Introduction

What is SAS Environment Manager?

Components
SAS Environment Manager is a monitoring and management system for SAS deployments. It consists of the following components:
- a web-based administrative interface
- an agent on each managed host
- a central server to which the agents report
- a store of information about managed resources

Main Features
In addition to providing new operational functionality, SAS Environment Manager also supports selected aspects of traditional SAS administration. The following list highlights key features:
- auto-discovery of resources
- monitoring of remote systems
- personal and role-based dashboards
- role-based access to resources and functionality
- alerting for events and metrics that relate to system health
visualizations for server monitoring, memory, and processor usage
web-based management of integrated object model servers and web application servers

Beginning in SAS Environment Manager version 2.4, functions and capabilities that enable SAS Environment Manager to fit into a service-oriented architecture (SOA) have been added. Extract, transform, and load (ETL) processes obtain metric data, convert it to a standard format, and load it into the SAS Environment Manager Data Mart. You can view the data by using stored process reports and reporting tools or you can send it to other reporting tools.

Relationship to VMware Hyperic
In order to offer enterprise class operational features, SAS Environment Manager incorporates much of VMware's Hyperic technology.

See Additional Documentation for SAS Environment Manager on page 6.

Relationship to Other SAS Administrative Applications
SAS Environment Manager is not currently a replacement for other administrative applications, such as SAS Management Console and the SAS Web Administration Console.

Our eventual intent is to consolidate SAS administrative functionality within one unified interface, SAS Environment Manager. At this time, no functionality has been removed from the other SAS administrative applications.

Concepts in SAS Environment Manager

Dashboards and Portlets
When you sign in to SAS Environment Manager, the first page that is displayed is the Dashboard page.

Here are some key points:
- Each user has their own personal dashboard.
- Each user also has access to one additional dashboard for each of their native roles.
- Each dashboard has two columns of portlets.
- Each portlet displays a particular type of information.
- Each user’s portlets display only the content that that user is allowed to see.

Agents and Inventory
An agent is a software process that runs on and interacts with a particular host. Each managed physical and virtual machine has its own agent. Each agent performs the following functions:
- auto-discovers the software components that run on its host
- periodically re-scans its platform for configuration changes
- gathers performance and availability metrics
- sends the inventory and performance data that it collects to a central server
- performs log and event tracking
- enables you to perform resource control actions
An inventory is a database of information about resources that are known to SAS Environment Manager. You can monitor and manage only those resources that are in inventory. SAS Environment Manager stores its inventory information in a Postgres database.

The central server that receives inventory and metric data from agents and stores it in the inventory database is called the inventory server. The inventory server performs the following functions:

- provides facilities for managing your software inventory
- implements the inventory model
- implements its own access control model
- detects when alerts are triggered
- performs alert notifications or escalation processes as defined

Resources

Classification

A resource is a computing component or process that is known to SAS Environment Manager. Resources are classified as follows:

- Each resource has an inventory type (for example, platform).
- Each platform, server, and service also has a resource type (for example, Linux).

Inventory Types

The following inventory types comprise a hierarchy:

- platform
  - a machine and operating system or a virtual or network host
- server
  - a software component that runs on a platform
- service
  - a software component that runs on a platform or a server

The following inventory types facilitate grouping of resources for the purpose of simplifying administration:

- application
  - a user-defined collection of services that fulfill a single business purpose
- resource group
  - one of the three following types of collections of resources:
    - autogroup
      - an automatically defined collection of resources that are of the same type and that have the same parent resource. Each autogroup contains all of the resources that are of the same resource type within a particular platform or server.
      - Note: An autogroup is named for the type of resources that it contains. For example, an autogroup that contains the CPUs on a platform is called CPU.
    - compatible group
      - a user-defined collection of similar resources (for example, JBoss 4.x servers or Linux platforms).
    - mixed group
      - a user-defined collection of resources
Resource Types
A resource type identifies the software brand or vendor that a resource is associated with. Only the hierarchical inventory types (platforms, servers, and services) have a resource type.

For example, Win32 is a resource type for a platform and JBoss 4.0 is a resource type for a server.

Resource Control Actions
A resource control action is a command that an agent can perform on an individual resource (usually a server) or on a compatible group of resources.

For example, resource control actions for a server might include starting and stopping that server.

A quick control action is a resource control action that is run on-demand, rather than being scheduled.

Alerts
An alert is a set of rules that define how to detect a problem and how to respond if that problem occurs.

The following list introduces key concepts:

- alert action
  - an action that is performed when an alert is triggered (for example, a notification or a resource control action)

- alert condition
  - a rule that determines when an alert triggers

- alert escalation
  - a type of alert action that consists of a predefined sequence of notification steps that begin when an alert is triggered

- notification
  - a type of alert action in which messages are sent to designated parties

- resource alert
  - an alert for an individual resource

- resource group alert
  - an alert for a compatible group of resources (a group that you have defined that contains selected resources, all of which have the same resource type)

- resource type alert
  - an alert for all instances of a particular resource type

- triggered alert
  - an individual occurrence of a situation where the conditions of a particular alert definition are met

Introduction to the User Interface
The following table describes the main functional areas in the SAS Environment Manager interface.

<table>
<thead>
<tr>
<th>Main Page</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td>Configurable collections of portlets.</td>
</tr>
<tr>
<td>Resources</td>
<td>Resource-level monitoring and management.</td>
</tr>
<tr>
<td>Analyze</td>
<td>Deployment-wide views.</td>
</tr>
<tr>
<td>Administration</td>
<td>Metadata folders, basic properties of metadata objects, metadata authorization controls.</td>
</tr>
</tbody>
</table>
What’s New in SAS Environment Manager 2.4

Overview
SAS Environment Manager has the following new features and enhancements:

- SAS Environment Manager Service Management Architecture has been added
- services that enable you to import and export events have been added
- the ability to view and store a snapshot of detailed system information has been added
- a facility for managing user definitions in SAS metadata has been added

SAS Environment Manager Service Management Architecture
SAS Environment Manager Service Management Architecture provides functions and capabilities that enable SAS Environment Manager to fit into a service-oriented architecture (SOA). In operation, SAS Environment Manager Service Management Architecture uses extract, transform, and load (ETL) processes to obtain metric data, convert it to a standard format, and load it into the SAS Environment Manager Data Mart. You can then leverage the data by using the supplied stored process reports and reporting tools or by using your own preferred reporting tools. SAS Environment Manager Service Management Architecture includes components that are delivered within these packages:

SAS Environment Manager Extended Monitoring
- implements best practices for SAS Environment Manager by creating a predefined set of alerts, resource groups, and best-practice metric configurations. This component also provides the framework needed for SAS Environment Manager Service Management Architecture by configuring the infrastructure of the SAS Environment Manager Data Mart.

Audit, Performance, and Measurement (APM) ETL
- collects information from SAS logs, standardizes it, and stores it in the SAS Environment Manager Data Mart, where it is used to populate stored process reports.

Agent-Collected Metric (ACM) ETL
- uses information collected about the computing resources (such as servers and disk storage), standardizes it, and stores it in the SAS Environment Manager Data Mart. The information is then used to populate stored process reports.

Solution kit framework
- extends the capabilities of SAS Environment Manager to support specific solutions or applications by providing support both for collecting and storing operation information about the solution in the SAS Environment Manager Data Mart and for using the associated reporting capabilities.

SAS Visual Analytics data feed
- copies selected data tables from the SAS Environment Manager Data Mart to a specified drop zone directory. SAS Visual Analytics then automatically loads the tables from the drop zone into the application.

Importing and Exporting Events
SAS Environment Manager provides services that enable you to import and export event data. Event importing provides a specified location and format for external applications or SAS code to write events to. When data is written to the specified location, SAS Environment Manager creates an event, which can then be handled just like any other event in the application. Event exporting operates in a similar manner. Every time an event occurs
in SAS Environment Manager, the application creates an entry in a specified location, using a specified format. You can then configure third-party monitoring tools to monitor the location for new entries and handle the exported events.

Environment Snapshot

Environment Snapshot contains a comprehensive listing of the system information in the SAS Environment Manager database. Environment Snapshot provides you with valuable information about your system. Environment Snapshot collects and displays the most current performance measures and configuration parameters from the SAS Environment Manager database, and also executes and gathers real-time usage information.

In addition, you can take a snapshot of the information, which saves all of the data in a text file. This file provides an easy way to communicate the status and configuration of your system when you are working with SAS Technical Support.

Metadata for User Administration

To make access distinctions and to track user activity, security systems must know who is making each request. User administration primarily provides information that helps systems make this determination. The main piece of user information that the SAS environment requires is one external account ID for each user. The SAS environment uses its copy of this ID to establish a unique SAS identity for the connecting user. All of a user's group memberships, role memberships, and permission assignments are ultimately tied to their SAS identity.

To access user administration features in SAS Environment Manager, select the Users module on the Administration tab. Your roles and permissions determine which user administration tasks you can perform.

Additional Documentation for SAS Environment Manager

Primary Documentation

All primary documentation for SAS Environment Manager is available from support.sas.com/documentation/onlinedoc/sev/index.html.

SAS Administration Documentation

SAS Environment Manager documentation is supplemented by a set of administration guides that are available from support.sas.com/documentation/onlinedoc/intellplatform/index.html.

The administration guides provide comprehensive and current information for intelligence platform topics including installation and configuration, backup and restore, logging, security, data management, servers, and management of web applications.

VMware Hyperic Documentation

For implementation-level details and extensibility information about Hyperic technology, see the Hyperic documentation set at www.vmware.com/support/pubs/vfabric-hyperic.html.

CAUTION! Not all of the content in the Hyperic documentation set is relevant to or accurate for SAS Environment Manager.

The following list provides guidance to help you make appropriate use of the Hyperic documentation:

- Do not use Hyperic’s documentation about system configuration, system requirements, supported platforms, or installation. SAS packages and installs the Hyperic technology that is incorporated into SAS Environment Manager.
- Do not use Hyperic’s documentation about its user interface. The SAS Environment Manager online Help provides a customized version of that content.
Do not use Hyperic’s documentation about rebranding. Instead, see the SAS Environment Manager chapter in the SAS Intelligence Platform: Web Application Administration Guide.

Do not use Hyperic’s documentation about LDAP or Kerberos configuration. Authentication to SAS Environment Manager is through the SAS Logon Manager. See the SAS Intelligence Platform: Middle-Tier Administration Guide.

Do not use Hyperic’s documentation for releases other than Hyperic 5.0. SAS Environment Manager uses the 5.0 release of Hyperic.

