VMware vRealize Operations for Horizon Administration Guide

17 OCT 2019

VMware vRealize Operations for Horizon 6.7

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

VMware vRealize Operations for Horizon Administration Guide

The *VMware vRealize Operations for Horizon Administration Guide* describes how to monitor VMware Horizon® environments through VMware vRealize® Operations Manager™.

Intended Audience

This information is intended for users who monitor the performance of objects in Horizon environments in vRealize Operations Manager and administrators who are responsible for maintaining and troubleshooting a vRealize Operations for Horizon deployment.

Terminology

For definitions of terms as they are used in this document, see the VMware Glossary at https://www.vmware.com/topics/glossary.

Monitoring Your Horizon Environment

1

The vRealize Operations for Horizon solution includes Horizon-specific dashboards and report templates that appear in the vRealize Operations Manager user interface. You can use these dashboards and reports together with the standard vRealize Operations Manager object monitoring features to monitor your Horizon environment.

This chapter includes the following topics:

Using the Horizon Dashboards

You can use preconfigured Horizon dashboards to view metrics and information about your environment and the objects in it.

The preconfigured Horizon dashboards are listed in the following table.

Table 1-1. Horizon Dashboards

Dashboard	What It Shows	When to Use It
Horizon Overview Dashboard	Status of your Horizon environment, including the top Horizon-related alerts.	■ Assess Horizon pod usage, client performance, and overall user experience. ■ View the top alerts.
Horizon Help Desk Dashboard	Detailed information about all connected sessions in your environment.	■ View detailed information about connected sessions. ■ View all alerts for the environment.
Horizon Infrastructure Dashboard	Information about the health, workload, and connectivity of infrastructure hosts, remote desktops, datastores, and RDS hosts in your environment.	■ Understand the relationships between objects in your Horizon infrastructure. ■ Assess the underlying vSphere and Horizon infrastructure.
Horizon User Sessions Dashboard	Metrics and performance information for all types of sessions, including VDI desktop sessions, RDS desktop sessions, and application sessions.	■ Identify and troubleshoot poorly performing user sessions.
Horizon VDI Pools Dashboard	Metrics and performance information for VDI pools.	■ Troubleshoot poorly performing desktop virtual machines and sessions.

Table 1-1. Horizon Dashboards (continued)

Dashboard	What It Shows	When to Use It
Horizon RDS Pools Dashboard	Metrics and performance information for RDS pools.	■ Identify the RDS hosts that are using the most resources. ■ Troubleshoot poorly performing RDS desktop and application sessions.
Horizon Applications Dashboard	Status and performance information for application pools and their associated farms, RDS hosts, application sessions, applications, and Horizon clients.	■ Understand the relationships between objects in your application infrastructure. ■ Troubleshoot remote applications.
Horizon Desktop Usage Dashboard	Usage data for all desktop pools in your environment.	■ View connected and disconnected sessions for all desktop pools. ■ View top alerts and resource trends for selected desktop pools. ■ Collect in-guest process data from desktop sessions.
Horizon User Session Details Dashboard	Detailed information about all types of sessions running in your environment, including VDI desktop sessions, RDS desktop sessions, and application sessions.	■ Troubleshoot poorly performing sessions. ■ Identify when session problems occurred. ■ Collect in-guest process data from desktop sessions.
Horizon RDS Host Details Dashboard	Detailed information about the RDS hosts in your Horizon environment.	■ View desktop and application sessions currently running on selected RDS hosts. ■ Identify when RDS host problems occurred. ■ Collect and view in-guest process data from RDS hosts.
Horizon Adapter Self Health Dashboard	License compliance information and health information for your Horizon Adapter instances and broker agents.	■ Troubleshoot Horizon Adapter problems. ■ Monitor license usage.
Horizon End User Experience Dashboard	Health information for your resources.	■ Troubleshoot problems related to end-user experience.
Horizon Root Cause Analysis Dashboard	Detailed information on specific metrics, including performance over time.	■ Troubleshoot problems related to specific object-related metrics.

The colored rectangles in certain widgets are representations of specific objects. You can point to any of these rectangles to view basic information about the object it represents. In the **Configurations** drop-down menu in the widget toolbar, you can select how the system arranges these objects by size and color.

The Horizon dashboards are created from standard vRealize Operations Manager widgets. If your user account has the necessary permissions, you can create or modify dashboards and widgets that use Horizon objects.

For more information about configuring dashboards and widgets, see "Configuring Data Display" in the *vRealize Operations Manager Configuration Guide*.

Horizon Overview Dashboard

Use the **Horizon Overview** dashboard to visualize your end-to-end Horizon environment, its underlying environment, and alerts.

Table 1-2. Horizon Overview Widgets

Widget	What It Shows
Top Horizon Alerts	Alerts of the greatest significance to Horizon objects. You can click an alert to see details.
Horizon Pods	All Horizon pods in your environment. Select a pod to see related information in the other widgets.
Pod Session Metrics	Session-related statistics and metrics, including login time, latency, and bandwidth, for the selected pod.
vCenter Server Instances	CPU, memory, and disk usage for each vCenter Server instance.
Capacity Remaining	Percentage of total vCenter Server instance resources that can still be used.
Unified Access Gateways	Information about Unified Access Gateway appliances configured for the selected pod.

Horizon Help Desk Dashboard

Use the **Horizon Help Desk** dashboard to view detailed information about all connected sessions running in your Horizon environment.

The objects displayed on this dashboard can be used for root cause analysis. Click an object and select **Dashboard Navigation > Navigate > Horizon Root Cause Analysis** in the widget toolbar to view information about the object in the **Horizon Root Cause Analysis** dashboard.

