Serviceability for VOS-Based Contact Center Applications

VOS-Based Contact Center Applications

This chapter describes serviceability for all Cisco Voice Operating System (VOS)-based Contact Center applications. VOS-based Contact Center applications include, for example, Live Data, Cisco Identity Service, Cisco Unified Intelligence Center and Cloud Connect.

Real Time Monitoring Tool

For Cisco Unified Intelligence Center, Live Data, and Cisco Identity Service (Cisco IdS), download the Real Time Monitoring Tool (RTMT) from the Cisco Unified Intelligence Center Administration page (**Tools > RTMT Plugin Download**).

Live Data and the Cisco IdS do not host the RTMT installer. For this reason, always connect to the Cisco Unified Intelligence Center Server and sign in to the Administration page to download the RTMT installer. You can, however, run the same RTMT client to connect to any of the Cisco Unified Intelligence Center, Live Data, or Cisco IdS servers (standalone or coresident).

RTMT runs as a client-side application. You can install RTMT on a Windows workstation or a Linux machine. RTMT is cluster-aware. RTMT provides critical service and performance monitoring (perfmon), trace/log collection and viewing, and Alert Management on the node for the IP address you request at launch. RTMT does not provide the status of all critical applications on all the nodes at the same time.

Use RTMT to:

- Monitor the health of the system by generating email alerts for objects whose values go above or below a threshold
- Collect and view traces
- View syslog messages

- Monitor performance counters

RTMT has extensive online help. Refer to it for information on alerts, schedule collection, performance monitoring, and collecting and downloading tracing and logging data.

Install and Launch RTMT

Procedure

Step 1 Log in to your Cisco Unified Intelligence Center Administration page through your browser.

Note The Live Data and the Cisco IdS servers do not provide the RTMT download link.

Note For Cloud Connect, download and install RTMT on a client computer. Use the following URL https://FQDN:8443/plugins/CcmServRtmtPlugin.exe. Where, FQDN is the Fully Qualified Domain Name of the Cloud Connect Primary or Secondary Node.

Step 2 Click **Tools > RTMT Plugin Download**.

Step 3 On the download page:

a) Select the **Windows** platform.
b) Click **Download**.
c) Locate the CuicServRtmtPlugin.exe file (where you downloaded it). Right-click the file, and choose **Properties**.
d) Click the **Compatibility** tab, and check the **Run this program in compatibility mode for** check box. From the drop-down list, choose applicable **Windows** version and click **OK**.
e) Run CuicServRtmtPlugin.exe, or save and then run it from the saved location.
f) Follow the prompts and click the buttons on the installation screens.

Step 4 To launch:

a) Click the **Cisco Unified Real-Time Monitoring Tool 11.5** desktop icon.
b) In the Host IP Address field, enter the IP address for the node you want to monitor.
c) Accept the default port (8443).
d) Check Secure Connection. You see an error if the Host IP Address is not found or there is no network connection.
e) Click **Yes** to accept the certificate.
f) Enter the User Name and Password for a superuser. (Only a superuser can install RTMT.)
g) If a message appears indicating that a time zone mismatch exists, click **No** to launch RTMT in your current time zone.
h) Click **OK** to accept the default configuration.

Note The performance counters are documented in the *Administration Console User Guide for Cisco Unified Intelligence Center.* The performance counters are not documented in the Online help.

RTMT Client Support Services

RTMT uses the following services/servlets:

- Cisco AMC service
- Cisco CallManager Serviceability RTMT
- Cisco RIS Data Collector
- Cisco Tomcat Stats Servlet
- Cisco Trace Collection Service
- Cisco Log Partition Monitoring Tool
- Cisco SOAP-Real_Time Service APIs
- Cisco-SOAP-Performance Monitoring APIs
- Cisco RTMT Reporter Servlet

The RTMT Interface

The following RTMT system monitoring objects are available in the left pane of the RTMT page:

- **System Summary**

  Displays information on Virtual Memory usage, CPU usage, Common Partition usage, and the alert history log.