---

## Dashboards and Portlets

### Dashboards and Portlets: Overview

**Available Portlets**

The following table lists the available portlets and provides links to additional information if applicable.

**Portlets**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-Discovery on page 9</td>
<td>Lists new and changed resources and enables you to add them to the inventory.</td>
</tr>
<tr>
<td>Availability Summary on page 10</td>
<td>Indicates the availability of selected resources, aggregated by resource type. This portlet refreshes every minute. This portlet is initially empty.</td>
</tr>
<tr>
<td>Control Actions on page 12</td>
<td>Lists recently performed actions on managed resources and upcoming scheduled actions. Also indicates which quick control actions are most frequently performed.</td>
</tr>
<tr>
<td>Favorite Resources on page 12</td>
<td>Lists selected resources. This portlet is initially empty.</td>
</tr>
<tr>
<td>Saved Charts on page 11</td>
<td>Displays selected charts as a slide show.</td>
</tr>
<tr>
<td>Recent Alerts on page 8</td>
<td>Lists the most recently triggered alerts for selected resources. This portlet refreshes every minute.</td>
</tr>
<tr>
<td>Recently Added on page 14</td>
<td>Lists platforms that have been recently added to inventory.</td>
</tr>
<tr>
<td>Search Resources</td>
<td>Enables you to search for resources. The search supports case-insensitive, partial-term queries for a specified inventory type.</td>
</tr>
<tr>
<td>Summary Counts on page 15</td>
<td>Displays a count of managed resources by inventory type. Only those resources that you are allowed to access are displayed.</td>
</tr>
<tr>
<td>Group Alerts Summary</td>
<td>Displays traffic light indicators for resource alerts and group alerts for selected groups. To view a list of alerts that have fired for a group, click that group’s traffic light. To view a group page, click that group’s name. This portlet is initially empty.</td>
</tr>
<tr>
<td>Metric Viewer on page 13</td>
<td>Displays selected metrics for selected resources. This portlet refreshes every minute. This portlet is initially empty.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Problem Resources on page 14</td>
<td>Lists all resources that have problem metrics and provides details including availability status, number of alerts per resource, number of times the metric has been out of bounds, and the most recent time that the out-of-bounds metric was collected.</td>
</tr>
</tbody>
</table>

**Customizations**

You can customize a dashboard as follows:

- To add a portlet to a column, scroll to the bottom of that column. Click the **Add content to this column** drop-down list, select a portlet, and click \( \text{Add portlet} \). The portlet is added at the bottom of the column.

- To remove a portlet, click \( \text{Remove portlet} \) in the portlet’s title bar. The removed portlet is available from the **Add content to this column** drop-down list (at the bottom of the column).

- To move a portlet up or down within a column, drag its title bar.

- To configure a portlet, click \( \text{Configure portlet} \) in the portlet’s title bar. Not all portlets are configurable.

**Multiple Dashboards**

In addition to your personal dashboard, you have access to a distinct dashboard for each of your native roles. See **Assign Roles to a User on page 52**.

To select a dashboard, click the **Select a Dashboard** drop-down list (above the top of the left column of portlets).

Initially, your default dashboard is your personal dashboard. If you want to use a different dashboard as your default, open that dashboard and click **Make Default**.

**TIP** The **Make Default** button is located to the right of the **Select a Dashboard** drop-down list. The button is displayed only for dashboards that are not currently your default dashboard.

**Recent Alerts Portlet**

**Contents**

The **Recent Alerts** portlet displays a list of recently triggered alerts.

For each alert, the following information is provided:

**Date/Time**  
when the alert was triggered

**Alert Name**  
the name of the alert definition

**Resource Name**  
the resource for which the alert was triggered

**Fixed**  
whether the alert has been marked as fixed

**Ack**  
whether the alert has been marked as acknowledged
To mark an alert as fixed or acknowledged, select its check box and then click the appropriate button. The **Fixed** and **Acknowledge** buttons are located at the end of the list of triggered alerts.

To view details about an alert or to document the resolution of an alert, click the link in the alert’s **Date/Time** column.

**Configuration**

To configure the **Recent Alerts** portlet:

1. Click 📋 at the right edge of the portlet’s title bar.

2. (Optional) On the **Dashboard Settings: Alerts** page, enter a description (the text that you enter here will be displayed at the top of the portlet).
   
   **Note:** Text that you enter here will be appended after the **Recent Alerts** label in the portlet’s title bar.

3. Set **Alert Range** criteria as follows:
   - the maximum number of alerts to include
   - the minimum level of alert priority to include
   - the maximum age of an alert to include
   - whether you want to alert for all resources or for only selected resources

   If you select **selected resources** from the last drop-down list in the **Display Settings** section, you must also select the resources of interest in the **Selected Resources** section.
     
   - At the bottom of the **Selected Resources** list, click **Add to List**.
   - On the **Dashboard Settings: Alerts Add/Remove Resources** page, use the check boxes and arrows to move items to the **Add Resources** list. You must select an item’s check box before you use an arrow to move it.
   
   - Click **OK**.

   **Note:** Only those triggered alerts that meet all specified criteria will be displayed in the portlet.

4. On the **Dashboard Settings: Alerts** page, click **OK**.

**Auto-Discovery Portlet**

**Contents**

The **Auto-Discovery** portlet lists recently added or modified platforms and servers. By default, a maximum of five entries are listed.

The listing criteria is as follows:

- A platform is listed if it (or a server that runs on it) is new or changed.
- A platform is new if neither its IP address nor its fully qualified domain name (FQDN) matches that of a platform that is already in the inventory.
- A platform is changed if an inventory property for it (or for a server that runs on it) has changed.
- Each new or changed server is listed below its platform.

**TIP** To view details, click a resource name.

The following table explains the values that can be displayed in the **Changes** column:
### Values in the Changes Column

<table>
<thead>
<tr>
<th>Value</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>server set changed</td>
<td>Indicates that changes to one or more servers on the platform were detected. The changed servers are listed below the platform.</td>
</tr>
<tr>
<td>name change</td>
<td>Indicates that the name of the resource has changed. A resource name can change when a resource is upgraded from one version to another (if the version number is part of the resource name).</td>
</tr>
<tr>
<td>install path changed</td>
<td>Indicates that the installation path for a server has changed. The installation path for a resource can change when a resource is upgraded from one version to another (if the version number is part of the path).</td>
</tr>
<tr>
<td>IP set changed</td>
<td>Indicates that the IP address has changed. When a discovery agent detects an IP address that is not associated with an existing platform in inventory, the agent checks for a platform with a matching FQDN. If such a platform is found, the platform is recognized as existing.</td>
</tr>
<tr>
<td>FQDN changed</td>
<td>Indicates that the fully qualified domain name has changed.</td>
</tr>
</tbody>
</table>

**Note:** The Auto-Discovery portlet does not include services. Services are discovered during run-time scans and are automatically added to inventory.

### Configuration

To set the maximum number of completed auto-discoversies that are displayed:

1. Click at the right edge of the portlet’s title bar.
2. On the Dashboard Settings: Auto-Discovery page, make a selection from the Auto-Discovery Range drop-down list.
3. Click OK.

### Add Discovered Resources to Inventory

To add new or updated resource information to inventory, click a resource name in the Auto-Discovery portlet and use the Auto-Discovery Results page. See Process Auto-Discovery Results on page 28.

### Availability Summary Portlet

**Contents**

The Availability Summary portlet indicates whether selected resources are running.

**Configuration**

To configure the Availability Summary portlet:

1. Click at the right edge of the portlet’s title bar.
2. (Optional) On the Dashboard Settings: Availability Summary page, in the Description field, enter a title for the portlet.
Note: Text that you enter here will be appended to the Availability Summary label in the portlet's title bar.

3 In the Display Range drop-down list, set the maximum number of resource types to list in the portlet.

4 Use the Selected Resources section to designate resources to include in the portlet.
   a At the bottom of the Selected Resources list, click Add to List.
   b On the Dashboard Settings: Availability Summary Add/Remove Resources page, use the check boxes and arrows to move items to the Add Resources list.

   **TIP** You must select an item's check box before you use an arrow to move it.
   c Click OK.

5 On the Dashboard Settings: Availability Summary page, click OK.

### Saved Charts Portlet

**Contents**
The Saved Charts portlet enables you to display charts in a dashboard and supports the following interactions:

- To open a full page view of a chart, click its title link (which is located immediately above the chart within the portlet).
- To remove a chart from the portlet, click Remove Chart and then click OK to confirm the removal.

If you add multiple charts to the same dashboard, the charts are displayed within a single Saved Charts portlet, as a slide show. The following interactions are supported:

- To explicitly display a chart, select it in the list to the left of the currently displayed chart.
- To pause or restart the slide show, click the icon in the lower left corner of the portlet.
- To locate a chart that has already been added to the portlet, you can enter text in the Live Search field. This is useful if you have a lot of charts in the portlet.

**Configuration**
To configure the Saved Charts portlet:

1 Click at the right edge of the portlet’s title bar.

2 The portlet contents are replaced with its configuration settings. Make adjustments as follows:
   - To disable the slide show, clear the Chart Rotation check box.
   - To change the speed of the slide show, use the Rotation Interval drop-down list.
   - To change the time range of the displayed data, use the Time Range drop-down list.

3 Click Save.

**Add a Chart**
To add a chart to the portlet:

1 From the Resources page, navigate to and open the chart that you want to add.
2 Click the **Save Chart to Dashboards** link.

**TIP** The link is one of several links that appear within the chart, near the top. The link is displayed only when you have fully drilled into a chart. For example, the charts on a resource’s **Monitor** page do not have these links. However, if you click the title of one of those charts, it opens in its own page and the **Save Chart to Dashboards** link is displayed.

3 In the **Save Chart to Dashboards** window, select the check box of the dashboard to which you want to add the chart. Click **Add**.

4 On the **Dashboard** page, verify that the chart is displayed as expected.

**TIP** If the chart is not displayed, make sure that the correct dashboard is selected in the **Select a Dashboard** drop-down list (at the top of the **Dashboard** page).

---

### Control Actions Portlet

#### Contents

The **Control Actions** portlet displays historical information about resource control actions as follows:

- The upper section, **Recent Control Actions**, lists resource control actions that occurred within a specified time period.
- The lower section, **Quick Control Frequency**, identifies the resources upon which the greatest number of on-demand actions have been performed (during the specified interval).

#### Configuration

To configure the **Control Actions** portlet:

1 Click at the right edge of the portlet’s title bar.

2 On the **Dashboard Settings: Control Actions** page, adjust settings as follows:

   - To list recent control actions, select the **Control Action Range** check box. Specify the maximum number of completed control actions to list and the eligible time period.
   - To list the resources for which the largest number of on-demand control actions have occurred, select the second check box. Specify the maximum number of resources to list.