Note vGPU widgets are not installed by default. To obtain them, see "Import vGPU Dashboards" in *vRealize Operations for Horizon Installation*.

Table 1-3. Horizon Help Desk Widgets

Widget	What It Shows
Horizon Connected Sessions	All connected VDI desktop sessions, RDS desktop sessions, and application sessions in your environment. Select a session to see related information in the other widgets.
Session Related Metrics	Health, alerts, workload, and other metrics related to the object selected in the **Select Session Related Objects** widget. **Note** **TX Bandwidth** is not displayed for Horizon 7.3 Blast sessions.
VM Metrics	Health, workload, and other metrics for the virtual machine associated with the selected session.
Session Processes	Information about in-guest desktop processes and their resource usage. To display information, select an action from the drop-down menu in the toolbar and click **Go**.
Session Logon Breakdown	AppStack attachment time, profile and shell loading time, and session interaction time for the logged-in user.
User Desktop Application Launch History	Desktop applications launched by users.
Host Metrics	Health, workload, and other metrics for the ESXi host of the virtual machine associated with the session.
All Environment Alerts	All alerts on the system. You can click an alert to see details.

Table 1-3. Horizon Help Desk Widgets (continued)

Widget	What It Shows
Selected User Session Alerts	Alerts for the selected session. You can click an alert to see details.
Selected Session Related Objects	Objects related to the selected session. Select an object to see related information in the **Session Related Metrics** widget.
Horizon Client Details	IP addresses and the name and type of machine for the selected session.
Virtual Desktop	Adapter type, object type, policy, collection state, and collection status of the virtual desktop.
vGPU	vGPUs for the selected session.
Selected vGPU Related Objects	Objects related to the selected vGPU.
User	Adapter type, object type, policy, collection state, and collection status of the user.
VM Host	Adapter type, object type, policy, collection state, and collection status of the ESXi host of the virtual machine associated with the session.

Horizon Infrastructure Dashboard

Use the **Horizon Infrastructure** dashboard to quickly assess the health, workload, and connectivity of the infrastructure that supports your Horizon environment.

Table 1-4. Horizon Infrastructure Widgets

Widget	What It Shows
Horizon Infrastructure Hosts	Hosts in your Horizon environment.
Horizon Datastores	Datastores in your Horizon environment.
Horizon VDI Desktop VMs	VDI desktop virtual machines in your Horizon environment.
Horizon RDS Hosts	RDS hosts in your Horizon environment.

Horizon User Sessions Dashboard

Use the **Horizon User Sessions** dashboard to obtain an overview of all sessions running in your Horizon environment.

Table 1-5. Horizon User Sessions Widgets

Widget	What It Shows
VDI Desktop Sessions	All VDI desktop sessions in your environment. Point to any session for details.
Top VDI Desktop Session PCoIP Latency	VDI desktop sessions with the highest PCoIP latency.
Top VDI Desktop Session PCoIP TX Bandwidth	VDI desktop sessions with the highest PCoIP transfer bandwidth.
Top VDI Desktop Session PCoIP Packet Loss	VDI desktop sessions with the highest PCoIP packet loss rate.
Top VDI Desktop Session Logon Time	VDI desktop sessions with the longest login time.
RDS Desktop Sessions	All RDS desktop sessions in your environment. Point to any session for details.
Top RDS Desktop Session PCoIP Latency	RDS desktop sessions with the highest PCoIP latency.

Table 1-5. Horizon User Sessions Widgets (continued)

Widget	What It Shows
Top RDS Desktop Session PCoIP TX Bandwidth	RDS desktop sessions with the highest PCoIP transfer bandwidth.
Top RDS Desktop Session PCoIP Packet Loss	RDS desktop sessions with the highest PCoIP packet loss rate.
Top RDS Desktop Session Logon Time	RDS desktop sessions with the longest login time.
Application Sessions	All application sessions in your environment. Point to any session for details.
Top Application Session PCoIP Latency	Application sessions with the highest PCoIP latency.
Top Application Session PCoIP TX Bandwidth	Application sessions with the highest PCoIP transfer bandwidth.
Top Application Session PCoIP Packet Loss	Application sessions with the highest PCoIP packet loss rate.
Top Application Session Logon Time	Application sessions with the longest login time.

Horizon VDI Pools Dashboard

Use the **Horizon VDI Pools** dashboard to view the performance of VDI desktop pools and sessions in your Horizon environment. VDI desktop pools include linked-clone, instant-clone, automated, and manual desktop pools.

Table 1-6. Horizon VDI Pools Widgets

Widget	What It Shows
VDI Desktop Pools	All VDI desktop pools in the environment and their type, health, capacity used, and number of sessions. Select a desktop pool to see related information in the other widgets.
Desktop Applications	All configured applications hosted by a VDI desktop. **Note** You must manually configure applications that you want to appear in the **Desktop Applications** widget. For more information, see Configure Desktop Applications.
VDI Desktop Pool VMs	All virtual machines in the selected desktop pool. Point to any virtual machine for details.
Top VDI Desktop VM CPU Workload	VDI desktop virtual machines with the highest CPU workload.
Top VDI Desktop VM Memory Workload	VDI desktop virtual machines with the highest memory workload.
Top VDI Desktop VM Datastore IO Workload	VDI desktop virtual machines with the highest datastore I/O workload.
Top VDI Desktop VM Network IO Workload	VDI desktop virtual machines with the highest network I/O workload.
VDI Desktop Pool Indicator Metrics	Metrics for the selected desktop pool and a graph of how they have changed over time.
Desktop Application Users	History of user login information for the selected application.
VDI Desktop Sessions	All desktop sessions in the selected desktop pool. Point to any session for details.
Top VDI Desktop Session PCoIP Latency	VDI desktop sessions with the highest PCoIP latency.