- **Server**

  Server objects are:

  - **CPU and Memory** - Displays information on Virtual memory usage and CPU usage for the server.
  - **Process** - Displays information on the processes running on the server.
  - **Disk Usage** - Displays information on the disk usage on the server.
  - **Critical Services** - Displays the name of the critical service, the status (whether the service is up, down, activated, stopped by the administrator, starting, stopping, or in an unknown state), and the elapsed time during which the services have existed in a particular state for the server or for a particular server in a cluster (if applicable).

    The Cisco Unified Intelligence Center services are listed under the **Intelligence Center** tab. The Live Data and Cisco IdS services are listed, along with the System services, under the **System** tab.

- **Performance**

  Performance objects are:

  - **Performance** - Performance monitoring allows you to monitor performance counters related to the Unified Intelligence Center server. You can continuously monitor a set of preconfigured objects and receive notification in the form of an email message. You can associate counter threshold settings to alter notification. Up to six perfmon counters in one chart for performance comparisons can be displayed. Performance queries can be used to add a counter to monitor. You can also save and

restore settings, such as counters being monitored, threshold settings, and alert notifications, for customized troubleshooting tasks.

- **Performance Log Viewer** - Displays data for counters from perfmon CSV log files in a graphical format.

- **Tools**

  Tools objects are:

  - **Alert Central** - Displays the history and status of every alert in the system. Click the **Intelligence Center** tab to see Unified Intelligence Center alerts, including those related to Cisco IdS.
  - **Trace & Log Central** - Allows you to browse or download trace and log files for a specific date range or absolute time.
  - **Job Status** - Shows the status of trace collection events.
  - **Syslog Viewer** - Allows you to view (by node) the system, application, and security logs.
  - **VLT** - Not applicable.
  - **AuditLog Viewer** - Allows you to view system audit logs.

Download Trace and Log Files

Perform the following steps to download the trace and log files for Cisco Unified Intelligence Center, Live Data, Cisco IdS and Cloud Connect.

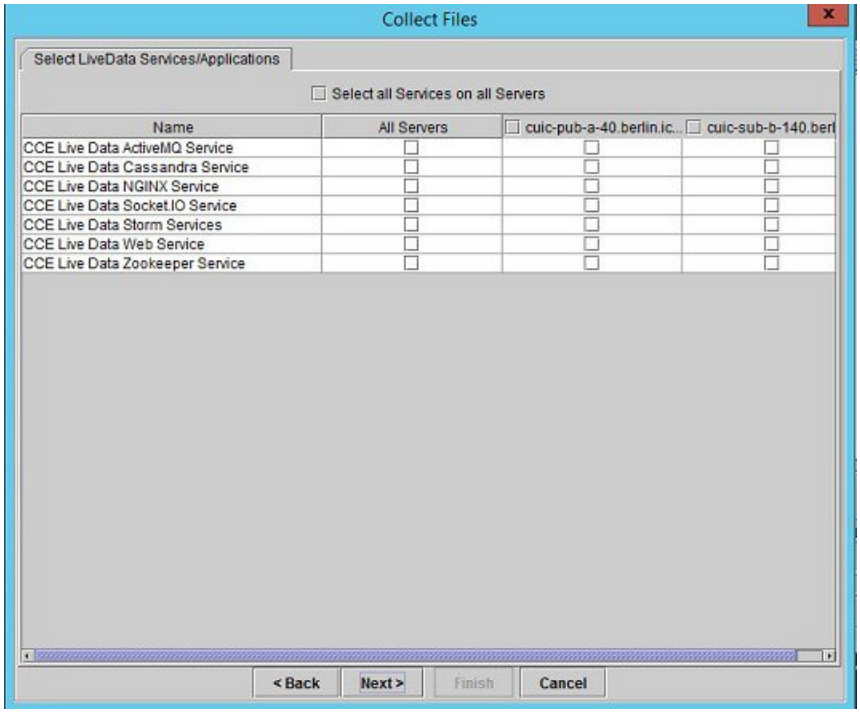
Procedure

Step 1 Run RTMT to connect to the target server, then choose **Tools** > **Trace & Log Central** in the **System** pane.

