must associate Published Applications objects with your vRealize Operations for Published Applications license key by editing license groups in vRealize Operations Manager.

- **Create an Instance of the vRealize Operations for Published Applications Adapter** on page 18
  After you install the vRealize Operations for Published Applications solution, you must create an instance of the vRealize Operations for Published Applications adapter in vRealize Operations Manager.

- **Enabling Firewall Rules for XA Servers, Web Interface Servers, and License Servers.** on page 19
  Before you install the broker agent and desktop agent, you must enable specific firewall rules for the XA server, Web Interface server, and License server.

- **Install the vRealize Operations for Published Applications Broker Agent** on page 20
  You install the vRealize Operations for Published Applications broker agent on a Windows machine. Install a broker agent for each farm in your infrastructure.

- **Configure the vRealize Operations for Published Applications Broker Agent** on page 20
  After you install the broker agent, you use the Broker Agent Configuration wizard to configure the broker agent on the Windows machine where you installed the broker agent. You can also use the Broker Agent Configuration wizard to make changes to your broker agent configuration.

- **Install a vRealize Operations for Published Applications Desktop Agent** on page 22
  You install desktop agents on all Citrix Delivery Controllers and Session Host servers.

- **Push the vRealize Operations for Published Applications Desktop Agent Pair Token Using a Group Policy** on page 23
  To use vRealize Operations for Published Applications to monitor a XenApp Farm, you must create a Group Policy (GPO) to contain the vRealize Operations for Published Applications group policies. You then apply the GPO to the remote desktops that you want to monitor.

### Downloading the vRealize Operations for Published Applications Installation Files

Registered VMware users can download the vRealize Operations for Published Applications installation files from the product download page.

**Table 4-1. vRealize Operations for Published Applications Installation Files**

<table>
<thead>
<tr>
<th>File Name</th>
<th>Component</th>
<th>Where to Install</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware-vrops-v4paadapter-6.1.0-buildnumber.pak</td>
<td>Adapter</td>
<td>vRealize Operations Manager server</td>
</tr>
<tr>
<td>VMware-v4pbrokeragent-6.1.0-buildnumber.exe</td>
<td>Broker agent installer for 32-bit Windows OS</td>
<td>On XA Controller or on a separate 32-bit Windows machine</td>
</tr>
<tr>
<td>VMware-v4pbrokeragent-x86_64-6.1.0-buildnumber.exe</td>
<td>Broker agent installer for 64-bit Windows OS</td>
<td>On XA Controller or on a separate Windows machine</td>
</tr>
<tr>
<td>VMware-v4pdesktopagent-x86_64-6.1.0-buildnumber.exe</td>
<td>Desktop agent installer for 64-bit Windows OS</td>
<td>On XA Controllers and Session Host servers</td>
</tr>
</tbody>
</table>
Install the vRealize Operations for Published Applications Solution

You install the vRealize Operations for Published Applications solution from a PAK file in vRealize Operations Manager.

Procedure
1. Copy the VMware-vrops-v4paadapter-6.1.0-buildnumber.pak file to a temporary folder.
2. Log in to the vRealize Operations Manager user interface with administrator privileges.
3. In the left pane of vRealize Operations Manager, click the Administration tab and click Solutions.
4. On the Solutions tab, click the plus sign.
   - a. Browse to locate the temporary folder and select the PAK file.
   - b. Click Upload.
      - The upload might take several minutes.
   - c. Read and accept the EULA and click Next.
      - Installation details appear in the window during the upload process.
   - d. When the installation is complete, click Finish.

After the installation is finished, vRealize Operations for Published Applications is listed as a solution.

What to do next
Provide licensing information for the vRealize Operations for Published Applications solution. See “Adding a vRealize Operations for Published Applications License Key,” on page 16.

Open the Ports Used by vRealize Operations for Published Applications

After you install the vRealize Operations for Published Applications adapter, you disable the firewall service and open the default ports.

Prerequisites
- Install the vRealize Operations for Published Applications adapter.
- Verify that you have root privileges.

Procedure
1. Log in to vRealize Operations Manager collector server.
2. Access the command prompt and run the service vmware-vcops-firewall stop to disable the vRealize Operations Manager firewall service.
3  Open the default ports by editing the configuration file.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
</table>
| Linux  | a  Access the `vmware-vcops-firewall.conf` file in the `/opt/vmware/etc/vmware-vcops-firewall.conf` directory.  
|        | b  In a text editor, modify the properties for the RMI service ports that you want to change, for example `TCPPORTS="$TCPPORTS 3095:3098"`. |
|        | b  Select [Specific local ports](https://docs.microsoft.com/en-us/windows/security/basics/windows-firewall) and type the ports that you are using, for example `3095-3098`.  
|        | The default ports are 3095-3098. If you changed the default ports, specify the ports that you are using. |

4  Run the `vmware-vcops-firewall start` command to start the service.

   If the service `vmware-vcops-firewall start` command does not enable the ports, start the collector server.

**What to do next**

Add a vRealize Operations for Published Applications license key. See “Adding a vRealize Operations for Published Applications License Key,” on page 16

**Adding a vRealize Operations for Published Applications License Key**

After you install the vRealize Operations for Published Applications solution, you must add a vRealize Operations for Published Applications license key in the vRealize Operations Manager user interface. vRealize Operations for Published Applications is not functional until it is licensed.

**NOTE**  You must also add a license key for vRealize Operations Manager.

You can have an evaluation license key or a product license key for vRealize Operations for Published Applications. The evaluation license key (**eval**) provides 60 days of unlimited product use. A product license key is encoded with an expiration date and a license count.

To add your vRealize Operations for Published Applications license key, select **Administration > Licensing** in the vRealize Operations Manager user interface and add your license key to **VMware Published Apps Solution** on the **License Keys** tab.

For detailed information about adding license keys, see the *vRealize Operations Manager Customization and Administration Guide*.

If your vRealize Operations for Published Applications license key expires, the vRealize Operations for Published Applications adapter stops populating vRealize Operations Manager with data. If you have a valid license key but you exceed the license count, vRealize Operations Manager generates alerts and a watermark appears on certain dashboards. The vRealize Operations for Published Applications adapter does not restrict data when the license count is exceeded.
Associate Published Applications Objects with Your vRealize Operations for Published Applications License Key

You must associate Published Applications objects with your vRealize Operations for Published Applications license key by editing license groups in vRealize Operations Manager.

A license group is a way to gather certain objects, called license group members, under a particular license key. By default, the vRealize Operations Manager and vRealize Operations for Published Applications license groups both include all host, virtual machine, and datastore objects. Because these objects are members of both license groups, they are covered by both your vRealize Operations Manager license and your vRealize Operations for Published Applications license.

Each license group includes membership criteria that you can use to filter the objects that are members of the license group. By editing the membership criteria for the vRealize Operations Manager and vRealize Operations for Published Applications license groups, you can specify that certain objects are covered only under your vRealize Operations for Published Applications license key.

Prerequisites

Add your vRealize Operations for Published Applications license key. See “Adding a vRealize Operations for Published Applications License Key,” on page 16.