Table 1-6. Horizon VDI Pools Widgets (continued)

Widget	What It Shows
Top VDI Desktop Session PCoIP TX Bandwidth	VDI desktop sessions with the highest PCoIP transfer bandwidth.
Top VDI Desktop Session TX Packet Loss	VDI desktop sessions with the highest transfer packet loss rate.
Top VDI Desktop Session Logon Time	VDI desktop sessions with the longest login time.

Horizon RDS Pools Dashboard

Use the **Horizon RDS Pools** dashboard to view the performance of the RDS farms, hosts, desktop pools, and application pools in your Horizon environment.

Table 1-7. Horizon RDS Pools Widgets

Widget	What It Shows
Farms	RDS farms, their health and type, and the number of sessions, desktops, and applications. Select a farm to see related information in the other widgets.
RDS Hosts	All RDS hosts. Point to a host for details.
Top RDS Host CPU Workload	RDS hosts with the highest CPU workload.
Top RDS Host Committed Bytes In Use	RDS hosts with the most committed bytes in use.
Top RDS Host Disk Transfers Per Second	RDS hosts with the most disk transfers per second.
Top RDS Host Bytes Sent Per Second	RDS hosts that send the most bytes per second.
RDS Desktop Pools	RDS desktop pools and their health and session information.
RDS Desktop Sessions	All RDS desktop sessions. Point to a session for details.
Top RDS Desktop Session PCoIP Latency	RDS desktop sessions with the highest PCoIP latency.
Top RDS Desktop Session PCoIP TX Bandwidth	RDS desktop sessions with the highest PCoIP transfer bandwidth.
Top RDS Desktop Session PCoIP Packet Loss	RDS desktop sessions with the highest PCoIP packet loss rate.
Top RDS Desktop Session Logon Time	RDS desktop sessions with the longest login time.
Application Pools	Application pools and their health and number of instances.
Application Sessions	All application sessions in your environment. Point to any session for details.
Top Application Session PCoIP Latency	Application sessions with the highest PCoIP latency.
Top Application Session PCoIP TX Bandwidth	Application sessions with the highest PCoIP transfer bandwidth.
Top Application Session PCoIP Packet Loss	Application sessions with the highest PCoIP packet loss rate.
Top Application Session Logon Time	Application sessions with the longest login time.

Horizon Applications Dashboard

Use the **Horizon Applications** dashboard to view the status and performance of application pools and their associated farms, hosts, instances, and users.

Table 1-8. Horizon Applications Widgets

Widget	What It Shows
Application Pools	All application pools in the environment. Select an application pool to see related information in other widgets.
Application Instances	Running instances of the selected application pool, including the user name, session state, duration, server, virtual machine, and collection status of each instance.
Application Users	Users that launched the selected application during the specified time period. You can click the **Date Controls** icon in the toolbar to configure up to three time periods. The default setting is the past hour.
Application Pool Relationship	Parent and children objects of the selected application pool.
Application Instance Resource Trend	Usage of application instance resources over time. You can click the **Time Range** icon in the toolbar to set the period of time in which you want to see trends. The default setting is the past hour.

Horizon Desktop Usage Dashboard

Use the **Horizon Desktop Usage** dashboard to view usage data for the VDI desktop pools in your Horizon environment.

Table 1-9. Horizon Desktop Usage Widgets

Widget	What It Shows
All Desktop Pools	All VDI desktop pools in the environment with their session and connection information. RDS and application pools are not included. Select a pool to see related information in the other widgets.
Pool Desktop Sessions	All sessions for the selected desktop pool and login information.
Running Application/Process	Information about in-guest desktop processes and their resource usage. To display information, select an action from the drop-down menu in the toolbar and click **Go**.
Pool Events	Timeline of events and alerts for the selected pool. You can set filtering criteria on the widget toolbar.
Top Pool Alerts	The most significant active alerts for the selected pool.
Desktop Resource Trend	Resource workload and metrics for the selected pool over time. You can click the **Time Range** icon in the toolbar to set the period of time in which you want to see trends. The default setting is the past hour.
User VDI Desktop Resource Consumption	Pool resources consumed by each VDI desktop user.

Horizon User Session Details Dashboard

Use the **Horizon User Session Details** dashboard to view detailed information about all types of sessions running in your Horizon environment.

Table 1-10. Horizon User Session Details Widgets

Widget	What It Shows
Horizon Remote Sessions	All VDI desktop sessions, RDS desktop sessions, and application sessions in your environment.
Session Indicator Metrics	Session health, workload, login time, latency, frame rate, and PCoIP and Blast metrics.
Session Logon Breakdown	Time metrics for AppStack attachment, profile and shell loading, and session interaction.
Session Processes	Session processes.
Session Health & Events	Timeline of health and alerts for the selected session. You can set filtering criteria on the widget toolbar.
Users	All active users in the current environment.
Applications Launched By User	Users that opened the selected application in the specified time period.
Session Related Objects	Objects related to the selected session.
Desktop Application Launched By User	Users that opened the selected desktop application in the specified time period.

Horizon RDS Host Details Dashboard

Use the **Horizon RDS Host Details** dashboard to view detailed information about RDS hosts in your Horizon environment, including host health, PCoIP-related data, detailed session data, and user resource consumption.