3 Click **OK**.

### Favorite Resources Portlet

#### Contents

The **Favorite Resources** portlet lists the resource name, resource type, current availability, and number of triggered alerts for selected resources.

#### Configuration

To configure the **Favorite Resources** portlet:
1. Click at the right edge of the portlet’s title bar.

2. On the Dashboard Settings: Favorite Resources Settings page, at the bottom of the Selected Resources list, click Add to List.

3. Use the check boxes and arrows to move items between the Resources and the Add Resources lists.

   **TIP** You must select an item’s check box before you use an arrow to move it.

4. Click OK.

5. On the Dashboard Settings: Favorite Resources Settings page, click OK.

**Add a Favorite**

When you view a resource on the Resources page, you can add it to the Favorite Resources portlet as follows:

1. Select Tools Menu ➔ Add to Dashboard Favorites

2. In the Add to Dashboard Favorites window, select the check box for the dashboard to which you want to add the current resource as a favorite. Click Add.

3. On the Dashboard page, verify that the resource is listed in the Favorite Resources portlet.

   **TIP** If the resource is not listed, make sure that the dashboard to which you added the resource is selected in the Select a Dashboard drop-down list (at the top of the Dashboard page).

**Metric Viewer Portlet**

**Contents**

The Metric Viewer portlet displays a selected metric for resources of a particular resource type.

   **TIP** To include multiple metrics in a dashboard, add multiple instance of the Metric Viewer portlet to that dashboard. See Customizations on page 8.

**Configuration**

To configure the Metric Viewer portlet:

1. Click at the right edge of the portlet’s title bar.

2. (Optional) On the Dashboard Settings: Metric Viewer page, enter a description.
   **Note:** Text that you enter here is appended to the Metric Viewer label in the portlet’s title bar.

3. Set inclusion criteria and sort order
   **Note:** The Display Range field sets a maximum number of resources to display in the portlet.

4. At the bottom of the Selected Resources section, click Add to List.
5 On the Dashboard Settings: Metric Viewer Add/Remove Resources page, use the check boxes and arrows to move resources between the Resources list and the Add Resources list.

   **TIP** You must select a resource’s check box before you use an arrow to move it.

   **TIP** To filter by resource name, enter a substring in the Filter by Name field.

6 Click OK.

7 On the Dashboard Settings: Metric Viewer page, click OK.

### Problem Resources Portlet

**Contents**

The Problem Resources portlet lists resources that have recently triggered alerts or had out-of-bounds metrics.

**Note:** Out-of-bounds metrics are metrics that have values that are outside a specified baseline range.

   **TIP** To configure tracking of out-of-bounds metrics, select the Manage page and click the Server Settings link. On the Edit Server Settings page, scroll to the Automatic Baseline Configuration Properties section.

The listed resources are ordered first by inventory type and then chronologically (by when the problem occurred).

**Configuration**

To configure the Problem Resources portlet:

1 Click at the right edge of the portlet’s title bar.

2 On the Dashboard Settings: Problem Resources Settings page, you can limit the resources that are displayed in the portlet as follows:
   - In the Show Maximum of drop-down list, select a maximum number of problem resources to include.
   - In the For the Last drop-down list, specify how many hours worth of problems to include.

3 Click OK.

### Recently Added Portlet

**Contents**

The Recently Added portlet lists platforms that have recently been added to inventory and indicates how long ago they were added.

**Configuration**

To configure the Recently Added portlet:

1 Click at the right edge of the portlet’s title bar.
2 On the Dashboard Settings: Recently Added page, select a maximum number of platforms from the Show Maximum of: drop-down list.

3 Click OK.

**Summary Counts Portlet**

**Contents**

By default, the Summary Counts portlet indicates how many resources there are for each inventory type. For example, the Summary Counts portlet might indicate that there are 3 platforms, 23 servers, and 786 services.

You can configure this portlet to also display counts by resource type. For example, the portlet might indicate that of the 23 servers, only one is a metadata server.

Links in this portlet provide access to resource lists and shortcuts for creating new resources.

**Configuration**

To configure the Summary Counts portlet:

1 Click ☐ at the right edge of the portlet’s title bar.

2 On the Dashboard Settings: Summary Counts page, select and clear check boxes to indicate which inventory types and resource types you want to see resource counts for.

3 Click OK.

---

**Resource Monitoring**

**Resource Navigation**

Use the Resources page to monitor, configure, and manage inventory resources.

Here are some tips for understanding the availability states in the Availability column:

- ![Resource is configured and fully available.](image)
- ![Resource is configured, but availability is less than 100%.](image)
- ![Resource has not been configured.](image)
- ![Resource is unavailable.](image)

Here are some tips for locating resources on the Resources page:

- Only one inventory type is displayed at a time. To access resources of a different inventory type, click one of the links in the table header (Platforms, Servers, Services, Compatible Groups/Clusters, Mixed Groups, or Applications).

- To further limit the display, specify criteria in the Search row and then click ☐ (at the end of the Search row). Not all criteria are supported for all inventory types.
To include only resources that are owned by the user that you are logged on as, select the **Owned by** check box.

There might be multiple pages of resources in the list. Use the controls below the list to navigate.

To return to a page that you recently viewed, use any of the following methods:

- Select **Resources ➔ Recently Viewed ➔ the page name**
- Click your web browser’s **Back** button.
- Click a link at the top of the page.

A lock icon indicates that a particular feature is not available for a particular resource, due to your permissions.

To view a list of resources that are not currently available, select **Resources ➔ Currently Down**. See **Unavailable Resources on page 22**.

**TIP** As an alternative to browsing and filtering on the **Resources** page, you can use the search field (at the right edge of the application banner) to quickly locate a resource by its name.

Here are some additional details about interacting with a list of resources on the **Resources** page:

- To view detailed information about a resource, click its name. See **Resource Detail Pages on page 23**.
- In each row, icons to the right of the check box (واق) provide shortcuts to particular resource detail pages (the **Monitor** page, the **Inventory** page, and the **Alerts** page).
- A lock icon indicates that a particular feature is not available for a particular resource, due to your permissions.
- To switch between the list view and the chart view, click **Show Chart View** or **Show List View** (on the right edge of the page).
- You can initiate resource management tasks from the **Resources** page. See **Resource Management: Overview on page 22**.

**Selecting Metrics**

On a resource’s **Monitor** page, settings on the left determine which charts and data are displayed on the right. Use the check boxes and options on the left to set criteria as follows:

- Specify which related resources you are interested in. For example, on a server’s **Monitor** page, you can select its parent platform and any of its child services. After you select or clear check boxes, click **View Metrics** to update the display.
- On the **Monitor ➔ Indicators** page, specify whether you are interested in all metrics or only problem metrics. Then add charts by clicking the right arrow icons. Or, open a chart in a separate window by placing your mouse pointer over a bubble icon and then clicking **View Full Chart**.
On the Monitor ⇨ Metric Data page, specify which metric categories and value types to display.

**Note:** On the Monitor ⇨ Metric Data page, you can use the **Keyword Search** field to locate a metric by its name. For example, if you search for the word *offset* on a server’s Monitor ⇨ Metric Data page, only the **Server Offset** metric is displayed.

### Indicator Charts

#### Availability and Events Bars

An availability bar is displayed at the top of a chart. It contains dots that correspond to time slices (intervals).

The duration of time that a time slice represents is determined by the **Metric Display Range** (at the top of the Monitor page). Here are some examples:

- If the display range is 8 hours, each time slice represents 8 minutes.
- If the display range is 4 hours, each time slice represents 4 minutes.

The color of a dot indicates the availability of the resource during that time period as follows:

- Green indicates 100% availability.
- Orange indicates availability greater than 0% and less than 100%.
- Red indicates 0% availability.

**TIP** To see the start time of a time slice, click its availability dot. The vertical bar helps you examine the state of each metric during the time slice.

**Note:** If a time slice is longer than the collection interval for the metric, the displayed availability is based on the multiple data points that are collected during the time slice.

To the right of the availability bar, the average availability over the current range is displayed.

An events bar is displayed at the bottom of a chart. In an events bar, a purple circular icon over a time slice indicates a logged event. To view an event’s details, click its icon.

### Interpretation

Here are some tips for interpreting the charts:

- The values that are labeled **LOW**, **AVG**, and **PEAK** are the lowest, average, and highest values that were collected during the metric display range.
- The area of each vertical bar indicates high and low values.
- The cross in each bar indicates average value.
- The charts are stacked vertically so that their X-axis (time) values align. This helps you correlate activity.

### Adjust or Save the Display

You can interact with the display as follows:

- To move a chart up or down in the display order, click its up or down arrow (↑ ↓).
- To remove a chart from display, click its ✗ icon.
To save a set of displayed charts, select Create New View from the View drop-down list, enter a name, and click.

To delete the current view, select Delete view from the View drop-down list.

**Metric Data**

**Introduction**
To view tabular data for a resource, select its Monitor ➔ Metric Data page. See Selecting Metrics on page 16.

The Metric Data page displays a summary of the measurements that were collected during the currently selected metric display range.

You can adjust the display as follows:

- To display all of the metrics that are supported for the resource, click next to Show All Metrics at the top of the Metric Data page.
- To display metric data for a single resource in a separate window, click at the end of that resource’s row.
- To change the frequency with which the page refreshes, click a link in the Metrics Refresh field (on the upper right edge of the table of data).

**Metric Baselines**

You can use the Change Value controls (at the bottom of the Metric Data page) to reset the baseline, acceptable high, and acceptable low values for a metric.

**Metric Collection Settings**

**Introduction**

The default metric collection settings for a resource are specified on the Manage ➔ Monitoring Defaults page for the associated resource type. You can alter the metric collection interval for a particular resource on its Metric Data page. However, subsequent updates to the monitoring defaults for the resource type overwrite any modifications to collection intervals made for a particular resource.

Changes that you make to metric collection settings for a group of resources affect all members of that group.

**Disable Collection**

To disable collection of selected metrics:

1. Clear the check boxes for the metrics that you want to disable.
2. Click Disable Collection (at the bottom of the page).

**Note:** If the currently selected resource is a compatible group, collection of the metric is disabled for all resources in the group.

**Enable Collection**

To enable collection of metrics:

1. Click the arrow that is located to the right of the Show All Metrics link (at the top of the page).
2. Select the check boxes for the metrics that you want to enable.