Procedure

1. Log in to the vRealize Operations Manager user interface.
2. In the left pane, select Administration > Licensing.
3. Click the License Groups tab.
   License groups appear in the top pane. The license group for vRealize Operations for Published Applications is called VMware Published Applications Licensing. The license group for vRealize Operations Manager is called Product Licensing.
4. Edit the membership criteria for the VMware Published Application Licensing group.
   a. Select VMware Published Applications Licensing and click Edit on the toolbar.
   b. Select the vRealize Operations for Published Applications license key under VMware vRealize Operations for Published Applications and click Next.
   c. In the first Select the Object Type that matches all of the following criteria drop-down menu, select Host System, define the criteria Relationship, Descendant of, is, and type All Hosts in the Object name text box.
   d. In the second Select the Object Type that matches all of the following criteria drop-down menu, select Virtual Machine, define the criteria Relationship, Descendant of, is, and type All Desktop VMs in the Object name text box.
   e. In the third Select the Object Type that matches all of the following criteria drop-down menu, select Datastore, define the criteria Relationship, Descendant of, is, and type All Storage in the Object name text box.
   f. Click Next and then click Finish to save your configuration.
5 Edit the membership criteria for the **Product Licensing** group.

You must edit the membership criteria for the **Product Licensing** group to exclude the objects that you included in the **VMware Published Application Licensing** group.

a Select **Product Licensing** and click **Edit** on the toolbar.

b Select the vRealize Operations Manager license key under **vRealize Operations Manager** and click **Next**.

c In the first **Select the Object Type that matches all of the following criteria** drop-down menu, select **Host System**, define the criteria **Relationship, Descendant of, is not**, and type **All Hosts** in the **Object name** text box.

d In the second **Select the Object Type that matches all of the following criteria** drop-down menu, select **Virtual Machine**, define the criteria **Relationship, Descendant of, is not**, and type **All Desktop VMs** in the **Object name** text box.

e In the third **Select the Object Type that matches all of the following criteria** drop-down menu, select **Datastore**, define the criteria **Relationship, Descendant of, is not**, and type **All Storage** in the **Object name** text box.

f Click **Next** and then click **Finish** to save your configuration.

### Create an Instance of the vRealize Operations for Published Applications Adapter

After you install the vRealize Operations for Published Applications solution, you must create an instance of the vRealize Operations for Published Applications adapter in vRealize Operations Manager.

You can create a single vRealize Operations for Published Applications adapter instance to monitor multiple XenApp Farms. If you need to create multiple vRealize Operations for Published Applications adapter instances, you must create each adapter instance on a unique cluster node or remote collector.

When you restart a vRealize Operations for Published Applications adapter instance, it takes several minutes before the vRealize Operations for Published Applications desktop agent and broker agent send information to the vRealize Operations for Published Applications adapter.

### Prerequisites

Install the vRealize Operations for Published Applications solution and add your license key.

### Procedure

1 Log in to the vRealize Operations Manager user interface with **administrator** privileges.

2 Click the **Administration** tab and click **Solutions**.

3 Select **VMware Published Application** and click the **Configure** button on the toolbar.

4 Select **Published Apps Adapter** in the Adapter Type pane.

5 Click the **Add** (plus sign) icon on the lower pane toolbar to add an adapter instance.

6 In **Adapter Settings**, type a name and description for the adapter instance.
7 In **Basic Settings**, configure an adapter ID and credential for the adapter instance.

   a Type an identifier for the adapter instance in the **Adapter ID** text box.

   The identifier must be unique across all vRealize Operations for Published Applications adapter instances in the cluster.

   b Configure the credential to use when the broker agent pairs with the vRealize Operations for Published Applications adapter instance.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use an existing credential</td>
<td>Select the credential from the <strong>Credential</strong> drop-down menu. When you create a vRealize Operations for Published Applications adapter instance for the first time, the <strong>Credential</strong> drop-down menu is empty.</td>
</tr>
<tr>
<td>Add a new credential</td>
<td>1 Click the <strong>Add New</strong> (plus sign) icon.</td>
</tr>
<tr>
<td></td>
<td>2 Type a name for the credential in the <strong>Credential name</strong> text box.</td>
</tr>
<tr>
<td></td>
<td>3 Type a server key for the adapter instance in the <strong>Server Key</strong> text box. The server key is required to enable pairing between the broker agent and the adapter. You must provide the server key when you configure the broker agent.</td>
</tr>
<tr>
<td></td>
<td>4 Click <strong>OK</strong> to save the new credential.</td>
</tr>
<tr>
<td></td>
<td>5 Select the new credential from the <strong>Credential</strong> drop-down menu.</td>
</tr>
</tbody>
</table>

c Click **Test Connection** to test the connection with the credential that you selected.

8 In **Advanced Settings**, select a collector to manage the adapter processes from the **Collector** drop-down menu.

   To run the adapter instance on a remote collector, select the remote collector. If you do not have a remote collector, select **Automatically select collector**.

9 Click **Save Settings** to save the adapter instance.

   The adapter instance is added to the list.

**What to do next**

Install the vRealize Operations for Published Applications broker agent. See “Install the vRealize Operations for Published Applications Broker Agent,” on page 20.

**Enabling Firewall Rules for XA Servers, Web Interface Servers, and License Servers.**

Before you install the broker agent and desktop agent, you must enable specific firewall rules for the XA server, Web Interface server, and License server.

The broker agent cannot communicate with the XA server, Web Interface server, or License server if the firewall is enabled on these servers.

Enable the following rules in XA Delivery Controller Servers, XA Session Host Servers, License Server, and Web Interface.

- Enable **Ping** in the firewall for all servers using the File and Printer Sharing (Echo Request - ICMPv4-In) rule.

- Enable **Remote WMI** in the firewall for all servers using the Windows Management Instrumentation (WMI-In) rule.

Enable the following rule in XA Delivery Controller Servers and XA Session Host Servers.

- Enable **Remote Powershell** by running the `Enable-PSRemoting` command in PowerShell command prompt.
Install the vRealize Operations for Published Applications Broker Agent

You install the vRealize Operations for Published Applications broker agent on a Windows machine. Install a broker agent for each farm in your infrastructure.

You only install one broker agent for each XenApp Farm.

Prerequisites

■ Install the vRealize Operations for Published Applications solution, add your license key, and create an instance of the vRealize Operations for Published Applications adapter.

■ Verify that you downloaded the broker agent installation file.

■ Verify that you configured the XenApp Controller, Web Interface server, and License server for remote WMI by granting DCOM remote access/activation permissions to the servers. The user name must include the user name that you indicated for the servers.

Procedure

1. Log in to the machine where you plan to install the broker agent using a domain account that is part of the local administrators group.

2. Install the broker agent.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>a. Access the command prompt.</td>
</tr>
<tr>
<td></td>
<td>b. Install the broker agent for your environment using the /s, v, or /qn options.</td>
</tr>
</tbody>
</table>
|             |   ■ For 32-bit systems run the VMware-v4pabrokeragent-6.1.0-
|             |       buildnumber.exe command.                                           |
|             |   ■ For 64-bit systems run the VMware-v4pabrokeragent-                  |
|             |       x86_64-6.1.0-buildnumber.exe command.                              |

| EXE file    | a. Copy the file for your environment to a temporary folder, and double-click the EXE file to start the installation procedure. |
|            |   ■ For 32-bit systems double-click the VMware-v4pabrokeragent-       |
|            |     6.1.0-buildnumber.exe file.                                       |
|            |   ■ For 64-bit systems double-click the VMware-v4pabrokeragent-       |
|            |     x86_64-6.1.0-buildnumber.exe file.                                 |
|             | b. Follow the steps in the installer.                                  |

The broker agent is installed and saved to the Program Files folder.

What to do next

Configure the broker agent. See “Configure the vRealize Operations for Published Applications Broker Agent,” on page 20.