Step 2 Click **Collect Files**.

Step 3 Click **Next** to browse through and select services and applications for which you want to collect files. For example, you can select one or more Live Data services; the list is shown here.

Figure 1: Select LiveData Services/Applications



Step 4 When you finish selecting services and applications, you can choose either of the **Collection File Options**:

- **Absolute Range** - Choose the **Reference Server Time Zone** from the drop-down list. Then choose the **From Date/Time** and the **To Date/Time**.
- **Relative Range** - From the drop-down lists, choose the number of files generated and the time duration (**Minutes**, **Hours**, **Days**, **Weeks**, or **Months**).

Step 5 Choose the **Download File Options**:

a. Choose either the **Active Partition** or **Inactive Partition** from the drop-down list.

b. Browse to or provide the path to the **Download File Directory**.

c. Select the **Zip Files** or **Do Not Zip Files** option.

d. To remove the log files from the server, check the **Delete Collected Log Files from Server** check box.

Step 6 Click **Finish**.

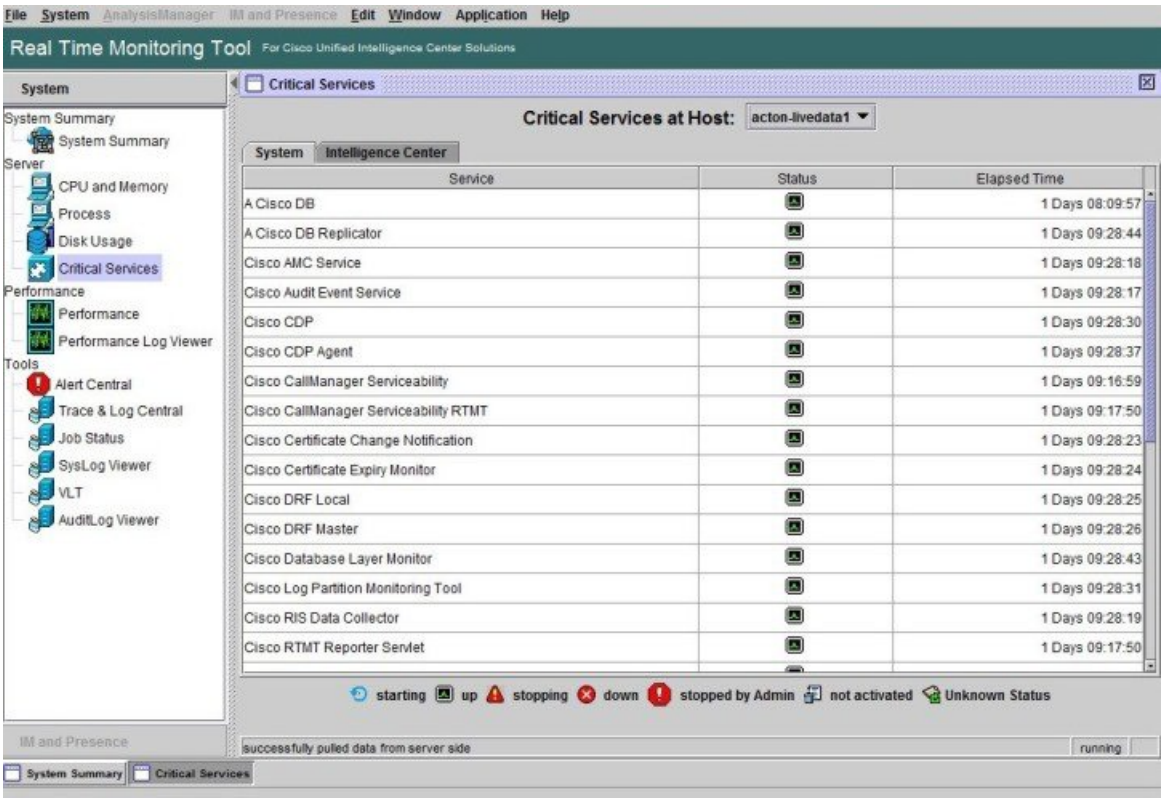
View the Status of Services

Procedure

Run RTMT to connect to the target server, then choose **Server** > **Critical Services** in the **System** pane.