3. Click **Enable Collection** (at the bottom of the page).

**Note:** If the currently selected resource is a compatible group, collection of the metric is enabled for all resources in the group.

**Set the Collection Interval**

To change the collection interval for selected metrics:

1. If the **Metric Data** page currently display all metrics for the resource, click **Hide Metrics Without Data**.

2. Select the check boxes for the metrics whose collection interval you want to modify.

   **TIP** Select multiple metrics only if you want to set the same collection interval for all of them.

3. To specify the frequency of metric collection:
   a. Enter an integer value in the **Collection Interval for Selected** field.
   b. Select **Minutes** or **Hours** from the drop-down list.
   c. Click the arrow that is to the right of the **Minutes/Hours** drop-down list.

**Metric Reference**

For each enabled metric for one or more members of a compatible group, the following information is displayed:

- **Alerts**
  - number of times that the metric value triggered an alert

- **OOB**
  - number of times that the metric was out-of-bounds

- **LOW**
  - lowest value that was collected

- **AVG**
  - average of values that were collected

- **PEAK**
  - highest value that was collected

- **LAST**
  - the last value that was collected

- **Collection Interval**
  - the frequency of metric collection (**NONE** indicates that data is not being collected)

For resources that are of the same type within an autogroup or a compatible group, the following information is displayed:

- **Number Coll**
  - number of data points that were collected across all of the group members for which the metric is enabled

- **Alerts**
  - number of times that a collected metric triggered an alert

- **OOB**
  - number of times that the metric was out-of-bounds, across all group members
LOW
lowest value that was collected, across all group members

AVG
average of values that were collected, across all group members

PEAK
highest value that was collected, across all group members

SUM
sum of all values that were collected (not for a metric whose unit is percentage)

Frequency of metric collection
NONE
indicates that data is not being collected

VARIES
indicates that the collection interval varies among members of the group

Member health data
for compatible groups, the lower portion of the Metric Data page lists each member resource, indicates its availability, and provides access to its Alerts page.

Full Page Charts

View a Full Page Chart
To view a full page chart, click one of the charts on the Monitor ⇒ Indicators page.

You can interact with a full page chart as follows:

- Select or clear check boxes in the chart legend, and click Redraw. The following list documents the options:
  - **Actual**
    - the observed metric value at any point in time
  - **Peak**
    - the highest observed metric value (a horizontal line)
  - **Average**
    - the average of observed metric values across the entire graph (a horizontal line)
  - **Low**
    - the lowest observed metric value (a horizontal line)
  - **Low Range**
    - the user-specific lowest acceptable metric value (a horizontal line)
  - **High Range**
    - the user-specific highest acceptable metric value (a horizontal line)
  - **Baseline**
    - the application-level or user-defined baseline value (a horizontal line)
  - **Control Actions**
    - indicates when control actions where performed on the resource (this helps you correlate actions with performance)

- Use the controls at the bottom right of the Metric Chart section to adjust the display range. Click Redraw.

- Change the baseline or acceptable range of values for the charted metric. This action is available only when a single metric is charted.
  - In Metric Baseline & Expected Range, click Change Value.
  - Adjust the settings and click Save Value.
Here are some additional details:

- The Y-axis represents the metric value and the X-axis represents time. Each column represents a 1/60 time slice of the selected metric display range. A chart can plot a maximum of 60 points.
- The chart displays the average, peak, and low observed values for the metric for the slice of time along the X-axis.
- The chart also displays the established baseline, high range (highest acceptable), and low range (lowest acceptable) values, if that information is available.
- Each column displays the observed metric value for that slice of time. For dynamic metrics, this can be an average. If the plotted point is an average, the range of metric values collected in that slice of time is displayed (as an I bar).
- For dynamic metrics, a point on the chart represents the average of the metric values that were observed over the period of time that ended at the specific time (X-axis value). For example, for a display range of eight hours, each charted point represents the average of the preceding eight-minute period (8 hours / 60 time slices along the X-axis = 8 minutes). If the metric is collected every 60 seconds, and the chart's display range is 60 minutes, each of the 60 plotted points on the graph represents the single, observed value for the metric at a single point in time.
- The values for data that is cumulative (trending up or down) such as bytes served, uptime, minimum response time, number of transactions are not averaged. A point charted for this type of data shows the maximum (or minimum) value for the time slice.

**Save or Export a Chart**

To save the current chart to a dashboard, click **Save Chart to My Dashboard**. See **Saved Charts Portlet** on page 11.

Note: If you have permission to edit multiple dashboards, the link is **Save Chart to Dashboards** instead of **Save Chart to My Dashboard**.

To save the current chart in CSV format, click **Export to CSV**.

**Metric Time Frame**

The metric display range specifies the time range for the metric data. For each user, one universal display range value is stored. When you change the display range, it affects the data that is displayed in the monitoring pages and in the charts.

The range can be defined as a specific time period (**Within a Date Range** option) or as a relative time period preceding the current time (**Last** option).

To change how the range is defined, click **Advanced Settings** on any **Monitor ⇒ Indicators** page.

**Comparing Metrics**

**Instructions**

To to compare resources:

1. On the **Resources** page, select a group of compatible resources.
2. On the compatible group's **Monitor ⇒ Metric Data** page, in the **Current Health of group's resources collecting metrics** section, select the check boxes of the resources that you want to compare.
3. Click **Compare Members of Selected**. The **Compare Metrics** page is displayed.
Interpretation

The Compare Metrics page lists the metrics that are collected for a set of resources. The page is organized by metric category, metric, and resource.

Note: If a metric was not collected for a particular resource during the current metric display range, that resource is not included in the section for that metric.

For each resource, the following data is provided:

**LOW**
the lowest observed metric value

**AVG**
the average of the observed metric values

**PEAK**
the highest observed metric value

**LAST**
the last observed metric value

**TIP** This page does not automatically refresh. To refresh the display, click the Get Current Values control (at the bottom of the page).

For a metric whose value type is Trends Up (for example, the metric Bytes Served metric), hyphens are displayed for the low, average, and peak values and a cumulative value is shown in the LAST column.

Unavailable Resources

To view a list of resources that are in inventory but not currently available, select Resources ➪ Currently Down.

Here are some tips to help you use this page:

- To list all currently unavailable resources of a particular inventory type, click a root node in the Resource Types pane. You can expand an inventory type link and select a resource type.
- To open a resource’s Indicators page, click its name in the Currently Down Resources list.
- The Down Since column indicates when the resource became unavailable.
- The Down Time column indicates how long the resource has been unavailable.
- To see a list of triggered alerts for a resource, click the icon in its Alerts column.
- To refresh the display, click at the top right.

Resource Management

Resource Management: Overview

**Purpose**

The purpose of resource management is to create and maintain the information infrastructure that is necessary to support operational monitoring and control actions.
Activities

Resource management involves the following activities:

- Adding platforms, servers, applications, and services to inventory.
- Creating logical groups of resources to simplify administration and facilitate comparisons.
- Configuring data collection settings for servers, resource groups, and individual resources.

Resource Detail Pages

The following table describes the monitoring and management features that are available within the Resources page. Each column in the following table represents a page within the Resources page. Not all pages are applicable for all types of resources.

Resource Detail Pages

<table>
<thead>
<tr>
<th>Page Contents</th>
<th>Monitor Page</th>
<th>Inventory Page</th>
<th>Alert Page</th>
<th>Control Page</th>
<th>Views Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indicator charts and metric data for the resource and any child resources.</td>
<td>General properties, child resources, resource group assignments, configuration properties, and monitoring levels.</td>
<td>Triggered alerts and configuration of additional resource-level alerts.</td>
<td>Status of in-progress actions, execution of on-demand actions, scheduling of actions, and history of completed actions.</td>
<td>For a platform, provides access to the Live Exec view (for running system commands).</td>
<td></td>
</tr>
</tbody>
</table>

Tips

- Use the check boxes on the left to select child resources of interest.
- Use the drop-down list to specify whether you are interested in all metrics or only problem metrics.
- To view a particular metric, click its arrow icon.

- To enable buttons such as Delete or Remove from List, select the check boxes of the resources that you want to affect.
- Within the Alert page, an Alerts page lists any triggered alerts. To enable the Fixed button, select a check box. The Acknowledge button is applicable to only alerts that have escalations.
- The Configure page lists alert definitions that affect the resource. To add a resource-specific alert, click New.
- Not all resources have defined views.

Resource Maps

For a graphical view of the servers on a platform, click Map on the platform’s Resource page. The platform is displayed at the bottom of the map and servers are displayed above the platform. Resource names are in bold and the resource type is displayed below, in smaller type. You can click a resource name to navigate to it.

To view a server’s child services and parent platform, click Map at the top of the server’s Resource page. You can click the name of a child or parent resource to open its Monitor page.
The map for a service displays a graphical view of the service and the resources that are related to it. The map illustrates the hierarchical inventory relationships and the service’s membership in groups or applications. The map for a compatible group shows the members of the group. There is no map for a mixed group.

**Add a Platform**

*Note:* Operating system platform types are auto-discovered and cannot be manually added to inventory.

To manually add a platform to inventory:

1. From the **Tools** menu, on the **Resources** page, select **New Platform**.
2. On the **New Platform** page, supply a name, platform type, IP address, and fully qualified domain name.
3. Click **OK**.

**Add a Server**

**Introduction**

Most servers are auto-discovered, rather than manually added to inventory. You might need to create a server manually under circumstances such as the following:

- The plug-in that manages the server does not support auto-discovery of server instances.
- The auto-discovery method that is used by the plug-in failed, because the entry that it looked for in the process table or Windows registry was not found. For example, the server's name in the process list is different from the name that the plug-in uses to detect server instances.

**Instructions**

To manually add a server to inventory:

1. On the parent platform’s **Resources** page, select **Tools ⇒ New Server**.
2. On the **New Server** page, enter a name, select a server type, and specify an install path.
   
   **Note:** If there are other servers of the same type on the current platform, make sure that the installation path that you define for the new server instance is unique. For auto-discovered servers, the plug-in sets the value of the **Install Path** property and uses it as the basis for the resource's auto-inventory identifier.

   **TIP** When you create a server manually, you must specify an **Install Path** property, but it does not have to be the actual installation path for the server. The only requirement is that all servers that are of the same resource type and on the same platform have unique **Install Path** property values.

3. Click **OK**.

On the **Inventory** tab for a new server, no services are displayed until any required configuration properties are defined.