Configure the vRealize Operations for Published Applications Broker Agent

After you install the broker agent, you use the Broker Agent Configuration wizard to configure the broker agent on the Windows machine where you installed the broker agent. You can also use the Broker Agent Configuration wizard to make changes to your broker agent configuration.

A check box in the Broker Agent Setup wizard controls whether the Broker Agent Configuration wizard opens immediately after you install the broker agent. This check box is selected by default.
During broker agent configuration, you pair the broker agent with a vRealize Operations for Published Applications adapter instance. Pairing the broker agent with a vRealize Operations for Published Applications adapter instance is a necessary authentication step that enables the broker agent and desktop agents to communicate with the vRealize Operations for Published Applications adapter. The broker agent and desktop agents cannot communicate with the vRealize Operations for Published Applications adapter until the pairing process is complete.

If you are monitoring multiple XenApp Farms, you can pair the broker agent installed in each Farm with the same vRealize Operations for Published Applications adapter instance as long as the total number of desktops that the vRealize Operations for Published Applications adapter instance handles does not exceed 10,000.

Each time you restart the broker agent service, a new log file is created. If a log file was created for the day and the broker agent is restarted on that day, a new log file is created. The name of the new log file is v4pa_brokeragent_svc_<date>_00.log, and the log rotation follows this series.

Prerequisites

- Install the vRealize Operations for Published Applications broker agent. See “Install the vRealize Operations for Published Applications Broker Agent,” on page 20.
- Verify that you have the server key for the vRealize Operations for Published Applications adapter. You specified the server key when you created a credential for the adapter instance.
- Verify that you have the IP address or hostname of the machine where you installed the vRealize Operations for Published Applications adapter.
- If the broker agent is installed on a Windows system outside of the XenApp server environment, verify that you configured remote PowerShell execution for the vRealize Operations for Published Applications broker agent.

Procedure

1. If the Broker Agent Configuration wizard is not already open, start it by selecting Start > VMware > vRealize Operations for Published Applications Broker Agent Settings.

2. In the Address text box, type the IP address of the vRealize Operations Manager node or remote collector where the vRealize Operations for Published Applications adapter instance is running.

3. In the Port text box, type the port used to connect to the vRealize Operations for Published Applications adapter. By default, the broker agent uses port 3095 to communicate with the vRealize Operations for Published Applications adapter. You can modify the default port number, depending on your network configuration.

4. Type and confirm the server key for the vRealize Operations for Published Applications adapter.

5. Click Pair to pair the broker agent with the vRealize Operations for Published Applications adapter, and click Test to test the connection. The status of the pairing process appears in the Text area.

6. After the pairing process succeeds, click Next.

7. On the Copy Information page, click Copy to copy the certificate string to the clipboard and click Next. Save this text to copy to the GPO Template.
8 Provide the requested information on the Citrix XenApp Controller Information window.

If you installed the broker agent on the XenApp Controller, the XenApp Controller Server Hostname text box is populated with localhost and you can skip to the next step.

a Type the XenApp Controller Server hostname, domain name, and credentials.

b Click Test to validate the connection to the XenApp Controller server.

c Click Next.

9 Provide the Web Interface Server details, and click Ping to verify that the Web Interface Server can be reached through ping.

10 (Optional) Edit the interval values on the Intervals and Timeouts page, and click Next.

11 (Optional) Configure the logging level and log rotation on the Configure the logging parameters page, and click Next.

12 (Optional) When the Service Configuration window appears, select Start/Rerstart, and then click Next.

13 Review the configurations and click Finish to apply the configurations.

The vRealize Operations for Published Applications broker agent is configured and available.

What to do next

Verify the status of the vRealize Operations for Published Applications broker agent in the Windows Services Management Console.

Review the logs by browsing to the C:\ProgramData\VMware\VMware vRealize Operations for Published Apps\Broker Agent\logs directory.

Install a vRealize Operations for Published Applications Desktop Agent

You install desktop agents on all Citrix Delivery Controllers and Session Host servers.

Prerequisites

 Verify that you downloaded the desktop agent installation file.

Procedure

1 Log in to the machine where you plan to install the desktop agent, using a domain account that is part of the local administrators group.

2 Install the desktop agent.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>a Access the command prompt.</td>
</tr>
<tr>
<td></td>
<td>b Run the VMware-v4padesktopagent-x86_64-6.1.0-buildnumber.exe command using the /s, v, or /qn options.</td>
</tr>
<tr>
<td>EXE file</td>
<td>a Copy the VMware-v4padesktopagent-x86_64-6.1.0-buildnumber.exe file to a temporary folder.</td>
</tr>
<tr>
<td></td>
<td>b Double-click the VMware-v4padesktopagent-x86_64-6.1.0-buildnumber.exe file.</td>
</tr>
<tr>
<td></td>
<td>c Follow the prompts to complete the installation, and when the installation is complete, click Finish.</td>
</tr>
</tbody>
</table>

The desktop agent is installed in Program Files folder.
Push the vRealize Operations for Published Applications Desktop Agent Pair Token Using a Group Policy

To use vRealize Operations for Published Applications to monitor a XenApp Farm, you must create a Group Policy (GPO) to contain the vRealize Operations for Published Applications group policies. You then apply the GPO to the remote desktops that you want to monitor.

You use the Microsoft Group Policy Editor to create the GPO. After you create the GPO, you must apply it to a base image or to an Organizational Unit (OU) on your Active Directory server, depending on your configuration.

vRealize Operations for Published Applications group-policy settings are provided in the v4pa_desktopagent.admx file that is installed in the %programfiles%\VMware\vRealize Operations for Published Apps\Broker Agent\extras\GroupPolicyFiles directory.

The language-specific resources, for example .adml files, are installed in the %programfiles%\VMware\vRealize Operations for Published Apps\Broker Agent\extras\GroupPolicyFiles\language directory.

If there is an Authentication Failure for a desktop agent you must update the GPO policy for desktop agent authentication. When you update the GPO policy for desktop agent authentication, and there are other policies that require updating, all pending policies are updated, not just the GPO policy for desktop agent authentication.

Procedure

1. Create an organizational unit (OU) in the domain controller machine.
2. If the XA server was already added to the computer account, move the XA server to the OU.
   a. Access Active Directory Users Computers, and select Computer, right-click your XA server, and in the context menu select Move....
   b. In the Move object into container window, select the OU you created.
      The XA server is now moved to the OU.
3. Create a Group Policy object using the Group Policy Management Console (GPMC).
4. Copy the certificate string and the RMI URL from the broker agent configuration utility.
5. Copy the v4pa_desktopagent.admx file to PolicyDefinitions folder, which is in the c:\Windows\PolicyDefinitions directory.
   The v4pa_desktopagent.admx file is in the "%ProgramFiles%\VMware\V4PA Broker Agent\Server\extras\GroupPolicyFiles directory.
6. Copy the v4pa_desktopagent.adml file to en-us folder, which is in the c:\Windows\PolicyDefinitions\en-us directory.
   The v4pa_desktopagent.adml file is in the "%ProgramFiles%\VMware\V4PA Broker Agent\Server\extras\GroupPolicyFiles\en_us directory.
7. Set the Group Policy.
   a. On the controller machine, click Start and type the gpmc.msc command in the search box.
   b. Right-click the GPO that you created and select Edit.
   c. Select Computer Configuration > Policies > Administrative Templates > VMware Published Apps Agent Configuration > vRealize Operations, and double-click the item in the right pane.
d  Select **Enable** and copy the RMI URL and certificate string in the policy template.
   
   You might receive a warning that you exceeded the maximum number of characters per line.

  e  (Optional) Break the line by pressing **Enter**, and click **Apply**, and then click **OK**.