Table 1-11. Horizon RDS Host Details Widgets

Widget	What It Shows
RDS Hosts	All RDS hosts in the environment with their collection status, health, and other metrics. Select a host to show information in the other widgets.
RDS Host Indicator Metrics	Key host metrics, including health, workload, sessions, and PCoIP latency, bandwidth, and packet loss.
RDS Host Processes & Users	Information about in-guest host processes and their resource usage. To display information, select an action from the drop-down menu in the toolbar and click **Go**.
RDS Host Sessions	Desktop and application sessions running on the selected host. The collection state and status, health score, workload, session state, protocol, and latency are displayed in sortable columns.
User Resource Consumption	Host resources consumed by each user, including CPU and storage metrics.
RDS Host Health and Events	Timeline of host health and alerts. You can set filtering criteria on the widget toolbar.

Horizon Adapter Self Health Dashboard

Use the **Horizon Adapter Self Health** dashboard to view health and licensing information for vRealize Operations for Horizon adapter instances and the broker agents that are connected to them.

Note Metric collection metrics are sent every five minutes, topology collection metrics are sent every hour, and event database collection metrics are sent when there are relevant events. For this reason, broker agent metrics might be outdated when compared with the metrics on other dashboards. In addition, if no events have been received during the past six hours, event-related metrics might display **No Data** even though data has been collected.

Table 1-12. Horizon Adapter Self Health Widgets

Widget	What It Shows
Horizon Adapter	All Horizon Adapter instances and their collection status and number of desktops reporting. Select an adapter instance to see related information in the **Horizon Adapter Status** and **Horizon Adapter Statistics** widgets.
Horizon Adapter Status	Length of the last collection period, number of desktops that sent data samples during that period, and the total number of objects that the adapter instance received during that period.
Horizon Adapter Statistics	Key adapter instance metrics over time. You can click the **Time Range** icon in the toolbar to set the period of time in which you want to see trends. The default setting is the past hour.
License Usage History	License usage over time. You can click the **Date Controls** icon in the toolbar to configure up to three time periods. The default setting is the past hour. You can also click the **Options** icon in the upper right corner to save a snapshot of the chart, download its data as a CSV file, or change the position of the chart in the widget.
Active License Alerts	License-related alerts for the selected adapter instance. You can click an alert to see details.
Horizon Broker Agent	All broker agents and their collection status and time. Select a broker agent to see related information in the other widgets.
Horizon Broker Agent Status	Collection time, number of user sessions, and number of events for the selected broker agent.
Horizon Broker Agent Topology Collection Statistics	Key metrics for topology collection on the selected broker agent.
Horizon Broker Agent Metric Collection Statistics	Key metrics for metric collection on the selected broker agent.
Horizon Broker Agent Event DB Collection Statistics	Key metrics for event collection on the selected broker agent.

Horizon End User Experience Dashboard

Use the **Horizon End User Experience** dashboard to monitor infrastructure performance that might negatively impact user session experience.

The objects displayed on this dashboard can be used for root cause analysis. Click an object and select **Dashboard Navigation > Navigate > Horizon Root Cause Analysis** in the widget toolbar to view information about the object in the **Horizon Root Cause Analysis** dashboard.

Note vGPU widgets are not installed by default. To obtain them, see "Import vGPU Dashboards" in *vRealize Operations for Horizon Installation*.

Table 1-13. Horizon End User Experience Widgets

Widget	What It Shows
vCPU Experience	Virtual machines and hosts in order of specified CPU metric. You can specify a metric in the **Configurations** drop-down menu in the widget toolbar. Select an object to display related information in the **vCPU Relationship** and **vCPU Ready% Chart** widgets.
vCPU Relationship	Parent and child objects of the selected virtual machine or host.
vCPU Ready% Chart	Changes over time for a metric associated with the selected virtual machine or host. The metric selected in the **Configurations** drop-down menu in the **vCPU Experience** widget is used to create this chart.
Session Experience	User sessions in order of specified metric. You can specify a metric in the **Configurations** drop-down menu in the widget toolbar. Select a session to display related information in the **Session Relationship** and **Session Chart** widgets.
Session Relationship	Parent and child objects of the selected session.
Session Chart	Changes over time for a metric associated with the selected session. The metric selected in the **Configurations** drop-down menu in the **Session Experience** widget is used to create this chart.
vGPU 3D Utilization Experience	vGPUs in order of percentage of computing resources used. You can specify a metric in the **Configurations** drop-down menu in the widget toolbar. Select an object to display related information in the **vGPU 3D Utilization Relationship** and **vGPU 3D Utilization Chart** widgets.
vGPU 3D Utilization Relationship	Parent and child objects of the selected vGPU.
vGPU 3D Utilization Chart	Changes over time for a metric associated with the selected object. The metric selected in the **Configurations** drop-down menu in the **vGPU 3D Utilization Experience** widget is used to create this chart.
vGPU Memory Utilization Experience	vGPUs in order of percentage of memory used. You can specify a metric in the **Configurations** drop-down menu in the widget toolbar. Select a session to display related information in the **vGPU Memory Utilization Relationship** and **vGPU Memory Utilization Chart** widgets.
vGPU Memory Utilization Relationship	Parent and child objects of the selected object.
vGPU Memory Utilization Chart	Changes over time for a metric associated with the selected object. The metric selected in the **Configurations** drop-down menu in the **vGPU 3D Utilization Experience** widget is used to create this chart.
vDisk Experience	Virtual machines and datastores in order of specified latency metric. You can specify a metric in the **Configurations** drop-down menu in the widget toolbar. Select an object to display related information in the **vDisk Relationship** and **vDisk Latency Chart** widgets.
vDisk Relationship	Parent and child objects of the selected virtual machine or datastore.
vDisk Latency Chart	Changes over time for a metric associated with the selected virtual machine or datastore. The metric selected in the **Configurations** drop-down menu in the **vDisk Experience** widget is used to create this chart.