**Add a Service**

**Instructions**

To add a platform service to inventory:
1 On the parent platform’s **Resources** page, select **Tools** ⇒ **New Platform Service**.
2 On the **New Service** page, enter a name and select a service type. See Reference: Platform Service Types on page 25.
3 Click **OK**.
4 On the new service’s **Inventory** page, click **Configuration Properties**.
5 On the **Configuration Properties** page, enter values for the required configuration properties (which are indicated by a red asterisk). See Reference: Platform Service Types on page 25.

**Reference: Platform Service Types**

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td></td>
</tr>
<tr>
<td>DHCP</td>
<td>Use to monitor a remote Dynamic Host Configuration Protocol server.</td>
</tr>
<tr>
<td>DNS</td>
<td>Use to monitor a remote Domain Name System server.</td>
</tr>
<tr>
<td>FileServer Directory</td>
<td></td>
</tr>
<tr>
<td>FileServer File</td>
<td></td>
</tr>
<tr>
<td>FileServer Mount</td>
<td>Use to monitor a remote filesystem mount point and associated disks and raid arrays. InetAddress Ping Use to ping a remote host for availability.</td>
</tr>
<tr>
<td>FileServer DirectoryTree</td>
<td>Use to monitor a directory and the entire tree under that directory.</td>
</tr>
<tr>
<td>HTTP</td>
<td>Use to monitor a particular URL.</td>
</tr>
<tr>
<td>FTP</td>
<td>Use to monitor a remote File Transfer Protocol server.</td>
</tr>
<tr>
<td>IMAP</td>
<td>Use to monitor a remote Internet Message Access Protocol server.</td>
</tr>
<tr>
<td>InetAddress Ping</td>
<td>Use to ping a remote host for availability.</td>
</tr>
<tr>
<td>LDAP</td>
<td>Use to monitor a remote Lightweight Directory Access Server.</td>
</tr>
<tr>
<td>Multiprocess</td>
<td>Use to monitor multiple related processes. For example, to monitor the number of https processes running on Apache and the system resource that they consume in aggregate.</td>
</tr>
<tr>
<td>NetworkServer Interface</td>
<td>Use to monitor a network interface.</td>
</tr>
<tr>
<td>NTP</td>
<td>Use to monitor a remote Network Time Protocol server.</td>
</tr>
</tbody>
</table>
### Service Description

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>POP3</td>
<td>Use to monitor a remote Post Office Protocol 3 server. Configure along with an SMTP service to monitor incoming and outgoing e-mail services.</td>
</tr>
</tbody>
</table>
| Process     | Use to monitor a process using a SIGAR Process Table Query Language (PTQL) query. To configure, you supply the PTQL query in the form:     

Class.Attribute.operator=value

For example:

Pid.PidFile.eq=/var/run/sshd.pid

<table>
<thead>
<tr>
<th>RPC</th>
<th>Use to monitor a Remote Procedure Call service.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Note:</strong> Not available on Windows platforms.</td>
</tr>
<tr>
<td>Script</td>
<td>Used to configure SAS Environment Manager to periodically run a script that collects a system or application metric.</td>
</tr>
<tr>
<td>SMTP</td>
<td>Use to monitor a remote Simple Mail Transfer Protocol server. Configure along with a POP3 service to monitor incoming and outgoing e-mail services.</td>
</tr>
<tr>
<td>SNMP</td>
<td>Use to monitor a remote Simple Network Management Protocol agent.</td>
</tr>
<tr>
<td>SSH</td>
<td>Use to monitor a remote SSH service.</td>
</tr>
<tr>
<td>TCP Socket</td>
<td>Use to monitor the availability of a remote TCP socket</td>
</tr>
<tr>
<td>Windows Service</td>
<td>Use to monitor an application that runs as a service under Windows. To configure it, you supply its Service Name in Windows.</td>
</tr>
</tbody>
</table>

### Add an Application

To add an application:

1. Select the Resources page.
3. On the New Application page, enter a name.
4. Click OK.
5. On the new application’s Resources page, in the Services section, click Add to List to assign services to the application. See Assign Services to an Application on page 27.

### Add a Resource Group

To add a resource group:

1. Select the Resources page.
3. On the New Group page, enter a name.
4 (Optional) If you want to make the group private, check the **Make group private** check box.

**Note:** A private group is invisible to other users, including administrators. You can share a private group with other users by associating it with a role. The name that you assign to a private group is automatically prefixed with the string **private to user name**, where user name is the user ID of the group’s creator.

5 In the **Contains Resources** setting, specify the type of group that you are creating and the resource types to include.

6 Click **OK**.

**TIP** When the **Browse** page lists platforms, servers, or services, you can select one or more resource instances and add them to a new or an existing group. Select the check boxes of the resources that you want to add and click **Group**.

**TIP** When the **Browse** page lists groups, you can select one or more resource instances and add them to a new group.

To create a new group that has other groups within it:

1 Click **Mixed** or **Compatible /Cluster**.

2 Select the check boxes of the groups that the new group will contain. Click **Group**.

3 On the **New Group** page, provide required information.

**Note:** To add groups to an existing group, navigate to the parent group and click **Add to List**.

### Assign Services to an Application

To assign services to an application:

1 On the application’s **Inventory** page, in the **Services** section, click **Add To List**.

2 Use the check boxes and arrows to move groups to the **Add Services** list.

3 Click **OK**.

### Assign a Resource Group to Roles

To assign a resource group to roles:

1 On the resource group’s **Inventory** page, in the **Roles Assigned To** section, click **Add To List**.

2 Use the check boxes and arrows to move groups to the **Add To Roles** list.

3 Click **OK**.

### Assign a Resource to Resource Groups

To assign a resource to resource groups:

1 On the resource’s **Inventory** page,

2 In the **Groups containing this resource** section, click **Add To List**.
On the Add to Groups page, use the check boxes and arrows to move groups to the Add to Groups list.

Click OK.

Process Auto-Discovery Results

Introduction
When you click a platform name in the Auto-Discovery portlet on the Dashboard page, the Auto-Discovery Results page is displayed.

The Auto-Discovery Results page displays the results of the most recent platform scan. You can filter the page to display only new or changed resources.

Note: In the current version, the Import Values/Do Not Import option in the Platform Type section has no effect.

Import or Skip Resources
To process the contents of the Auto-Discovery Results page:

1 Examine the new and changed properties.
2 From the Modified Properties drop-down list, select Import Values.
3 If you want to exclude selected changes from the import, change the selection in the per-cell drop-down list in the Action column.
   Note: If you choose not to import a new platform into inventory, its servers are also excluded. Excluded resources will be displayed in the portlet again (when they are discovered by another scan).
4 At the bottom of the page, click OK.

TIP In general, monitoring of a discovered resource begins when you add that resource to inventory. However, for a few resource types, additional configuration is required before monitoring can begin. To identify configuration requirements, examine the Configuration Properties section on a resource's Inventory page.

Change Resource Ownership
By default, the owner of a resource is the account under which the resource was added to inventory. A resource’s owner can be changed by its current owner or by a super user.

To assign a different owner to a resource:

1 At the top of the resource’s Inventory page, next to the Owner field, click the Change link.
2 Make changes on the General Properties page.
3 Click OK.

Delete Resources
To delete a resource from inventory, locate it in a resources list, select its check box, and click Delete.

Here are some important points about deleting resources:
A deleted resource is permanently removed from inventory. It can no longer be monitored or controlled from SAS Environment Manager.

Resource deletion is asynchronous. There might be a slight delay before resources are removed from inventory. If you restart an agent before the resource is removed, and you re-add the resource to memory after the agent rediscovers it, errors might occur.

Do not attempt to re-import a platform immediately after you delete it. This might fail.

**Note:** Until the delete process that is running in background completes, a deleted platform remains on the Health page's Agent tab.

If you delete a platform, its services and servers are also deleted.

If you delete all of the platforms that a particular agent manages, the saved authentication token for that agent is also deleted. The agent can no longer connect to the inventory server. To enable the agent to rediscover its platform, you must repeat the agent setup process. Otherwise, shut down the agent and uninstall it from that platform.

### Operate Agents

#### Introduction

Agent operations can be performed on an individual agent or on a group of agents.

#### Restart

To restart an agent:

1. On the agent's Views page, click **Agent Commands**.
2. Select the restart command.
3. Click **Execute**.

This command invokes the agent's Java Service Wrapper's restart command. The command shuts down the JVM process in which the agent runs, waits for the process to terminate cleanly, and spawns a new JVM process for the agent.

During the restart process, the agent's metric collection and resource control functionality is interrupted.

The restart command happens asynchronously. To verify that a restart is successful, navigate to the agent and check its availability.

#### Ping

To ping an agent:

1. On the agent's Views page, click **Agent Commands**.
2. Select the **ping** command.
3. Click **Execute**.

This command invokes the agent's Java Service Wrapper's ping command on the agent.

The result of the ping attempt is displayed in the **Result** pane on the right side of the page.
Upgrade
To upgrade an agent:
1 On the agent’s Views page, click Agent Commands.
2 Select the upgrade command.
3 Select a bundle from the agent bundle drop-down list.
4 Click Execute.
   The following results occur:
   - The selected agent bundle is transferred from the server to the target agent (or agents).
   - The agent expands the bundle locally.
   - The agent updates the local bundle property.
   - The server restarts the agent.
   - The configuration settings that are in the agent.properties file are preserved.

Push a Plug-in
To transfer new, custom, updated, or patched plug-ins from the server's plug-ins directory to the target agents' plug-ins directory:
1 On the agent’s Views page, click Agent Commands.
2 Select the push plug-in command.
3 Select a plug-in from the plug-in drop-down list.
4 Click Execute.
   Note: Pushing a plug-in to an agent causes that agent to restart.

Scan a Platform
To scan a platform:
1 Open the Resources page for the platform that you want to scan.
   Note: Only a platform that runs an agent can be scanned.
2 Select Tools ⇒ New Auto-Discovery.
3 To run a default scan, click OK at the top of the page.
4 To run a file scan and a default scan:
   a Select check boxes to indicate which Server Types to look for.
   b In Directories to scan, specify directories to scan.
   c In Directories to exclude from scan, specify directories to skip.
   d From the Filesystem types to scan drop-down list, select the type of file system to scan.
   e In the How deep field, specify the depth of the scan.
To follow symbolic links when scanning, select the **Should symlinks be followed?** check box.

Click **OK**.

**Clone a Platform**

**Introduction**
You can copy the configuration properties for servers and manually created platform services from one platform to another.

**Note:** Manually created platform services are services that cannot be auto-discovered. In general, these are proxy metrics for network services and devices (for example, HTTP, POP3, or DNS services).

Platform cloning is supported between platforms of the same resource type (for example, **Linux**) that run the same version of an agent.

Use platform cloning to replicate configuration properties for resources of the same type.