8  Verify on the XA server machine that the RMI URL and certificate string in the
    HKLM\Software\Policies\VMware, Inc.\vRealize operations for published Apps\Desktop Agent
directory.

**What to do next**

Install desktop agent on the XA server. If you already installed a desktop agent and planned to push
through GPO at later stage, there might be exceptions in the desktop agent log files. After the pair token is
pushed using the GPO, you should restart the desktop agent service.
When you install the vRealize Operations for Published Applications solution, preconfigured dashboards and predefined report templates appear in the vRealize Operations Manager user interface. You can use these Citrix XenApp-specific dashboards and reports along with the standard vRealize Operations Manager object monitoring features to monitor your Citrix XenApp environment.

This chapter includes the following topics:

- “Using the Citrix XenApp Dashboards,” on page 25
- “Using the XA Reports,” on page 29

### Using the Citrix XenApp Dashboards

The Citrix XenApp dashboards are in the XA group in the Dashboard List menu in the vRealize Operations Manager user interface.

#### Widget Interaction in Citrix XenApp Dashboards

vRealize Operations Manager supports interaction between widgets in a single dashboard. Widgets are combined so that the content of the destination widget is updated according to the value selected in the source widget.

For information about creating and modifying dashboards and customizing widgets see vRealize Operations Manager Customization and Administration Guide.

<table>
<thead>
<tr>
<th>Dashboard</th>
<th>Source Widget</th>
<th>Destination Widget</th>
</tr>
</thead>
<tbody>
<tr>
<td>XA Overview</td>
<td>Farms</td>
<td>Farm Indicator Metrics</td>
</tr>
<tr>
<td>XA Overview</td>
<td>Adapter Health</td>
<td>Adapter Health Metrics</td>
</tr>
<tr>
<td>XA Infrastructure</td>
<td>Web Interface Servers</td>
<td>Web Interface Server Indicator Metrics</td>
</tr>
<tr>
<td>XA Infrastructure</td>
<td>Licensing Servers</td>
<td>License Usage</td>
</tr>
<tr>
<td>XA Servers</td>
<td>Session-host Servers</td>
<td>Virtual Machine of Session-host Server</td>
</tr>
<tr>
<td>XA Servers</td>
<td>Session-host Servers</td>
<td>Session-host Server Resource Utilization</td>
</tr>
<tr>
<td>XA Servers</td>
<td>Session-host Servers</td>
<td>Session-host Server Indicator Metrics</td>
</tr>
<tr>
<td>XA Servers</td>
<td>Controller Servers</td>
<td>Virtual Machine of Controller Server</td>
</tr>
<tr>
<td>XA Servers</td>
<td>Controller Servers</td>
<td>Controller Server Indicator Metrics</td>
</tr>
<tr>
<td>XA Servers</td>
<td>Controller Servers</td>
<td>Controller Server Resource Utilization</td>
</tr>
<tr>
<td>XA Session Detail</td>
<td>Sessions</td>
<td>Application Session Indicator Metrics</td>
</tr>
</tbody>
</table>
### Table 5.1. Widget Interaction in Citrix XenApp Dashboards (Continued)

<table>
<thead>
<tr>
<th>Dashboard</th>
<th>Source Widget</th>
<th>Destination Widget</th>
</tr>
</thead>
<tbody>
<tr>
<td>XA Session Detail</td>
<td>Sessions</td>
<td>Session Resource Utilization</td>
</tr>
<tr>
<td>XA Session Detail</td>
<td>Session-host Servers</td>
<td>Server Session Statistics</td>
</tr>
<tr>
<td>XA Session Detail</td>
<td>Session-host Servers</td>
<td>Server Session Trend</td>
</tr>
<tr>
<td>XA Servers Detail</td>
<td>Farms</td>
<td>Farm Session Statistics</td>
</tr>
<tr>
<td>XA Servers Detail</td>
<td>Farms</td>
<td>Farm Session Trend</td>
</tr>
<tr>
<td>XA Applications</td>
<td>Session-host Servers</td>
<td>Server Indicator Metrics</td>
</tr>
<tr>
<td>XA Applications</td>
<td>Session-host Servers</td>
<td>Application Instances</td>
</tr>
<tr>
<td>XA Applications</td>
<td>Application Instances</td>
<td>Application Instances Indicator</td>
</tr>
<tr>
<td>XA Application Usage</td>
<td>Farms</td>
<td>Application Instance</td>
</tr>
<tr>
<td>XA Application Usage</td>
<td>Application Instances</td>
<td>Application Instance Metrics</td>
</tr>
<tr>
<td>XA Application Usage</td>
<td>Applications</td>
<td>Application Launch Time</td>
</tr>
<tr>
<td>XA Application Usage</td>
<td>Applications</td>
<td>Application Sessions</td>
</tr>
<tr>
<td>XA Application Usage</td>
<td>Applications</td>
<td>Application Indicator Metrics</td>
</tr>
<tr>
<td>XA Application Usage</td>
<td>Applications</td>
<td>Application User Statistics</td>
</tr>
</tbody>
</table>

### Introducing the Citrix XenApp Dashboards

You can use the preconfigured Citrix XenApp dashboards to monitor the performance of your Citrix XenApp environment.

#### Table 5.2. Citrix XenApp Dashboard Summary

<table>
<thead>
<tr>
<th>View Dashboard</th>
<th>What It Shows</th>
<th>When To Use It</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;XA Overview Dashboard,&quot; on page 27</td>
<td>Status of your end-to-end XA environment, including the XA-related alerts, key Farm metrics, Adapter health metrics.</td>
<td>• Assess overall XA performance, and the overall user experience.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View the top XA-related alerts.</td>
</tr>
<tr>
<td>&quot;XA Infrastructure Dashboard,&quot; on page 28</td>
<td>Web interface server metrics, license usage, and information about XA infrastructure servers.</td>
<td>• Assess workload and performance of the Web interface server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View detailed license usage information on specific licensing servers.</td>
</tr>
<tr>
<td>&quot;XA Servers Dashboard,&quot; on page 28</td>
<td>Session-host server metrics and related vSphere VMs, controller-server metrics and related vSphere VMs.</td>
<td>• Assess workload and performance of servers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View metrics for related vSphere VMs.</td>
</tr>
<tr>
<td>&quot;XA Session Detail Dashboard,&quot; on page 28</td>
<td>Session metrics, session related statistics across session-host servers, farm session metrics</td>
<td>• Troubleshoot session and server issues reported by users.</td>
</tr>
<tr>
<td>&quot;XA Applications Dashboard,&quot; on page 29</td>
<td>Applications published on each server and related session-host workload and performance, application instance metrics.</td>
<td>• Identify and troubleshoot application issues reported by users.</td>
</tr>
<tr>
<td>&quot;XA Application Usage Dashboard,&quot; on page 29</td>
<td>Application alerts, application launch time across farms, application sessions, application launch users.</td>
<td>• View the workload, historical usage, and average launch time of applications.</td>
</tr>
</tbody>
</table>
Understanding the Health Badge

The health badge indicates immediate issues that might require your attention. It helps you identify the current health of your system.

vRealize Operations Manager combines workload, anomalies, and faults to assess the overall health of your system and to determine the expected workload level in that environment. A low health score might indicate a potential issue.

The health badge is enabled on vRealize Operations for Published Applications objects.