Table 1-13. Horizon End User Experience Widgets (continued)

Widget	What It Shows
vRAM Experience	Virtual machines in order of specified RAM metric. You can specify a metric in the **Configurations** drop-down menu in the widget toolbar. Select an object to display related information in the **vRAM Relationship** and **vRAM Chart** widgets.
vRAM Relationship	Parent and child objects of the selected virtual machine.
vRAM Chart	Changes over time for a metric associated with the selected virtual machine. The metric selected in the **Configurations** drop-down menu in the **vRAM Experience** widget is used to create this chart.
Active Session Alerts	All alerts for active Horizon sessions.
Pool Critical Alerts	Number of critical alerts for VDI desktop pools.

Horizon Root Cause Analysis Dashboard

Use the **Horizon Root Cause Analysis** dashboard to obtain a detailed view of an object's metrics for use in further analysis.

To use this dashboard, first locate an object on the **Horizon Help Desk** or **Horizon End User Experience** dashboard that you want to analyze. Click the object and select **Dashboard Navigation > Navigate > Horizon Root Cause Analysis** in the widget toolbar. The object is displayed in the **Selected Object Relationship** widget, and metrics and alerts for the object are displayed in the other widgets. You can also select another object in the **Selected Object Relationship** to view its metrics.

In the **Selected Object Analysis Snapshot** widget, you can select one or more metrics to display charts showing their changes over time in the **Selected Metric Chart** widget. The widget can contain metrics from more than one object.

In the **Selected Metric Chart** widget toolbar, you can click the **Time Range** icon in the toolbar to set the period of time in which you want to see trends. You can also click the **Options** icon in the upper right corner to save a snapshot of the chart, download its data as a CSV file, or change the position of the chart in the widget.

Using the Horizon Reports

You can use predefined templates to generate reports about your Horizon objects. These reports provide information about remote desktop and application usage, desktop and application pool configuration details, and license compliance.

You can see a list of all report templates and generated reports by clicking **Dashboards** in the main menu and then **Reports** in the left pane. Enter `Horizon` in the **Quick filter** text box to display only Horizon reports. You can also double-click a Horizon object and select the **Reports** tab to view all report templates available for the object and all generated reports associated with it.

Table 1-14. Horizon Reports

Template Name	Objects	Report Content
Horizon Application Instance Usage	■ Hosted application	CPU and memory usage.
Horizon Application Pool Details	■ Application pool ■ Pod pools tier ■ Horizon pod	Application pool configuration and application pool, RDS farm, and RDS host usage information.
Horizon Application Pool Usage	■ Application pool ■ Pod pools tier ■ Horizon pod	Application instances running, session durations, and last login timestamps.
Horizon Application Usage Report	■ Horizon pod ■ Application pool	Pool name, farm name, times launched, peak concurrent instances, and total usage time over the past seven days.
Horizon Desktop Application Instance Usage	■ Desktop application instance	CPU and memory usage.
Horizon Desktop Application Usage	■ Desktop application ■ Horizon pod ■ Desktop applications tier	Times a desktop application was launched, peak concurrent instances, and total usage time.
Horizon Desktop Pool Usage	■ VDI desktop pool ■ RDS desktop pool ■ Pod pools tier ■ Horizon pod	Number of connected and disconnected sessions, session durations, and last login timestamps.
Horizon Pod License Compliance	■ Horizon pod	Current license usage, highest daily usage, and trends over the past 30 days.
Horizon Pool Usage Overview	■ Pod pools tier ■ Horizon pod	Desktop and application pool session usage.
Horizon RDS Desktop Pool Details	■ RDS desktop pool ■ Pod pools tier ■ Horizon pod	Session and instance information for RDS pools.
Horizon User Session Statistics	■ User	Session and instance duration over the past seven days.
Horizon VDI Desktop Pool Details	■ VDI desktop pool ■ Pod pool tier	Usage, configuration, source, sessions, desktops, users, connection time, PCoIP latency, errors, and desktop status.
Horizon VDI Desktop Session Statistics	■ VDI desktop pool ■ Pod pool tier	Connection, login, PCoIP, and workload statistics.

Maintaining vRealize Operations for Horizon 2

You can modify your vRealize Operations for Horizon configuration at any time to respond to changes in your Horizon environment.

This chapter includes the following topics:

Modify Broker Agent Settings

If your Horizon environment changes after the initial configuration of the broker agent, you can modify the broker agent settings on the Horizon Connection Server host where the broker agent is installed.

Procedure

1 Log in to the Horizon Connection Server host as a Horizon administrator.

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

3 Click through each page of the wizard and make any necessary changes.

   - Pair the broker agent to a different adapter instance or use a different credential.
   - Update Horizon Connection Server or event database credentials.
   - Add or remove desktop pools from the scope of monitored objects.
   - Add or remove App Volumes Manager installations and Unified Access Gateway appliances from the scope of monitored objects.
   - Modify collection interval, timeout, and logging settings.

4 On the **Ready To Complete** page, review your settings and click **Finish**.

   The **Broker Agent Config Utility for Horizon** wizard closes, and the broker agent service is restarted.

Stop or Restart the Broker Agent Service

You can stop, start, and restart the broker agent service on the Horizon Connection Server host where the broker agent is installed.

Procedure

1. Log in to the Horizon Connection Server host as a Horizon administrator.
2. Select **Start > VMware > vRealize Operations for Horizon Broker Agent Settings**.
3. Click **Next** until the **Broker Agent Service** page is displayed.
4. Click the **Start**, **Stop**, or **Restart** button to make the necessary change.

   The status of the broker agent service is shown next to **Current Status**.
5. Click **Next** and click **Finish** to exit the wizard.

Configure Desktop Applications

You manually configure desktop applications that you want to appear on dashboards and reports.