**What Cloning Does**
The cloning process creates new resources on the target platform or updates existing resource configuration properties as follows:

- It copies the configuration properties for each server on the source platform to corresponding servers of the same type on the target platforms. If there is not a corresponding server of the same type on a target platform, it is created, with the same configuration properties as the source server.

- It copies the configuration properties for each manually created platform service on the source platform to the target platforms. This adds new platform services to the target platform's inventory and updates the configuration properties of corresponding instances in the target platform inventory.

**What Cloning Does Not Do**
Here are some limitations of the cloning process:

- It does not update auto-discovered properties.
- It does not create or update platform services that are auto-discovered.
- It does not create or update services that comprise the cloned servers. The child services are added to inventory through auto-discovery.

**Instructions**
To clone a platform:

1. Open the **Resources** page for the platform that you want to clone.
2. Select **Tools ➤ Clone Platform**.
3. In the **Clone Platform** window, the **Available clone targets** list displays platforms that are of the same type as the source platform.

   **TIP** You can narrow the list by entering a string in the **Search resources** box.

4. Move the target platforms from the **Available clone targets** list to the **Selected clone targets** list.
Click Queue for Cloning.

Note: Cloning occurs asynchronously. You do not have to wait for the cloning process to complete before you perform other tasks in SAS Environment Manager. The Event Center indicates the start and stop of the cloning process for the source platform.

Define Platform Dependencies

Introduction

The Network and Host Dependency Manager is available from the Plug-ins section of the Manage page. It enables you to define relationships between a top level platform (a network device or virtual host) and lower level platforms (operating systems) that depend on it.

To extend the benefits of SAS Environment Manager hierarchical alerting to top level platforms, define dependency relationships.

Instructions

To define or change the dependent platforms for a top-level platform, you first select the top level platform. You can peruse a complete or filtered list of top-level platforms in inventory to find the one that you want to update.

TIP If the top-level platform that you want to update already has a dependent platform, you can instead begin from there. Select the By Dependent Platform tab to list all operating system platforms that have a top-level platform defined. Click the top-level platform name to select it.

To add dependencies:

1. Click Add.
2. In the Available Platforms window, select one or more operating systems.
   
   Note: The Available Platforms window identifies operating system platforms that are in inventory but not currently assigned to a top-level platform.
3. Click Add Dependency. The dependency is immediately added.
4. When you are finished updating dependencies for the top-level platform, click Done.

To remove dependencies, use the Select and Remove controls on the page.

Alerts and Events

Alerts: Overview

Use alerts to automate and manage problem detection and response processes.

The alerts system includes the following features:

- Trigger and report an alert when a specified condition (or set of conditions) occurs.
- Notify designated personnel or stakeholders when an alert is triggered.
- Run designated resource control operations when an alert is triggered.
- Track the resolution status of problems that are revealed by alerts.
Analyze alert and alert action history.

Establish an escalation process for an alert. An alert that has an associated escalation process has an acknowledged status that indicates whether designated responsible or interested parties are aware of the problem.

Manage Triggered Alerts

Introduction

The default view when you click a resource’s Alert page is a list of the alerts that triggered on the current day for the resource.

You can use the navigation controls on the page to list all alerts for the resource that are still in the database. By default, alerts are removed from the database after 31 days. The retention period is configurable on the Manage ⇒ Server Settings page.

The following information is shown for each alert.

Alert List for a Resource

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>the priority that is assigned to the alert definition</td>
</tr>
<tr>
<td>Alert Date</td>
<td>the date and time that the alert was triggered</td>
</tr>
<tr>
<td>Alert Definition</td>
<td>the name of the alert. Click to view the alert definition.</td>
</tr>
<tr>
<td>Alert Condition</td>
<td>the alert condition that was triggered</td>
</tr>
<tr>
<td>Actual Value</td>
<td>the reported metric value triggered the condition (if the alert condition is a metric comparison)</td>
</tr>
<tr>
<td>Fixed</td>
<td>whether the alert has been marked as fixed</td>
</tr>
<tr>
<td>Ack</td>
<td>an icon in this column indicates that the alert has an escalation assigned and has not yet been acknowledged</td>
</tr>
</tbody>
</table>

Select a Different Day

You can use the arrows or calendar to display alerts for a different date.

Mark Alerts as Fixed

**TIP** Marking an alert as fixed is a record-keeping activity. Marking an alert as fixed does not fix the underlying situation that triggered the alert.

To mark alerts as fixed:

1. Select the appropriate check boxes and click **Fixed**.
2. In the Alerts window:
   a. (Optional) Enter a comment in the **Resolution for Fix for Selected Alerts** area.
Click Fixed.

Note: If there are multiple unfixed alerts with the same alert definition, you can select Fix all previous.

**Acknowledge an Escalated Alert**

Alerts that have unacknowledged escalations have an icon in the Ack column. If you click the icon to acknowledge the alert, you cannot supply a comment or exercise an escalation pause option, (if one is defined). If you want to comment on or exercise a pause option, acknowledge the alert from a different page. Select the alert’s check box and click Acknowledge (at the bottom of the page).

See Alert Escalations on page 43.

**Alert Definitions for a Resource**

To view a list of alert definitions that apply to a resource, click **Configure** in the resource’s Alerts page. The list includes resource type alert definitions alerts that are defined at the resource type level.

Here are some tips for working with alert definitions from an individual resource’s alerts list:

- To add an alert definition, click **New**. The definition will apply to only the current resource.
- Do not enable, disable, edit, or delete an alert definition that has an asterisk (*). The asterisk indicates that the definition is assigned at the resource type level. It is not assigned directly to the current individual resource.

**TIP** To work with alert definitions for a resource type, click **Monitoring Defaults** on the Manage page. Then click **Edit Alerts** in the row for the resource type.

**Add an Alert for a Resource**

To create a new alert definition for an individual resource:

1. On the resource’s **Alert** page, click **Configure**.
2. At the bottom of the list of alerts, click **New**.
3. On the **New Alert Definition** page, define properties and conditions for the alert. See Alert Properties on page 35 and Alert Conditions on page 36.
4. Click OK to save your changes.
5. (Optional) Define actions for the server to perform when an alert is triggered. See Alert Actions on page 38.

**Alert Definitions for a Resource Type**

To view a list of alert definitions that apply to a particular resource type, click **Monitoring Defaults** on the Manage page. Then click **Edit Alerts** in the row for the resource type.

When you work with alert definitions at the resource type level, all instances of resources of the current resource type are affected by your changes.

**Add an Alert for a Resource Type**

To create a new alert definition for a resource type:
1 On the Manage page, in the Server Settings section, click Monitoring Defaults.

2 On the Monitoring Defaults page, click the Edit Alerts link in the row for the resource type for which you want to define an alert.

3 On the Monitoring Defaults page, at the bottom of the list of alert definitions, click New.

4 On the Alert Detail page, define properties. See Alert Properties on page 35.

5 Define conditions for the alert. See Alert Conditions on page 36.

6 Define actions for the alert. See Alert Actions on page 38.

Enable or Disable Alerts
To enable or disable all alerts for specified resources on the Resources page, select check boxes and click Enable All Alerts or Disable All Alerts.

Alert Properties
An alert definition has the following properties:

Name
a name for the alert. A triggered alert is identified by this name and a timestamp.

TIP An alert definition name should clearly communicate the nature of the problem. For example, you might assign the name Down for an alert on availability, or the name Low Memory for an alert on free memory.

Description
a description of the alert.

Priority
the severity of the problem that the alert is for (as defined by the person creating the alert). A triggered alert's priority is displayed in alert status and alert notification pages.

TIP Establish a consistent policy for setting the priority. This makes it easier to triage problems appropriately.

Active
whether the alert is currently enabled or disabled. Alerts are triggered for only enabled alerts.

Alert Notifications
To specify who is notified when an alert is triggered:

1 If the alert is not already open, navigate to it and open it.

TIP To open an alert for an individual resource, click Configure on that resource’s Alert page.

TIP To open an alert for a resource type, click Monitoring Defaults on the Manage page. See Add an Alert for a Resource Type on page 34.
2 At the bottom of the Alert Definition page, click Notify Roles. Then click Add to List. Use the check boxes and arrows to move roles to the Add Role Notification list. Click OK.

Note: To notify selected users, click Notify Users. To send notifications to people that are not registered users of SAS Environment Manager, click Notify Other Recipients and enter a comma-separated list of e-mail addresses.

Alert Conditions

Introduction

An alert condition specifies a resource metric value or event that triggers an alert. Different types of conditions are supported for different resource types.

To define a condition, choose a condition type and supply the required parameter values.

For example, a metric condition is based on the value of a metric that is collected for the resource. To define a metric condition:

1 On the Alert Definition page, in the Condition Set section, in the If Condition field, select the Metric radio button and select a metric from the drop-down list.

Note: To use a metric that is not currently listed, you must first enable collection of that metric. Update the metric collection settings for the resource type (choose Monitoring Defaults from the Manage page) or for the specific resource (click Metrics on the resource’s Monitor page).

2 Define the rule for evaluating the metric value as follows:

- To compare the metric value to an absolute value, select the first radio button. Select an operator and enter a value.

  Note: If the metric value is a percentage, specify it as a float value. For example, enter .99 for 99% and enter 1.0 for 100%. Use a period (.) as a decimal separator, not a comma (,).

- To compare the metric value to a minimum, baseline, or maximum value, select the second radio button. Select an operator, specify a value, and choose Min Value, Baseline Value or Max Value.

  Note: In order to use this approach, base lining must be enabled.

- To trigger the alert when the metric value changes, select the third radio button (value changes).

The following list provides information about other types of conditions.

Control Action condition

a condition that is triggered when a particular control action is performed, or when a particular control action causes a particular result status

Events/Logs condition

a condition that is triggered by a tracked log event. Select a message severity level. The condition is met when a message of the specified severity (that contains the match string, if one was specified) is written to a tracked log file.

Note: In order to use this approach, log tracking must be enabled for the resource. To identify the log files that are tracked for a particular resource, see the Configuration Properties section of that resource’s Inventory page.

Note: The log files that are tracked for a resource are defined using the server.log_track.files property.

Config changed condition

a condition that is triggered by a change to a monitored configuration file for a particular resource. To limit the condition to a single configuration file, enter the filename in the match filename field. If you do not specify a filename, a change to any monitored file triggers the alert.
Note: To identify the monitored log files for a particular resource, examine the Configuration Properties section of the resource’s Inventory page.

Note: The configuration files that are monitored for a resource are defined using the server.config_track.files property. The maximum filename length that you can enter is 25 characters.