You see a number of services on the **System** tab, as shown in the following example.

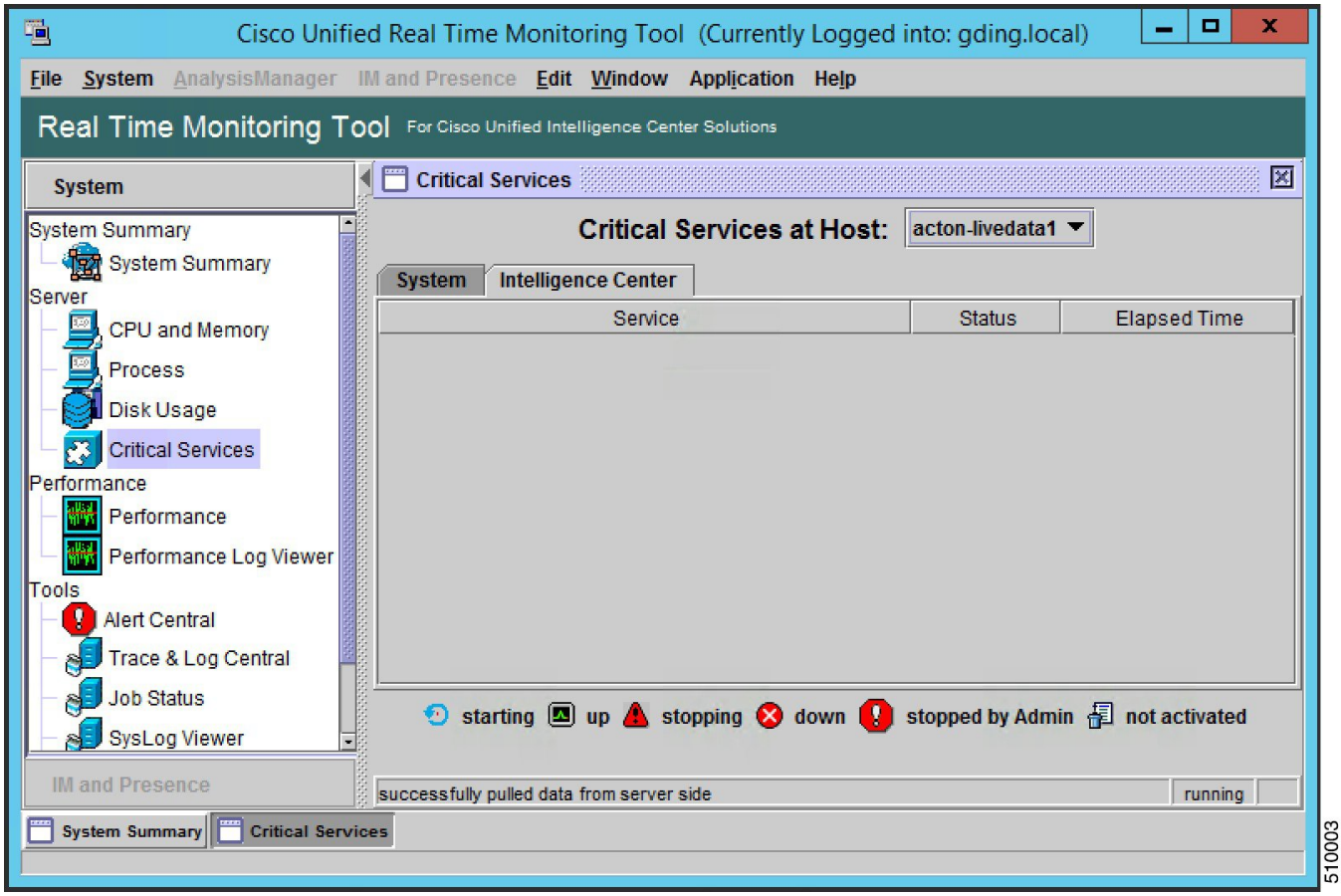
Figure 2: RTMT Critical Services System Tab