Procedure

1. Open the `/usr/lib/vmware-vcops/user/plugins/inbound/V4V_adapter3/conf/v4v-desktop-app-config.properties` file on the vRealize Operations Manager master node.
2. Add entries for the desktop applications that you want to monitor.

   Use the *name*,*full-path*,*pod-name* format for application entries. If you do not specify a pod name, the application is monitored on all pods.

   For example, the following entry monitors Microsoft Notepad on a pod named Cluster-SERVER621:

   ```
   myapp,c:\windows\notepad.exe,Cluster-SERVER621
   ```
3. (Optional) Enable application instance monitoring. If you do not enable this feature, the system displays only the desktop applications tier and desktop applications objects.

   a. Open the `/usr/lib/vmware-vcops/user/plugins/inbound/V4V_adapter3/conf/v4v.properties` file on the vRealize Operations Manager master node.

   b. Change the value of `enableDesktopApplicationInstance` to `true`.
4. Restart all nodes that collect data from the affected pods.

   ```
   service vmware-vcops --full-restart
   ```

   These nodes might be remote collector nodes or the master node. You can also choose to restart the entire cluster.

The configured desktop applications are displayed on vRealize Operations for Horizon dashboards and reports.

Clean Up Objects

Some objects might continue to appear on the dashboards even after agents have stopped collecting data about them. You can set a time after which such objects will be cleaned up.

Procedure

1. Open the `/usr/lib/vmware-vcops/user/plugins/inbound/V4V_adapter3/conf/v4v.properties` file on the vRealize Operations Manager master node.
2. Modify the value of parameters whose cleanup time you want to change.

   The value is given in days. Enter a floating-point number for a period of time less than one day. For example, 0.5 is twelve hours and 0.0417 is one hour. An empty value indicates that the object is never cleaned up.

Parameter	Default Value	Description
timeToExpire.VirtualMachine	30	Virtual machines
timeToExpire.UserDesktop	30	VDI sessions
timeToExpire.RDSSession	30	RDS sessions
timeToExpire.AppSession	30	Application sessions
timeToExpire.RDSApplication	30	Hosted applications
timeToExpire.ViewNetwork	30	View network objects
timeToExpire.DesktopApplicationInstance	30	Desktop application instances
timeToExpire.User		Users
timeToExpire.ViewPool		VDI pools
timeToExpire.AppPool		Application pools
timeToExpire.RDSPool		RDS pools
timeToExpire.RDSFarm		RDS farms
timeToExpire.RDSServer		RDS servers

3. Log in to the vRealize Operations Manager user interface as an administrator.
4. In the menu, click the **Administration** tab and in the left pane click **Solutions**.
5. Select **VMware Horizon** in the upper pane and restart collection on each adapter displayed in the lower pane.

Objects will be cleaned up from the dashboards after one hour and from vRealize Operations Manager after two hours.

Uninstall vRealize Operations for Horizon

If you no longer want to use vRealize Operations for Horizon, you can uninstall the solution and broker agents.

Desktop agents that are installed as part of Horizon Agent cannot be independently uninstalled.

Procedure

1. Uninstall broker agents.
   1. Log in to the Horizon Connection Server host as a Horizon administrator.
   2. Select **Control Panel > Programs > Programs and Features**.
   3. Select **VMware vRealize Operations for Horizon Broker Agent** and click **Uninstall**.
2. Uninstall the vRealize Operations for Horizon solution.
   1. Log in to the vRealize Operations Manager user interface as an administrator.
   2. In the menu, click the **Administration** tab and in the left pane click **Solutions > Repository**.
   3. On the **VMware Horizon** solution, click **Uninstall**.
   4. Select **I understand the risk and agree.** and click **OK**.

RMI Communication in vRealize Operations for Horizon

3

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

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

This chapter includes the following topics:

- RMI Services
- RMI Security with Remote Collectors
- Change the Default RMI Service Ports

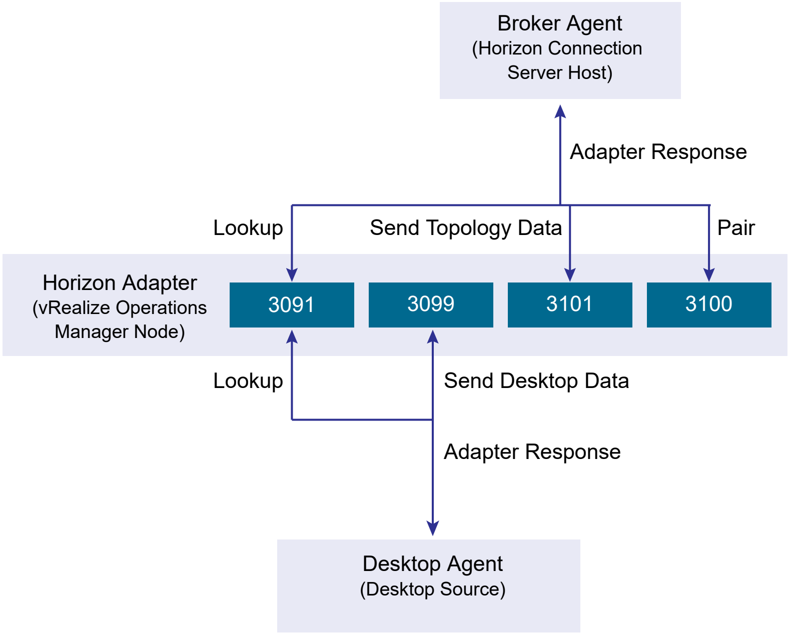
RMI Services

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

Table 3-1. RMI Services

Service	Description	Default Port
RMI registry service	The broker and desktop agents initially connect to the RMI registry service and request the address of a specific RMI server. Because the RMI registry service is used only for lookup and no sensitive data is transmitted to it, it does not use an encrypted channel.	3091
Desktop message server	The desktop agents connect to the desktop message server and use it to send desktop performance data to the Horizon Adapter. The desktop message server uses a TLS channel to encrypt the data that is sent from the desktop agents.	3099
Certificate management server	The broker agent connects to the certificate management server during the certificate pairing process. The certificate management server does not use an encrypted channel. Certificates are encrypted by using the server key during the certificate pairing process. For more information, see Certificate Pairing.	3100
Broker message server	The broker agents connect to the broker message server and use it to send Horizon inventory information to the Horizon Adapter. The broker message server uses a TLS channel to encrypt the data that is sent from the broker agent.	3101