**Inventory Property** condition
- a condition that is based on the value of an inventory property

**Multiple Conditions**
You can define up to three conditions for an alert. To add a condition, click Add Another Condition.

Specify whether both the new condition and the preceding one must be met for the alert to be triggered (AND) or whether only one of the conditions must be met (OR).

**Recovery Conditions**
A recovery alert condition detects when a condition that triggered a primary alert is no longer true. When a recovery alert is triggered, it marks the primary alert as Fixed and the primary alert definition is re-enabled.

To designate the alert that you are defining as a recovery alert, select a primary alert definition from the Recovery Alert for: drop-down list. The primary alert definition should be configured to Generate one alert and then disable alert definition until fixed. See Reduction of Redundant Alerts on page 37.

**Trigger Frequency and Filtering**
You can make an alert trigger each time its condition is met. As an alternative, you can make an alert trigger only if its condition is met a specified number of times within a specified number of minutes.

You can use an action filter to control alert triggering and alert actions.

**Reduction of Redundant Alerts**
To disable an alert definition after it is triggered (and re-enable it when the alert that triggered it is marked Fixed), click the Generate one alert and then disable alert definition until fixed check box.

This option eliminates redundant alerts for a single problem. If you do not select this option, the alert triggers repeatedly, as long as the triggering condition remains true.

You can use this option in conjunction with recovery alerts to automate the process of disabling and re-enabling an alert definition. This yields the following results:
- There are no redundant alerts.
- You do not have to manually fix an alert that is triggered by a transient problem.

**Coordination of Related Alerts**
The Disregard control actions that are defined for related alerts check box is displayed on Alert Definition pages for resources that support control actions. This option is applicable only when all of the following circumstances exist:
- The current alert includes an alert action.
- The resource that is associated with the alert is a member of an application.
- There are other members of the same application that have alerts that trigger control actions (ideally, the same control action).

Under the preceding circumstances, this configuration option ensures that if multiple alerts are triggered within a short period of time for resources that are members of the same application, only one control action is executed.
For example, this option prevents a server from being restarted several times in a short period of time for the same alert conditions. There might be one alert with an action to restart a Tomcat server (if the JVM Free Memory gets too low) and another alert with an action to restart the same server (if the JVM Active Thread count gets too high). If both alerts trigger at the same time and they are filtering control actions, only one restart control action is executed.

Alert Actions

Introduction
The types of actions that are available in the Alert Definition page vary based on the following factors:
- the type of resource the alert applies to
- whether the types of actions that must be enabled before you can use them (such as escalations, OpenNMS trap actions, and SNMP notifications) have been configured

You can specify multiple actions to be performed automatically when an alert triggers. To define an alert action, select a tab and supply the required information. The following topics provide details.

E-mail Notifications
You can designate users, roles, or explicit e-mail addresses to receive notifications when an alert triggers. See Alert Notifications on page 35.

OpenNMS Notifications
If the server is configured for OpenNMS integration, you can use this tab to configure SAS Environment Manager to send an SNMP trap to OpenNMS when the alert triggers. The notification is generated by the opennms_notify.gsp alert notification template.

To configure an OpenNMS trap action, enter a listen address and port for the OpenNMS server.

SNMP Notification
If the server is configured to send SNMP notifications to your NMS, you can use this tab to configure a trap notification action. See Server Settings on page 94.

The notification that is sent when the alert triggers contains three variable bindings:
- sysUptimeOID.0 (no configuration is required for this binding)
- snmpTrapOID.0 (this binding is configured on the Server Settings page)
- A variable binding for the alert data specified in the snmp_trap.gsp the alert definition name and the short reason for triggering.

Note: Alert templates can be customized.

For richer capability, you can configure an SNMP notification as a step in an escalation. An SNMP notification in an escalation can be configured with additional variable bindings.

To configure an SNMP notification action, provide the following information:
- **IP Address** - the address and port of the target NMS
- **OID** - the OID of the notification to send, which contains the alert details specified in the snmp_trap.gsp template
- **Notification Mechanism** - the type of SNMP notification to send
Escalations

To assign an escalation to an alert definition, select an escalation from the Escalation Scheme drop-down list (at the bottom of an alert definition page). The page refreshes and displays the escalation steps.

You must define an escalation before you can assign it to an alert definition. To create an escalation, click Escalation Schemes Configuration on the Manage page.

**TIP** Using an escalation that is repeats until the alert is fixed is a good way to prevent redundant alerts firing for the same problem.

Advanced

You can define a resource control action to be performed when an alert triggers. See Alert Actions: Control Actions on page 42.

You can define a script to be performed when an alert triggers. See Alert Actions: Scripts on page 39.

Alert Actions: Scripts

**Define a Script Action for an Alert**

A script action enables you to use environment variables that contain information about a triggered alert.

To use a script action, write a script that implements the action that you want to perform using alert-related environment variables. When you configure the alert, specify the script to be executed when the alert triggers. The script is server-side only, so it must be accessible and executable by the identity that runs the Server process.

Script actions can be defined for resource alerts and resource type alerts. Escalation schemes do not support script actions.

Script actions execute one at a time. Until a script action completes, additional alerts will not trigger on the resource.

Script actions are forked by the server's Java process. Most operating systems duplicate the Java process memory before executing the new process (exact behavior varies by operating system). If the operating system does not provide for over-committing memory, script execution requires an amount of free memory that is equal to the amount of memory that the server's Java process consumes. Otherwise, the script action will not run.

**Environment Variables for Triggered Alert Data**
## Environment Variables for Triggered Alert Data

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Example Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>HYPERIC_ALERT_ALERT_TIME</td>
<td>The time at which the alert fired, in milliseconds from epoch.</td>
<td>1219167000000</td>
</tr>
<tr>
<td>HYPERIC_ALERT_CONDITION</td>
<td>The condition that caused the alert to fire. Note: This environment variable is supported only on Unix-based platforms. The value contains the Java 'n' character, which causes errors under Windows. In Windows environments, use the HYPERIC_ALERT_SUMMARY variable, which provides the same information without the 'n' character.</td>
<td>If Load Average 5 Minutes &gt; 1.0 (actual value = 1.4)</td>
</tr>
<tr>
<td>HYPERIC_ALERT_DESCRIPTION</td>
<td>The description of the alert that fired.</td>
<td>This alert will fire when the load rises</td>
</tr>
<tr>
<td>HYPERIC_ALERT_ID</td>
<td>The internal SAS Environment Manager ID for the alert that fired.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: The HYPERIC_ALERT_ID for an alert is not committed to the SAS Environment Manager database until all alert actions are complete. Therefore, an alert action script (whether it uses SQL or HQApi) cannot query or update the SAS Environment Manager database using the alert's HYPERIC_ALERT_ID, because that value will not yet exist in the SAS Environment Manager database.</td>
<td></td>
</tr>
<tr>
<td>HYPERIC_ALERT_NAME</td>
<td>The name of the alert that fired.</td>
<td>High Load</td>
</tr>
<tr>
<td>HYPERIC_ALERT_PRIORITY</td>
<td>The priority of the alert that fired, 1 for High, 2 for Medium, 3 for Low.</td>
<td>2</td>
</tr>
<tr>
<td>HYPERIC_ALERT_SUMMARY</td>
<td>A condensed data string that contains the relevant alert and resource names and values which triggered the alert.</td>
<td>Mac OS X DOWN The-Idea-Men Availability (0.0%)</td>
</tr>
<tr>
<td>HYPERIC_FIXED_ALERT_ID</td>
<td>Valid for recovery alerts only. Supplies the internal SAS Environment Manager ID for the primary alert to which the recovery alert is assigned.</td>
<td></td>
</tr>
<tr>
<td>HYPERIC_FIXED_ALERT_NAME</td>
<td>Valid for recovery alerts only. Supplies the name of the primary alert to which the recovery alert is assigned.</td>
<td>High Load</td>
</tr>
<tr>
<td>HYPERIC_PLATFORM_NAME</td>
<td>The platform on which this alert fired.</td>
<td>localhost.hyperic.com</td>
</tr>
<tr>
<td>HYPERIC_RECOVERY_ALERT</td>
<td>A Boolean that indicates whether the alert is a recovery alert.</td>
<td>false</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
<td>Example Output</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>HYPERIC_RESOURCE_ID</td>
<td>The internal ID for the resource for which the alert fired.</td>
<td></td>
</tr>
<tr>
<td>HYPERICRESOURCE_NAME</td>
<td>The name of the resource for which the alert fired.</td>
<td>localhost.hyperic.com</td>
</tr>
</tbody>
</table>
Example Script

The following script (alert.pl) is an example of using the alert variables.

Note: The example script writes the time at which the script executed and the variables to a log file. It is intended as a simple example, not as a realistic use case.

```perl
#!/usr/bin/perl
my $logfile = "/tmp/output.txt";
my $date = localtime();
open LOGFILE, ">$logfile" or die "Cannot open log file for writing";
print LOGFILE "# Running script at $date", "\n";
foreach $key (sort keys(%ENV)) {
  if ($key =~ m/^HYPERIC/) {
    my $msg = "$key = $ENV{$key}";
    print LOGFILE $msg, "\n";
  }
}
close LOGFILE;
```

Assign a Script Action to an Alert

To assign a script action to an alert definition:

1. Select the alert definition.
2. At the bottom of the Alert Definition page, click Script.
3. Enter the full path to script and click Save Changes.

Alert Actions: Control Actions

You can configure an alert to trigger a supported resource control action. The action can be on either on the resource for which the alert triggered or on another resource within the same platform. You can assign either a built-in or a custom control action to an alert definition.

To use a control action as an alert action:

1. At the bottom of the Alert Definition page, click Control Action. Then click Edit.
2. On the Add Control Action page, select the target resource type from the Resource Type drop-down list.
   - **Note:** The list includes all resource types that have supported control actions that exist on the current platform.
   - **Note:** If you want to assign a custom control action to the alert, select File Service.
3. From the Resource Name drop-down list, select the resource that is the target of the control action.
   - **Note:** If the selected type is FileServer File, select the custom control action to be run.
4. From the Control Type drop-down list, select the command that you want to run when the alert triggers.
   - **Note:** For a custom control action that is configured as a FileServer File service, the only command available is run.
5. Click OK.
Note: To remove a resource control action from an alert definition, select None from the Control Type drop-down list and click OK.