<table>
<thead>
<tr>
<th>Table 5-3. Understanding the Health Badge</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Object</strong></td>
</tr>
<tr>
<td>XA Application Instance</td>
</tr>
<tr>
<td>XA Session-host Server</td>
</tr>
<tr>
<td>XA Controller Server</td>
</tr>
<tr>
<td>XA Farm</td>
</tr>
<tr>
<td>XA Application Session</td>
</tr>
<tr>
<td>XA Broker Collector</td>
</tr>
</tbody>
</table>

XA Overview Dashboard

The XA Overview dashboard shows the overall status of your Citrix XenApp environment. Use the XA Overview dashboard to visualize the end-to-end Citrix XenApp environment, farm session metrics, adapter metrics, and alerts.

The XenApp Top Alerts widget shows the alerts of the greatest significance for XenApp objects.

**Tips for Using the XA Overview Dashboard**

- Click an alert in the Top Alerts widget to open the alert details.
- To view the overall status of a Farm, view the values of the Farm Session Metrics and Farm Capacity Metrics widgets.
- To view the overall status of an Adapter, view the values of the Adapter Health and Adapter Health Metrics widgets.
**XA Infrastructure Dashboard**

The XA Infrastructure dashboard shows the overall status of XA infrastructure servers. Use the XA Infrastructure dashboard to visualize and assess the performance of Web Interface servers and license usage information for licensing servers.

When you select a server in the Web Interface Servers widget, the Web Interface Server Indicator Metrics widget shows data for the server you selected.

When you select a server in the Licensing Servers widget, the Licensing Usage widget shows data for the server you selected.

**Tips for Using the XA Infrastructure Dashboard**

- Use the Web Interface Server Indicator Metrics widget to view the percentage for processor time, privileged time, and user time for the CPU of the server you selected.
- Use the Licensing Servers widget to view specific license information and collection information for the server you selected.

**XA Servers Dashboard**

Use the XA Servers dashboard to assess the health and resource utilization of servers, and the metrics of related vSphere virtual machines.

**Tips for using the XA Servers Dashboard**

- Use the Virtual Machine of Session-host Server widget to view the badge health and badge workload for the VM of the session-host server.
- Use the Virtual Machine of Controller Server widget to view badge health and badge workload for the VM of the controller server.
- Use the Session-host Server Indicator Metrics widget to view the health, workload, number of application sessions, ICA session latency, ICA session input bandwidth, and ICA session output bandwidth for the session-host server.

**XA Session Detail Dashboard**

Use the XA Session Detail dashboard to view detailed information about Farm sessions, application sessions, and server sessions.

You can use the widgets in the XA Session Detail dashboard to troubleshoot session and server issues that users report, for example, an application is running slowly.

**Tips for Using the XA Session Detail Dashboard**

- Use the Application Session Indicator Metrics widget to view session health, reconnect duration, logon duration, profile load duration, session duration and session state.
- Use the Session Resource Utilization widget to view CPU processor time, disk reads per second, disk writes per second, bytes received per second, bytes sent per second, and used memory.
- Use the Server Session Trend widget to view the number of application sessions during a specific time range at a set time interval. You can customize the time range and the time interval.
- Use the Server Farm Trend widget to view the number of total sessions during a specific time range at a set time interval. You can customize the time range and the time interval.
If there is a Desktop Agent Data Fault alert for all Session-host servers, verify the following configurations.

- Verify that you configured the GPO policy correctly. See “Push the vRealize Operations for Published Applications Desktop Agent Pair Token Using a Group Policy,” on page 23
- Verify that you configured the broker agent successfully. See “Configure the vRealize Operations for Published Applications Broker Agent,” on page 20
- Verify that the desktops agents started successfully.

**XA Applications Dashboard**

Use the XA Applications dashboard to view the overall health and performance of XenApp applications.

**Tips for Using the XA Applications Dashboard**

- Select a server to view the server metrics in the Server Indicator Metrics widget.
- Select an application instance to view application instance metrics in the Application Instance Indicator Metrics widget.
- Use the Application Instance Metrics widget to view CPU processor time, disk reads per second, disk writer per second, IO read operations per second, IO write operations per second, IO other operations per second, memory pages faults per second, and used memory.

**XA Application Usage Dashboard**

Use the XA Application Usage dashboard to view the workload, historical use, and average launch time for applications.

The All Application Alert List widget shows the alerts of the greatest significance for applications. When you select an application in the All Application Alert List widget, the Applications Sessions, Application Indicator Metrics, and Application User Statistics widgets show data for the application that you selected.

**Tips for Using the XA Application Usage Dashboard**

- Click an alert in the All Application Alert List widget to open the alert details.
- Click the name of an application in the Application Launch Time widget to view the health, health alerts, risk, risk alerts, efficiency and efficiency alerts for the application.
- Click the green arrow icon in the Application User Statistics widget to export the application user data, for example user and application launch time, to a CSV file.

**Using the XA Reports**

VMware vRealize Operations Manager has several report templates that you can generate for detailed information about applications, farms, license usage, and servers. You can also create new report templates, edit existing report templates, and clone report templates.

To access the vRealize Operations for Published Applications report templates, select **Content > Report** in vRealize Operations Manager.
Introducing the XA Reports

The predefined report templates provide detailed information about your XenApp environment. You can generate the report as a PDF or CSV file.

Table 5.4. Summary of XA Reports

<table>
<thead>
<tr>
<th>Template Name</th>
<th>Report Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Published Apps Application Report</td>
<td>Includes information about your applications.</td>
</tr>
<tr>
<td>Published Apps Server Report</td>
<td>Includes overall information about your servers.</td>
</tr>
<tr>
<td>Published Apps Farm Overview Report</td>
<td>Includes summary information about your farms. The Published Apps Server Summary section displays the average number of sessions. The average might appear as a fraction, for example, 1.729 sessions. The number of current applications sessions for a server is calculated every five minutes and recorded in vRealize Operations Manager. The average number of sessions is the average of current applications sessions for this server over the last 30 day period. If the time period is less than 30 days, the average number session is the average of current applications sessions for this server recorded in vRealize Operations Manager at the time that you generate the report.</td>
</tr>
<tr>
<td>Published Apps License Trend Report</td>
<td>Includes information about the trend of Citrix XenApp license usage.</td>
</tr>
<tr>
<td>Published Apps License Usage Report</td>
<td>Includes information about all Citrix XenApp license usage on your licensing server.</td>
</tr>
</tbody>
</table>

Subjects for Reports

When you configure reports, vRealize Operations Manager generates the report subjects according to your configurations.

To ensure the best possible reports, use the following report subjects.

Table 5.5. Subjects for Reports

<table>
<thead>
<tr>
<th>Report</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>Published Apps Farm Overview Report</td>
<td>XA Farm</td>
</tr>
<tr>
<td>Published Apps Server Report</td>
<td>XA Session-host Server and XA Controller Server</td>
</tr>
<tr>
<td>Published Apps Application Report</td>
<td>XA Application, XA Farm</td>
</tr>
<tr>
<td>Published Apps License Usage Report</td>
<td>XA Licensing Server</td>
</tr>
<tr>
<td>Published Apps License Trend Report</td>
<td>XA License</td>
</tr>
</tbody>
</table>

Subjects for Report Views

When you configure the views for a report, vRealize Operations Manager generates the views according to your configurations.