Live Data and Cisco IdS services are also included on the **System** tab. To view the Unified Intelligence Center services, click the **Intelligence Center** tab.

When RTMT is connected to either a Unified Intelligence Center standalone server or a Cisco IdS standalone server, no services are listed on the Intelligence Center tab, as shown in the following figure.

Figure 3: RTMT Critical Services Intelligence Center Tab (Unified Intelligence Center or Cisco IdS Standalone)



When RTMT is connected to standalone cloud connect server. **Cloud Connect** services will be included as part of the **System** tab.

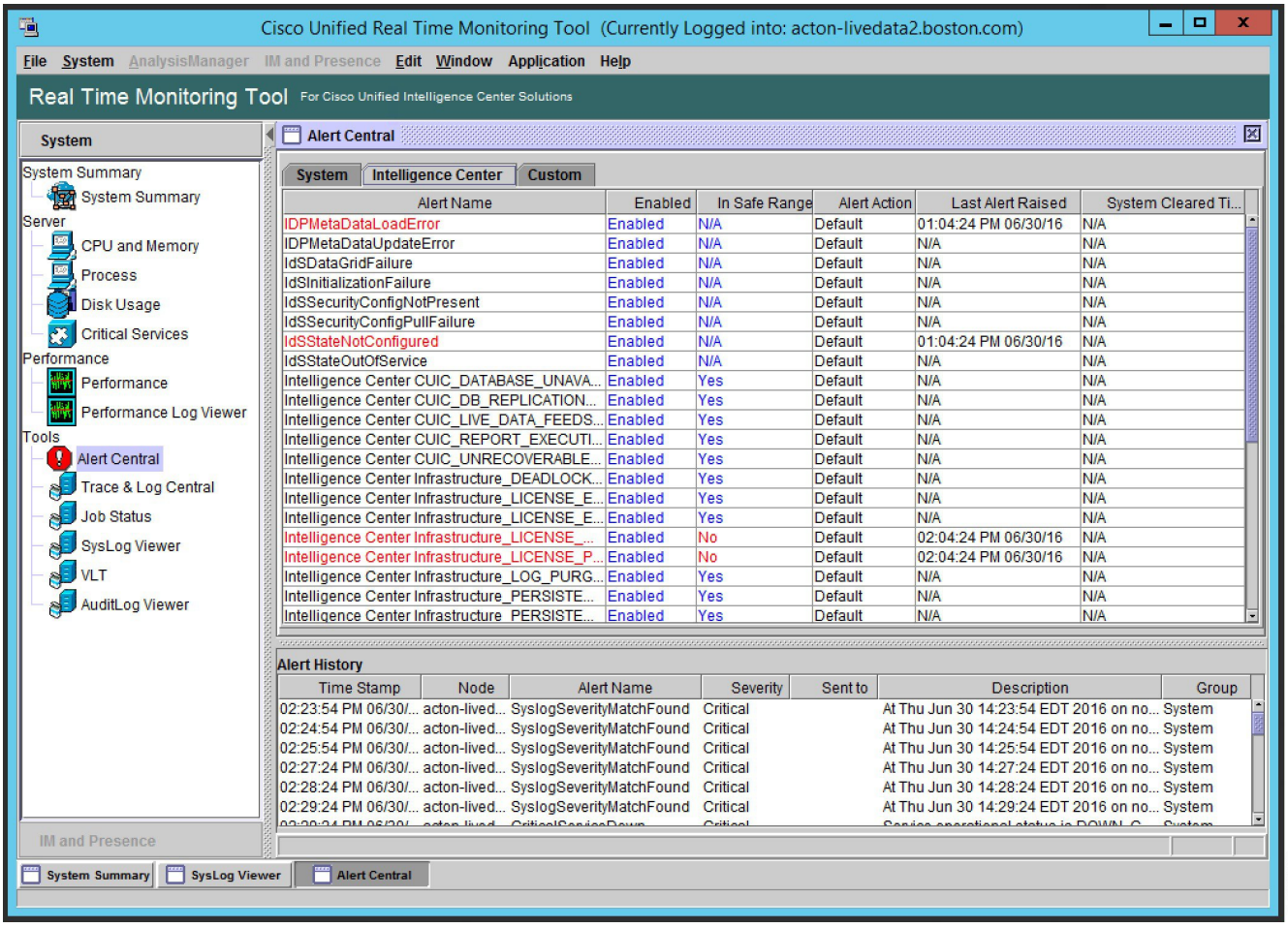
Alert Central

To view system and application-defined alerts, perform the following step.

Procedure

Run RTMT to connect to the target server, then choose **Tools** > **Alert Central** in the **System** pane.

Figure 4: RTMT Alerts



Cisco Identity Service Alerts

You can view the Cisco Identity Service alerts from the **Intelligence Center** pane.

The following table describes these alerts.

Table 1:

Alert Name	Syslog Alarm Name	Description
IdSInitializationFailure	IDS_INIT_ERROR	This alert occurs when an error is encountered during IdS initialization.
IDPMetaDataLoadError	IDP_META_DATA_LOAD_ERROR	This alert occurs when the trust could not be established between IdS and IdP during initialization.
SPMetaDataLoadError	SP_META_DATA_LOAD_ERROR	This alert occurs when SAML SP metadata Initialization fails.