Figure 3-1. Communication Through RMI Service Ports



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

RMI Security with Remote Collectors

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

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

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

Change the Default RMI Service Ports

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

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

Table 3-2. RMI Service Port Properties

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

Procedure

1 Open the `/usr/lib/vmware-vcops/user/plugins/inbound/V4V_adapter3/work/msgserver.properties` file on the node where the Horizon Adapter instance is running.

2 Modify the values of the properties corresponding to the RMI service ports that you want to change.

3 Open the `/opt/vmware/etc/vmware-vcops-firewall.conf` file and locate the following command:

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

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

5 Restart the firewall.

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

TLS Configuration in vRealize Operations for Horizon

4

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

This chapter includes the following topics:

TLS Configuration Properties

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

Each agent and server supports a certain set of protocol versions and ciphers. When an RMI connection is established between an agent and a server, the agent and server negotiate the protocol and cipher to use by selecting the strongest protocol and cipher that both ends support.

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

The properties that control TLS configuration are described in the following table.

Table 4-1. TLS Configuration Properties

Property	Description
`enforcesslprotocols`	Whether to enforce TLS 1.2.
`sslProtocols`	List of accepted TLS versions, separated by commas.
`sslCiphers`	List of accepted TLS ciphers, separated by commas.

If `enforcesslprotocols` is set to true, the values of `sslProtocols` and `sslCiphers` cannot be changed. These values are fixed as follows:

- `sslProtocols`: `TLSv1.2`
- `sslCiphers`: `TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_DSS_WITH_AES_128_GCM_SHA256`

If `enforcesslprotocols` is set to false, the default values of `sslProtocols` and `sslCiphers` are as follows:

- `sslProtocols`: `TLSv1,TLSv1.2`
- `sslCiphers`: `TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_128_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_DSS_WITH_AES_128_GCM_SHA256`

To change these values, see Change the Default TLS Configuration.

Change the Default TLS Configuration

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

Prerequisites

Determine the TLS cipher suites supported by the operating system on all target machines. Ensure that the Horizon Adapter instance and each agent have at least one cipher suite in common.

Procedure

1. Log in to the vRealize Operations Manager node where the Horizon Adapter instance is running and open the `/usr/lib/vmware-vcops/user/plugins/inbound/V4V_adapter3/work/msgserver.properties` file.
2. Set the value of the `enforcesslprotocols` property to `false`.
3. Set the value of the `sslProtocols` property to the desired versions of TLS.

   Separate multiple values with a comma (,). The following values are supported:

   - `TLSv1.2`
   - `TLSv1.1`
   - `TLSv1`
4. Set the value of the `sslCiphers` property to the desired TLS cipher suites.
5. Log in to the Horizon Connection Server host where the broker agent is running and open the `C:\ProgramData\VMware\vRealize Operations for Horizon\Broker Agent\conf\msgclient.properties` file.

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

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

8 Modify the value of the `enforcesslprotocols`, `sslProtocols`, and `sslCiphers` properties to match the Horizon Adapter.

Authentication in vRealize Operations for Horizon

5

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

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

This chapter includes the following topics:

Certificate Pairing

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

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

The certificate pairing process is as follows:

1 The broker agent encrypts its certificate with the server key configured for the adapter instance.

2 The broker agent opens a connection to the certificate management server, and the encrypted certificate is sent to the adapter instance.

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

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

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

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

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

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

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

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

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

Component Authentication

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

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

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

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

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

Certificate and Trust Store Files

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

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

Horizon Adapter

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

Table 5-1. Adapter Certificate Properties

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

Broker Agent

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

Table 5-2. Broker Agent Certificate Properties

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

Replacing the Default Certificates

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

Replace the Default Certificate for the Horizon Adapter

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

Prerequisites

Obtain the keystore passwords from the `msgserver.properties` file on the vRealize Operations Manager node where the adapter instance is running.

Procedure

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

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

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

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

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

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

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

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

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

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

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

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

7 Restart the Horizon Adapter service.

   ```
   service vmware-vcops restart
   ```

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

8 Pair broker agents with the adapter instance again.

   a Log in to the Horizon Connection Server host as a Horizon administrator.

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

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

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

Replace the Default Certificate for the Broker Agent

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

Prerequisites

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

Procedure

1. Log in to the Horizon Connection Server host where the broker agent is installed and open the `C:\ProgramData\VMware\vRealize Operations for Horizon\Broker Agent\conf` directory.
2. Run the `keytool` utility with the `-genkeypair` option to generate a new self-signed certificate for the broker agent.

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

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

   dn-of-org is the distinguished name of the organization to which the certificate is issued, for example, "OU=Management Platform, O=VMware\, Inc., C=US".
3. Run the `keytool` utility with the `-certreq` option to generate a certificate signing request.

   ```
   keytool -certreq -alias v4v-brokeragent -file cert-request-file -keystore v4v-brokeragent.jks
   ```
4. Upload the certificate signing request to a certificate authority and request a signed certificate.