To ensure the best possible report views, use the following view subjects.
<table>
<thead>
<tr>
<th>Report View</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>Published Apps Application Daily User Count Trend</td>
<td>XA Application</td>
</tr>
<tr>
<td>Published Apps Application Instance Count Trend</td>
<td>XA Application</td>
</tr>
<tr>
<td>Published Apps Application Resource Utilization</td>
<td>XA Application</td>
</tr>
<tr>
<td>Published Apps Application Summary</td>
<td>XA Application, XA Farm</td>
</tr>
<tr>
<td>Published Apps Farm App Instance Trend</td>
<td>XA Farm</td>
</tr>
<tr>
<td>Published Apps Farm Session Count Trend</td>
<td>XA Farm</td>
</tr>
<tr>
<td>Published Apps Farm Session Trend</td>
<td>XA Farm</td>
</tr>
<tr>
<td>Published Apps Farm Summary</td>
<td>XA Farm</td>
</tr>
<tr>
<td>Published Apps License Usage Summary</td>
<td>XA Licensing Server</td>
</tr>
<tr>
<td>Published Apps License Usage Trend</td>
<td>XA License</td>
</tr>
<tr>
<td>Published Apps Most Used Applications</td>
<td>XA Farm</td>
</tr>
<tr>
<td>Published Apps Most Utilized Servers</td>
<td>XA Farm</td>
</tr>
<tr>
<td>Published Apps Server CPU Trend</td>
<td>XA Session-host Server, XA Controller Server</td>
</tr>
<tr>
<td>Published Apps Server Disk Trend</td>
<td>XA Session-host Server, XA Controller Server</td>
</tr>
<tr>
<td>Published Apps Server ICA Bandwidth Trend</td>
<td>XA Session-host Server</td>
</tr>
<tr>
<td>Published Apps Server Memory Trend</td>
<td>XA Session-host Server, XA Controller Server</td>
</tr>
<tr>
<td>Published Apps Server Network Trend</td>
<td>XA Session-host Server, XA Controller Server</td>
</tr>
<tr>
<td>Published Apps Server Session Count Trend</td>
<td>XA Session-host Server</td>
</tr>
<tr>
<td>Published Apps Server Summary</td>
<td>XA Session-host Server, XA Controller Server, XA Farm</td>
</tr>
<tr>
<td>Published Apps Session ICA Bandwidth Trend</td>
<td>XA Application Session</td>
</tr>
<tr>
<td>Published Apps Session ICA Latency Trend</td>
<td>XA Application Session</td>
</tr>
<tr>
<td>Published Apps Session Statistics</td>
<td>XA Session-host Server, XA Farm</td>
</tr>
</tbody>
</table>
Managing RMI Communication in vRealize Operations for Published Applications

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

For detailed descriptions of the vRealize Operations for Published Applications components, see “vRealize Operations for Published Applications Architecture,” on page 8.

This chapter includes the following topics:
- “RMI Services,” on page 33
- “Default Ports for RMI Services,” on page 34
- “Changing the Default RMI Service Ports,” on page 34

**RMI Services**

The vRealize Operations for Published Applications adapter exposes various RMI service.

<table>
<thead>
<tr>
<th>Service Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RMI registry service</td>
<td>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.</td>
</tr>
<tr>
<td>Desktop message server</td>
<td>The desktop agents connect to the desktop message server and use it to send Published Applications performance data collected by the desktop agent. The desktop message server uses an SSL/TLS channel to encrypt the data that is sent from the desktop agents.</td>
</tr>
<tr>
<td>Broker message server</td>
<td>The broker agent connects to the broker message server and uses it for sending Published Applications inventory information to the vRealize Operations for Published Applications adapter. The broker message server uses an SSL/TLS channel to encrypt the data that is sent from the broker agent.</td>
</tr>
<tr>
<td>Certificate management server</td>
<td>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 Chapter 11, “Certificate Pairing,” on page 49.</td>
</tr>
</tbody>
</table>
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 6-1. Default Ports for RMI Services

<table>
<thead>
<tr>
<th>RMI Service</th>
<th>Default Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>RMI registry</td>
<td>3095</td>
</tr>
<tr>
<td>Desktop message server</td>
<td>3096</td>
</tr>
<tr>
<td>Broker message server</td>
<td>3097</td>
</tr>
<tr>
<td>Certificate management server</td>
<td>3098</td>
</tr>
</tbody>
</table>

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 vRealize Operations for Published Applications adapter is running.

Table 6-2. RMI Service Port Properties

<table>
<thead>
<tr>
<th>RMI Service</th>
<th>Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>RMI registry</td>
<td>registry-port</td>
</tr>
<tr>
<td>Desktop message server</td>
<td>desktop-port</td>
</tr>
<tr>
<td>Broker message server</td>
<td>broker-port</td>
</tr>
<tr>
<td>Certificate management server</td>
<td>certificate-port</td>
</tr>
</tbody>
</table>

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 vRealize Operations for Published Applications adapter is running.

Prerequisites

- Verify that you can connect to the node where the vRealize Operations for Published Applications adapter is running.
- Become familiar with the RMI service port properties. See “RMI Service Port Properties,” on page 34.

Procedure

1. Log in to the node where the vRealize Operations for Published Applications adapter is running.
2 In a text editor, open the msgserver.properties file.

<table>
<thead>
<tr>
<th>Platform</th>
<th>File Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>/usr/lib/vmware-vcops/user/plugins/inbound/V4PA_adapter3/work/msgserver.properties</td>
</tr>
<tr>
<td>Windows</td>
<td>C:/vmware/vcenter-operations/user/plugins\inbound\V4PA_adapter3\work\msgserver.properties</td>
</tr>
</tbody>
</table>

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 “Open the Ports Used by vRealize Operations for Published Applications,” on page 15.

**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 vRealize Operations for Published Applications 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 vRealize Operations for Published Applications 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.

   a Execute service vmware-vcops-firewall restart.
Changing the Default SSL/TLS Configuration in vRealize Operations for Published Applications

The vRealize Operations for Published Applications broker message server uses an SSL/TLS channel to communicate with the broker agents. The vRealize Operations for Published Applications 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 Protocols and Ciphers for vRealize Operations for Published Applications,” on page 37
- “SSL/TLS Configuration Properties,” on page 38
- “Change the Default SSL/TLS Configuration for Servers,” on page 38
- “Change the Default SSL/TLS for Agents,” on page 39

Default SSL Protocols and Ciphers for vRealize Operations for Published Applications

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_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_DH_DSS_WITH_AES_256_CBC_SHA
- TLS_DH_RSA_WITH_AES_256_CBC_SHA

VMware, Inc.
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 7-1. SSL/TLS Configuration Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>sslProtocols</td>
<td>List of accepted SSL/TLS protocols, separated by commas.</td>
</tr>
<tr>
<td></td>
<td>TLSv1</td>
</tr>
<tr>
<td>sslCiphers</td>
<td>List of accepted SSL/TLS ciphers, separated by commas.</td>
</tr>
<tr>
<td></td>
<td>TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA,</td>
</tr>
<tr>
<td></td>
<td>TLS_DHE_DSS_WITH_AES_128_CBC_SHA</td>
</tr>
</tbody>
</table>

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 vRealize Operations for Published Applications adapter is running.

Prerequisites

- Verify that you can connect to the node where the vRealize Operations for Published Applications adapter is running.
- Become familiar with the SSL/TLS configuration properties. See “SSL/TLS Configuration Properties,” on page 38.

Procedure

1. Log in to the node where the vRealize Operations for Published Applications adapter is running.
2. In a text editor, open the `msgserver.properties` file.
3. Modify the SSL/TLS configuration properties.
4. Save your changes and close the `msgserver.properties` file.
Change the Default SSL/TLS for Agents

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

Prerequisites
- For the desktop agents, verify that you can connect to the remote Published Applications server.
- For a broker agent, verify that you can connect to the host where the Published Applications broker agent is installed.
- Become familiar with the SSL/TLS configuration properties. See “SSL/TLS Configuration Properties,” on page 38.