IDPMetaDataUpdateError	IDP_META_DATA_UPDATE_ERROR	This alert occurs when there is an error updating IdP metadata and propagating across the cluster.
SPMetaDataUpdateError	SP_META_DATA_UPDATE_ERROR	This alert occurs when SAML SP certificate regeneration fails.
TokenMetaDataUpdateError	TOKEN_META_DATA_UPDATE_ERROR	This alert occurs when TOKEN Keystore regeneration or update fails.
IdSSecurityConfigNotPresent	IDS_SECURITY_CONFIG_NOT_PRESENT	This alert occurs when some IdS security configuration files are not present on the secondary node.
IdSSecurityConfigPullFailure	IDS_SECURITY_CONFIG_PULL_FAILURE	This alert occurs when the security config could not be pulled from the primary IdS node.
SAMLCertificateLoadFailed	SAML_CERTIFICATE_LOAD_FAILED	This alert occurs when the system is unable to read the SAML SP certificate.
IdSStateNotConfigured	STATE_NOT_CONFIGURED	This alert occurs when the trust between IdS node and IdP is yet to be established or when the IdS configuration could not be synchronized from the primary node.
IdSStateOutOfService	STATE_OUT_OF_SERVICE	This alert occurs whenever a system error results in the IdS Application failing to start.

Note To view or edit values for any alert, right-click the alert and select **Set Alert/Properties**.

Cloud Connect Syslog and Alert

Below are the set of syslog messages and alert which can be viewed from RTMT.