   If the certificate authority requests a password for the certificate private key, use the password configured for the certificate store.
5. After the certificate authority returns a signed certificate, copy the certificate file to the `C:\ProgramData\VMware\vRealize Operations for Horizon\Broker Agent\conf` directory.
6. Run the `keytool` utility with the `-import` option to import the new certificate.

   ```
   keytool -import -alias v4v-brokeragent -file new-certificate-filename -keystore v4v-
   brokeragent.jks
   ```
7. Run the `keytool` utility with the `-import` option again to import the root certificate of the certificate authority.

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

8 Restart the broker agent service.

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

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

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

9 Pair the broker agent with the adapter instance again.

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

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

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

Reissue Horizon Desktop Authentication Tokens

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

TLS and Authentication-Related Log Messages

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

Table 5-3. Log Message Types

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

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

For more information, see Viewing Horizon Adapter Log Files and Modify the Logging Level for the Horizon Adapter.

Troubleshooting vRealize Operations for Horizon

6

You can follow troubleshooting procedures to view log files and resolve some problems that might occur after you install and configure vRealize Operations for Horizon.

This chapter includes the following topics:

Oracle Event Databases

You might encounter an error when connecting the vRealize Operations for Horizon broker agent to an Oracle event database.

Problem

During broker agent configuration, testing event database credentials fails with the following error:

```
Event DB username and password cannot be validated. System.Data.OracleClient requires Oracle client
software version 8.1.7 or greater. An Error has Occurred. Operation Validate DB Credentials has
Failed.
```

Cause

To use an Oracle event database, you must install a recent version of ODAC and the Oracle Instant Client on the host where the broker agent is installed.

Solution

1. Go to the 64-bit Oracle Data Access Components (ODAC) for Windows download page at https://www.oracle.com/database/technologies/odac-downloads.html and download the latest Xcopy for Windows x64 ODAC release.
2. Follow the procedure given in the `readme.html` file included in the installation package.

3 Go to the Instant Client for Microsoft Windows (x64) 64-bit download page at https://www.oracle.com/database/technologies/instant-client/winx64-64-downloads.htmland download the latest version of Oracle Instant Client.

   You can choose the Basic or Basic Light edition.

4 Unzip the Instant Client package to a directory and add the directory to the `PATH` environment variable.

   If you have multiple versions installed, ensure that the new version occurs first in the path.

Viewing Agent Log Files

You can access vRealize Operations for Horizon broker and desktop agent log files for troubleshooting.

- Broker agent log files are located in `C:\ProgramData\VMware\vRealize Operations for Horizon\Broker Agent\logs` on the Horizon Connection Server host where the agent is installed.
- Desktop agent log files are located in `C:\ProgramData\VMware\vRealize Operations for Horizon\Desktop Agent\logs` on the remote desktop being used.

You can also create a Data Collection Tool (DCT) bundle that contains log files from one or more remote desktops. For more information, see "Create a Data Collection Tool Bundle for Horizon Agent" in the *Horizon 7 Administration* document.

Viewing Horizon Adapter Log Files

You can access Horizon Adapter log files in vRealize Operations Manager to use for troubleshooting.

Procedure

1 Log in to the vRealize Operations Manager user interface as an administrator.

2 In the menu, click the **Administration** tab and in the left pane select **Support > Logs**.

3 In the **Group by** drop-down menu, select **Log Type**.

4 Double-click the **COLLECTOR** folder and then double-click the folder for the node on which the adapter instance is running.

5 Select a log file, enter desired values in the **Starting Line** and **Number of Lines** text boxes, and click **Go**.

The specified section of the log file is displayed in the right pane. You can click the **>** icon to select a minimum level of logs to display or to search for text within the log file.

Modify the Logging Level for the Horizon Adapter

You can modify the level of logs recorded on the collector node that contains a Horizon Adapter instance.

Procedure

1 Log in to the vRealize Operations Manager user interface as an administrator.

2 In the menu, click the **Administration** tab and in the left pane select **Support > Logs**.

3 Double-click the node on which the Horizon Adapter instance is running.

4 Select the **COLLECTOR** folder and click the **Edit Properties** icon.

5 If you have not previously modified the logging level for the Horizon Adapter, add a log class.

   a Click the **Add Log Class** icon.

   b Enter `V4V_adapter3` and click **OK**.

6 In the lower pane, locate **V4V_adapter3** in the **Log Name** column and set a logging level in the drop-down menu in the **Logging Level** column.

Modify the Logging Level for the Broker Agent

You can modify the level of logs recorded on the host that contains the vRealize Operations for Horizon broker agent.

Procedure

1 Log in to the Horizon Connection Server host as a Horizon administrator.

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

3 Click **Next** until the **Logging** page is displayed.

4 Set the level of logs to create and the policy for log rotation.

5 Click **Next** until the final page is displayed.

6 Review your settings and click **Finish**.

   The **Broker Agent Config Utility for Horizon** wizard closes, and the broker agent service is restarted.

Create a Support Bundle

If the Horizon Adapter does not operate as expected, you can create a vRealize Operations Manager support bundle that includes log and configuration files for analysis.

Procedure

1 Log in to the vRealize Operations Manager user interface as an administrator.

2 In the menu, click the **Administration** tab and in the left pane select **Support > Support Bundles**.

3 Click the **Create Support Bundle** icon.

4 Select the type of support bundle and the nodes to include and click **OK**.

5 After the status of the support bundle changes to **Succeeded**, select the support bundle and click the **Download Support Bundle** icon.

6 (Optional) View the files in the support bundle or send the support bundle to VMware for support.