Procedure

1. Modify the SSL/TLS configuration properties for a desktop agent.
   a. Log in to the Published Applications server where the Published Applications agent is running.
   b. In a text editor, open the msgclient.properties file.
      The msgclient.properties file is in the C:\ProgramData\VMware\vRealize Operations for Published Apps\Desktop Agent\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 remote collector 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\vRealize Operations for Published Apps\Broker Agent\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 Published Applications

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

To increase security, you can replace the default self-signed certificates that the vRealize Operations for Published Applications adapter and broker agents use.

Understanding Authentication for Each Component

Each vRealize Operations for Published Applications component handles authentication differently.

vRealize Operations for Published Applications 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 vRealize Operations for Published Applications 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 vRealize Operations for Published Applications adapter and broker agent before the agents can communicate with the vRealize Operations for Published Applications adapter. See Chapter 11, “Certificate Pairing,” on page 49.

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 desktop agent generates a unique authentication token for each remote desktop.

In addition, the desktop agent generates a serverID for the Published Applications server and write the serverID into vRealize Operations Manager. When a desktop agent attempts to send data to the vRealize Operations for Published Applications adapter, the adapter will verify whether the authentication token has been cached in memory. If there is no server with same name, the adapter caches the server name and authentication token in memory. If the server has been cached, compare the cached authentication token and the one sent. If the tokens are same, accept the message, else reject the desktop agent message.
The vRealize Operations for Published Applications adapter also checks whether a VM with same serverID exists in vRealize Operations Manager, and adds the VM into the topology when a VM with the same name exists.

**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 trust store for the vRealize Operations for Published Applications adapter 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 you first install the broker agent, a self-signed certificate is generated. The broker agent uses this self-signed certificate by default to authenticate to the vRealize Operations for Published Applications adapter. Because this certificate is generated dynamically, you must manually pair the vRealize Operations for Published Applications adapter and broker agent before the broker agent can communicate with the vRealize Operations for Published Applications adapter. For more information, see Chapter 11, “Certificate Pairing,” on page 49.
Certificate and Trust Store Files

The vRealize Operations for Published Applications 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.

This chapter includes the following topics:

- “vRealize Operations for Published Applications Adapter Certificate and Trust Store Files,” on page 43
- “Broker Agent Certificate and Trust Store Files,” on page 44

vRealize Operations for Published Applications Adapter Certificate and Trust Store Files

The certificate and trust store files for the vRealize Operations for Published Applications 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 vRealize Operations for Published Applications adapter is installed. On Linux, the path to the work directory is /usr/lib/vmwarevops/user/plugins/inbound/V4PA_adapter3/. On Windows, the path to the work directory is C:\vmware\vcenteroperations\user\plugins\inbound\V4PA_adapter3/.

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

Table 9-1. Java Key Stores in the work Directory

<table>
<thead>
<tr>
<th>Java Key Store</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>v4pa-adapter.jks</td>
<td>Contains the certificate that the adapter uses to authenticate itself to agents.</td>
</tr>
<tr>
<td>v4pa-truststore.jks</td>
<td>Contains the trust store that the adapter uses to authenticate the broker agent certificate.</td>
</tr>
</tbody>
</table>

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 9-2. Adapter Key Store Configuration Properties in the msgserver.properties File

<table>
<thead>
<tr>
<th>Property</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keyfile</td>
<td>v4pa-adapter.jks</td>
<td>Name of the key store file that contains the adapter certificate.</td>
</tr>
<tr>
<td>keypass</td>
<td></td>
<td>Password to the key store file that contains the adapter certificate. The password is dynamically generated.</td>
</tr>
</tbody>
</table>
**Table 9-2. Adapter Key Store Configuration Properties in the msgserver.properties File (Continued)**

<table>
<thead>
<tr>
<th>Property</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>trustfile</td>
<td>v4pa-truststore.jks</td>
<td>Name of the key store file that contains the adapter trust store.</td>
</tr>
<tr>
<td>trustpass</td>
<td></td>
<td>Password to the key store file that contains the adapter trust store. The password is dynamically generated.</td>
</tr>
</tbody>
</table>

**Broker Agent Certificate and Trust Store Files**

The broker agent certificate and trust store files are in the C:\ProgramData\VMware\vRealize Operations for Published Apps\Broker Agent\conf directory on the vRealize Operations for Published Applications broker 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 9-3. Java Key Stores in the conf Directory**

<table>
<thead>
<tr>
<th>Java Key Store</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>v4pa-brokeragent.jks</td>
<td>Contains the certificate that the broker agent uses to authenticate itself to the vRealize Operations for Published Applications adapter.</td>
</tr>
<tr>
<td>v4pa-truststore.jks</td>
<td>Contains the trust store that the broker agent uses to authenticate the vRealize Operations for Published Applications adapter certificate.</td>
</tr>
</tbody>
</table>

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 9-4. Broker Agent Key Store Configuration Properties in the msgclient.properties File**

<table>
<thead>
<tr>
<th>Property</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keyfile</td>
<td>v4pa-brokeragent.jks</td>
<td>The name of the key store file that contains the broker agent's certificate.</td>
</tr>
<tr>
<td>keypass</td>
<td></td>
<td>The password to the key store file that contains the broker agent's certificate. The password is dynamically generated.</td>
</tr>
<tr>
<td>trustfile</td>
<td>v4pa-truststore.jks</td>
<td>The name of the key store file that contains the broker agent's trust store.</td>
</tr>
<tr>
<td>trustpass</td>
<td></td>
<td>The password to the key store file that contains the broker agent's trust store. The password is dynamically generated.</td>
</tr>
</tbody>
</table>
Replacing the Default Certificates

By default, the vRealize Operations for Published Applications 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.

This chapter includes the following topics:

- “Replace the Default Certificate for the vRealize Operations for Published Applications Adapter,” on page 45
- “Replace the Default Certificate for the Broker Agent,” on page 47

Replace the Default Certificate for the vRealize Operations for Published Applications Adapter

A self-signed certificate is generated when you first install the vRealize Operations for Published Applications 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 vRealize Operations for Published Applications adapter is running.
- Verify that you have the password for certificate store. You can obtain the password from the msgserver.properties file. See “vRealize Operations for Published Applications Adapter Certificate and Trust Store Files,” on page 43.
- Become familiar with the Java keytool utility. Documentation is available at http://docs.oracle.com.

Procedure

1. Log in to the node where the vRealize Operations for Published Applications adapter is running.
2. Navigate to the vRealize Operations for Published Applications adapter’s work directory.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Directory Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>/usr/lib/vmware-vcops/user/plugins/inbound/V4PA_adapter3/work</td>
</tr>
<tr>
<td>Windows</td>
<td>C:\vmware\vcenteroperations\user\plugins\inbound\V4PA_adapter3\work</td>
</tr>
</tbody>
</table>
3 Use the keytool utility with the -selfcert option to generate a new self-signed certificate for the vRealize Operations for Published Applications 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 v4pa-adapter -dname dn-of-org -keystore v4pa-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 v4pa-adapter -file certificate-request-file -keystore v4pa-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 vRealize Operations for Published Applications adapter work directory and run the keytool utility with the -import option.