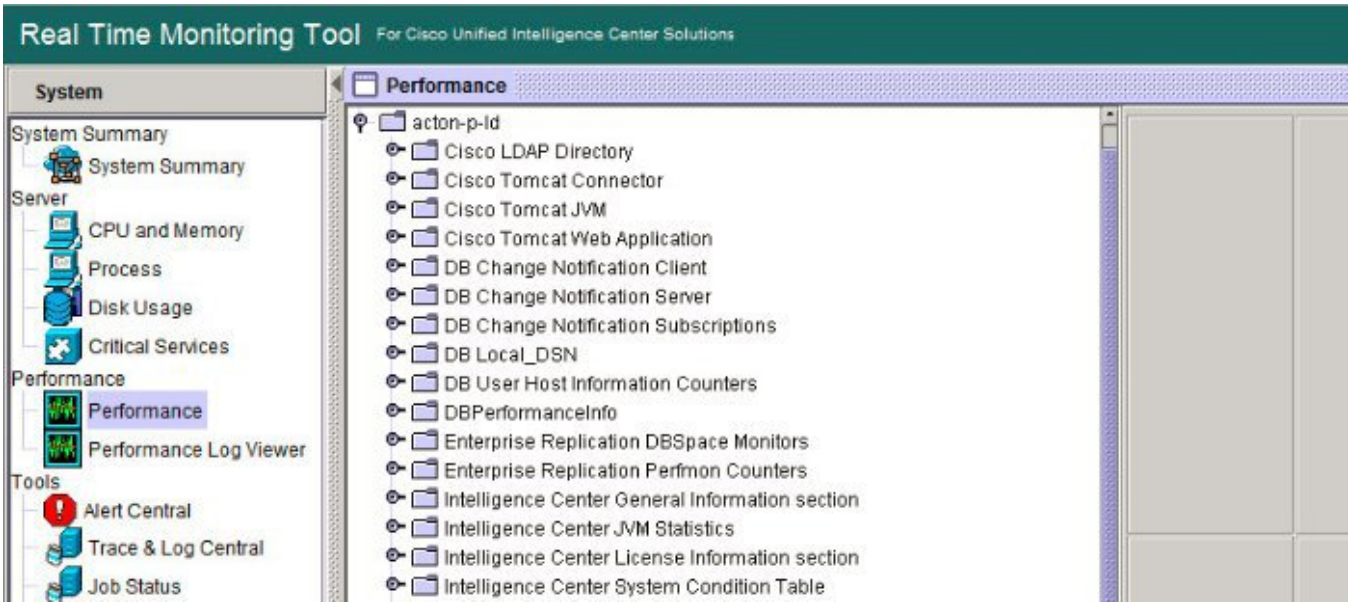
Syslog Alarm Name	Display Name in RTMT	Description
CONTM_INIT_FAILURE	ContainerManagerInitFailure	Container Manager initialisation failed
CONTM_INIT_HTTP_FAILURE	ContainerManagerInitProvisioningFailure	Container Manager HTTP Server initialisation failed
CONTM_INIT_PROVISIONING_FAILURE	ContainerManagerHTTPServerInitFailure	Container Manager fails to initialise the provisioning
SERVICE_FAILURE	CloudConnectServiceFailure	Cloud Connect Service encountered an error requiring manual intervention

View Performance Counters

Procedure

Run RTMT to connect to the target server, then choose **Performance** > **Performance** in the **System** pane.

Figure 5: RTMT Performance Interface



Disaster Recovery

The Disaster Recovery System includes the following capabilities:

- A user interface for performing backup and restore tasks.
- A distributed system architecture for performing backup functions.
- Scheduled backups or manual (user-invoked) backups.

To back up and restore a Unified Intelligence Center standalone or coresident (Unified Intelligence Center, Live Data, and Cisco IdS) server, see the *Administration Console User Guide for Cisco Unified Intelligence Center* at https://www.cisco.com/en/US/products/ps9755/prod_maintenance_guides_list.html. The procedures in the Disaster Recovery System chapter in this document also apply to the Live Data standalone, Cisco IdS standalone server and Cloud Connect.

Disaster recovery does not completely cover the Live Data application. After you complete a disaster recovery, reconfigure the Live Data application. To reconfigure Live Data, complete the tasks in the Live Data Installation procedure in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at https://www.cisco.com/en/US/products/sw/custcosw/ps1844/prod_installation_guides_list.html.