For example:

```
keytool -import -alias v4pa-adapter -file certificate-filename -keystore v4pa-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 vRealize Operations for Published Applications adapter on the node where the adapter is running.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>Run the <code>service vmware-vcops restart</code> command.</td>
</tr>
<tr>
<td>Windows</td>
<td>Use the Windows Services tool (<code>services.msc</code>) to restart the vRealize Operations for Published Applications Adapter service.</td>
</tr>
</tbody>
</table>

What to do next

After you restart the vRealize Operations for Published Applications adapter, you must pair any broker agents that are attached to the vRealize Operations for Published Applications adapter. See Chapter 11, “Certificate Pairing,” on page 49.
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 vRealize Operations for Published Applications 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 Published Applications Session host where the broker agent is installed.
- Verify that the keytool utility is added to the system path on the data collector 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 44.
- Become familiar with the Java keytool utility. Documentation is available at http://docs.oracle.com

Procedure

1. Log in to the vRealize Operations for Published Applications Server host where the broker agent is installed.

2. Use the keytool utility with the -selfcert option 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 v4pa-brokeragent -dname dn-of-org -keystore v4pa-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 v4pa-brokeragent -file certificate-request-file -keystore v4pa-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 v4pa-brokeragent -file certificate-filename -keystore v4pa-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 v4pa-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 for Published Applications Broker Agent Settings wizard, or by restarting the vRealize Operations for Published Applications Broker Agent Service.

**What to do next**

After you restart the broker agent, you must pair it with the vRealize Operations for Published Applications adapter. See Chapter 11, “Certificate Pairing,” on page 49.
Before broker agents can communicate with the vRealize Operations for Published Applications 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 is 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 Published Applications Session hosts with Group Policy.

After the certificates are successfully paired, they are cached in the trust stores for each individual component. If a new Published Applications server is provisioned, the adapter’s certificate is sent to the server by using the Group Policy, 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 for Published Applications Broker Agent Settings wizard to pair certificates.
SSL/TLS and Authentication-Related Log Messages

The vRealize Operations for Published Applications adapter logs SSL/TLS configuration and authentication-related messages.

Table 12-1. vRealize Operations for Published Applications Adapter Log Message Types

<table>
<thead>
<tr>
<th>Log Message Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONFIGURATION</td>
<td>The SSL/TLS configuration that is being used.</td>
</tr>
<tr>
<td>AUTHENTICATION SUCCESS</td>
<td>A remote desktop has been successfully authenticated.</td>
</tr>
<tr>
<td>AUTHENTICATION FAILED</td>
<td>A remote desktop has failed authentication.</td>
</tr>
</tbody>
</table>

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.
Create a vRealize Operations Manager Support Bundle

If the vRealize Operations for Published Applications adapter does not operate as expected, you can collect log and configuration files in a support bundle and send the support bundle to VMware for analysis.

Procedure
1. Log in to the vRealize Operations Manager user interface with admin privileges.
2. Click the Administration tab and select Support > Support Bundles.
3. Click the Create Support Bundle (plus sign) icon.
4. Select the type of support bundle to generate and the nodes to include in the support bundle.
5. Click OK to create the support bundle.

The progress of the support bundle appears in the Status column on the Support Bundles pane. Support bundle creation might take several minutes, depending on the size of the logs and the number nodes. You can click the Reload Support Bundle icon to refresh the status.
6. Select the support bundle and click the Download Support Bundle icon to download the support bundle to the server.

You cannot download a support bundle until its status is Succeed. For security, vRealize Operations Manager prompts you for credentials when you download a support bundle.
7. (Optional) Send the support bundle to VMware for support.
Download vRealize Operations for Published Applications Broker Agent Log Files

If the vRealize Operations for Published Applications broker agent does not operate as expected, you can download the broker agent log files.

Prerequisites
Verify that you have administrator privileges.

Procedure
1. Log in to the machine where the broker agent is installed.
2. Navigate to `C:\ProgramData\VMware\vRealize Operations for Published Apps\Broker Agent\logs` on broker agent machine.
   The `logs` directory contains the broker agent log files.
3. Use an archive program to create a ZIP file that contains the log files in the `logs` directory.
4. Send the ZIP file to VMware for support.
Download vRealize Operations for Published Applications Desktop Agent Log Files

If the vRealize Operations for Published Applications desktop agent is not operating as expected, you can download the desktop agent log files from the remote desktop and send the log files to VMware for support.

vRealize Operations for Published Applications retains desktop agent log files of the previous seven days by default. You can specify the number of days that vRealize Operations for Published Applications retains desktop agent log files by updating the registry entry LogPruneThreshold under HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\vRealize Operations for Published Apps\Desktop Agent.

Procedure

1. Log in to the controller server or session host server where the desktop agent is installed.
2. Navigate to C:\ProgramData\VMware\vRealize Operations for Published Apps\Desktop Agent\logs and locate the desktop agent log files.
   Desktop agent log file names begin with v4pa-.
3. Use an archive program to create a ZIP file that contains the desktop agent log files.
4. Send the ZIP file to VMware for support.
View Collector and vRealize Operations for Published Applications Adapter Log Files

You can view collector and vRealize Operations for Published Applications adapter log files in the vRealize Operations Manager user interface. Log files are organized in log type folders.

Prerequisites
Verify that you have administrator privileges.

Procedure
1. Log in to the vRealize Operations Manager user interface with admin privileges.
2. Click the Administration tab, click Support, and click Logs.
3. Select Log Type from the Group by drop-down menu.
4. Double-click the Collector folder and double-click the folder for the node on which the adapter instance is running.
5. View the log files.
   a. Double-click a log file to view the contents of the log file.
   b. Type line numbers in the Starting line and # of lines text boxes and click the Load log content icon (> ) to view a specific part of the log file.
6. Click the Reload Tree icon to reload the log tree information and collapse all open folders.
Modify the Logging Level for vRealize Operations for Published Applications Adapter Log Files

You can modify the logging level for the collector node that contains the log files for a vRealize Operations for Published Applications adapter instance.

**Prerequisites**
Verify that you have administrator privileges.

**Procedure**
1. Log in to the vRealize Operations Manager user interface.
2. Click the Administration tab, click Support, and click Logs.
3. Select Log Type from the Group by drop-down menu.
4. Expand the Collector folder.
5. Select the node on which the vRealize Operations for Published Applications adapter instance is running and click the Edit Properties icon.
6. In the Logging Level column, click the logging level for the vRealize Operations for Published Applications adapter log class.
7. Select a logging level from the drop-down menu.

To troubleshoot problems, set the logging level to Info. To view detailed messages, including micro steps, queries, and returned results, set the logging level to Debug.

**Note** If you set the logging level to Debug, log files can become large very quickly. Set the logging level to Debug only for short periods of time.
P
ports
default 15
RMI services 34
product compatibility 11

R
replacing the default certificate, broker agent 47
reports, subjects 30
RMI communication 33
RMI services
  changing default ports 34
  ports 34

S
security, RMI communication 33
software requirements 11
SSL/TLS
ciphers 37
  configuration 37
SSL/TLS configuration properties 38
SSL/TLS configuration 37
system requirements 11
system components 8

T
troubleshooting
  adapter 59, 61
  broker agent 55
  configuration files 53
  desktop agent 57
  log files 53, 55, 57, 59, 61
  support bundle 53
  trust store files, broker agent 44

U
using reports 29

W
Web Interface server, firewall rules 19
Web Interface servers 28

X
XA Application Usage dashboard 29
XA Applications dashboard 29
XA Infrastructure dashboard 28
XA Overview dashboard 27
XA server, firewall rules 19
XA Servers dashboard 28
XA Session Detail dashboard 28