Alert Escalations

Create an Escalation

1. On the Manage page, click Escalation Schemes Configuration.
2. Enter a name.
3. In the If the alert is acknowledged section, select one of the following options:
   - To enable a user to pause the escalation when acknowledging the alert, click Allow user to pause escalation for and make a selection from the drop-down list. This gives the user who acknowledges an alert the option of pausing the escalation process for the specified period of time.
   - To prevent a user from pausing the escalation, click Continue escalation without pausing.
4. In the If the alert state has changed section, select one of the following options:
   - To send alert state change notifications to only those notification recipients who already received a notification in previous escalation steps, click Notify previously notified users of the change.
   - To send alert state change notifications to all notification recipients in the escalation (regardless of whether they received a previous notification), click Notify entire escalation of the change.
5. In the If alert is fixed section, select one of the following options:
   - Stop escalation execution - With this default setting, the escalation will not be repeated for an alert that is unfixed at the end of the escalation.
   - Repeat escalation actions - Click to repeat the escalation process if the alert has not been fixed by the end of the escalation.
6. Click Next Step and define escalation actions. See Escalation Actions on page 44.

View an Escalation

To view an escalation:

1. On the Manage page, click Escalation Schemes Configuration.
2. In the Escalation Name panel (on the left side of the page), click the escalation's name. The escalation details are displayed on the right side of the page.

Edit an Escalation

CAUTION! Editing an escalation affects escalations that are in progress. When you edit an escalation scheme, any escalations that are in progress for alerts to which the escalation is assigned immediately stop executing. When an escalation for an alert has been stopped, that alert cannot be acknowledged. No further notifications of alert state changes are issued. Although an alert with a stopped escalation can be fixed, notification recipients that are configured for the escalation will not be notified that the alert was fixed.

Changes that you make to an escalation scheme take effect for all alert definitions to which the escalation is assigned.

Note: You cannot edit an escalation action. You must instead delete the action and then create a new action.
To change a scheme's name, description, or high-level instructions, click **Edit**, change the values, and click **Save**.

**Delete an Escalation**

**CAUTION!** Deleting an escalation affects associated alerts and escalations that are in progress. When you delete an escalation scheme, any escalations that are in progress for alerts to which the escalation is assigned stop executing immediately. The escalation is removed from any alert definition to which the escalation is was assigned. When an alert that had the escalation triggers, the escalation process is not performed.

To delete an escalation, click **Delete** (to the right of the scheme’s name).

**Escalation Actions**

**E-mail and SMS Notifications**

To create an e-mail or short message service (SMS) escalation action:

1. Select the **E-mail** or **SMS** action type.
2. From the **Select who to notify** drop-down list, select one of the following notification target types:
   - **Notify Roles** notifications are sent to members of native roles that you select
   - **Notify Users** notifications are sent to native users that you select
   - **Notify Other Recipients** notifications are sent to a comma-separated list of the e-mail addresses
3. (Optional) To cause a delay before the next step is performed, select an interval from the drop-down list, instead of leaving the default setting of **Continue**.
4. Click **Save**.

Note: You can add another action to the escalation.

**System Log Notifications**

When you configure an alert escalation to issue a system log notification, the notification logs a line in the following format:

```
SyslogAction[ALERT_ID]: DB_1 4 META/PRODUCT/VERSION RESOURCE_NAME : ALERT_NAME - ALERT_CONDITION
```

The following list provides details:

**RESOURCE_NAME** specifies the resource for which the alert was fired.

**ALERT_NAME** specifies the alert definition that triggered the alert

**ALERT_CONDITION** specifies the alert condition and reported measurement that led to the alert triggering.

To create a system log escalation action:

1. Select the **Sys Log** action type.

   **Note:** This action type is available only if system log notifications are enabled in the configuration.
Supply values for the segments of the message (meta, product, and version).

(Optional) To cause a delay before the next step is performed, select an interval from the drop-down list, instead of leaving the default setting of Continue.

Click Save.

Note: You can add another action to the escalation.

SNMP Notifications

You can define an SNMP notification to be performed as a step in an escalation if the server is configured for your NMS. See Server Settings on page 94.

To create an SNMP notification action:

The trap that is sent when the escalation step is performed contains the following variable bindings:

- sysUptimeOID.0 - No configuration is required for this binding.
- snmpTrapOID.0 - This binding is configured on the Server Settings page.
- A variable binding for the alert data that is specified in snmp_trap.gsp.

Note: The snmp_trap.gsp file is a Groovy Server Page template that returns the alert definition name and the short reason for triggering. This template can be customized.

Any additional variable bindings that you define.

To configure an SNMP notification as an escalation step:

1. Select the SNMP Notification action type.

2. Supply values as follows:

   **IP Address**
   Enter the address and port of the target SNMP server.

   **Notification Mechanism**
   Choose the type of notification to send.
   - v1 Trap
   - v2c Trap
   - Inform

   Note: The Inform setting is not supported if the server is configured for SNMP v1.

   **OID**
   Enter the OID of the notification that will contain the alert details that are specified in the snmp_trap.gsp template.

3. For each additional variable binding that you want to add, click Add Another Variable Binding and supply an OID (as plain text or as an alert variable).

4. (Optional) To cause a delay before the next step is performed, select an interval from the drop-down list, instead of leaving the default setting of Continue.

5. Click Save.

Note: You can add another action to the escalation.
Suppress Alerts

This action stops the alert from triggering repeatedly. It can be useful for an alert definition that is not configured to fire once until fixed. It prevents repetitive triggering at a specific point in the escalation process. After this type of action is performed, the alert does not fire again until after it is fixed.

1 Select the Suppress Alerts action type.

2 (Optional) To cause a delay before the next step is performed, select an interval from the drop-down list, instead of leaving the default setting of Continue.

3 Click Save.

Note: You can add another action to the escalation.

Importing and Exporting Events

Importing Events

To import events, you must first create an event importer service.

1 Select Resources ➔ Browse ➔ Platforms, and then select the platform on which you want to create the service.

2 On the detail page for the selected platform, select Tools Menu ➔ New Platform Service.

3 On the New Service page, specify a name for the service and select SAS Event Importer in the Service Type field. Click OK to define the service.

4 Select Resources ➔ Browse ➔ Services, and then select the SAS Event Importer service that you just defined.

5 The detail page for the service displays a message that the service has not been configured. Click the Configuration Properties link.

6 On the Configuration Properties page, select the importer.enable check box to turn on event importing. Also select the service.log_track.enable check box to enable log tracking. Specify the log files that you want to track in the service.log_track.files field. The files that you specify in this field are the log files that external SAS applications or programs write to. Click OK to save the configuration.

If you want a SAS program to create an event, add the EVEVENTS macro. This macro creates an event in the proper format and stores it in a specified directory. See SAS Environment Manager 2.5 User’s Guide for syntax.

Exporting Events

To export events, you must create an event exporter service.

1 Select Resources ➔ Browse ➔ Platforms, and then select the platform on which you want to create the service.

2 On the detail page for the selected platform, select Tools Menu ➔ New Platform Service.

3 On the New Service page, specify a name for the service and select SAS Event Exporter in the Service Type field. Click OK to define the service.

4 Select Resources ➔ Browse ➔ Services, and then select the SAS Event Exporter service that you just defined.
The detail page for the service displays a message that the service has not been configured. Click the **Configuration Properties** link.

On the Configuration Properties page, select the `exporter.enable` check box to turn on event exporting. Specify the log files that you want to track in the `service.log_track.files` field. The files that you specify in this field are the log files that external SAS applications or programs write to. Click **OK** to save the configuration.

Specify the user ID and password of a SAS Environment Manager user that is used to query events. The user must be a member of the Super User role.

In the `exporter.filename` field, specify the filename and location where event records are to be written. You need to point your third-party monitoring application to this location in order to read events as they are recorded. Click **OK** to save the configuration.

**Using the Alert Center**

**Introduction**

The **Alert Center** page provides a deployment-wide view of alerts and alert definitions. The **Alert Center** is available from the **Analyze** button.

**View, Fix, or Acknowledge Alerts**

The **Alerts** page displays the following data for each displayed alert:

- **Date**
  - The date and time the alert was triggered.

- **Alert Definition**
  - The name of the alert definition that prompted the alert.

- **Resource**
  - The resource the alert was triggered on.

- **Platform**
  - The platform that contains the resource on which the alert was triggered.

- **Fixed**
  - Whether the alert was fixed.

- **Ack**
  - The name of the user who acknowledged the alert.

- **Priority**
  - The alert's priority.

The following table describes options for filtering the list of alerts.

**Filtering the List of Alerts**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show</td>
<td>Filters by the state of the alert.</td>
<td>All</td>
</tr>
<tr>
<td>Alert type</td>
<td>Filters by the type of target resource.</td>
<td>Resource</td>
</tr>
</tbody>
</table>
### Option | Description | Default Setting
--- | --- | ---
Minimum Priority | Filters the list of alerts by displaying those that are set to the specified priority or higher. | Low
In the last | Limits the list to alerts that were triggered within a specified recent period of time. | day
Groups | Limits the list to alerts that were triggered on resources in a group. | All Groups

* If you select Resource, only alerts that are triggered on individual resources are displayed (including alerts that are applied at the resource type level). If you select Group, only alerts that fired on resource groups appear.

To mark an alert as Fixed or to acknowledge an alert that is in escalation, select check boxes and then click Fixed or Acknowledge (at the bottom of the page). You can acknowledge an alert only if it has an escalation scheme defined for it.

### View Alert Definitions

The Definitions tab on the Alert Center page lists alert definitions in your deployment (resource alerts, resource type alerts, and group alerts).

The Resource Alert Definitions pane displays the following data for each definition:

**Name**
The alert definition's name. Click to view the alert definition in the Resource Hub.

**Created**
Date and time the alert was defined

**Modified**
Date and time the alert was modified (if at all)

**Active**
Whether the alert definition is configured to generate alerts) or not. If the alert is defined to fire once, and not again until after it is fixed, a yellow flag icon will be displayed in this column if the alert is not fixed.

**Last Alert**
Date and time the alert was last triggered. Click to view a list of alerts that fired for the alert definition.

**Resource**
The resource, resource type, or group for which the alert was defined. Click to view the resource’s Monitor page.

**Escalation**
The name of the escalation scheme assigned to the alert definition. Click to view the escalation.

**Priority**
The alert definition priority. Click a column heading to sort the table by the content of that column.

Here are some tips for filtering the list:

- The **Definition Type** enables you to limit the list to alert definitions of a particular type (resource alerts, resource group alerts, or resource type alerts).
- The **Exclude Type-Based Definitions** option is available only when Resource is selected for Definition Type. Select check boxes to exclude resource type alert definitions from the list.
- The **Show Only Disabled Definitions** option further limits the list to show only those alert definitions that are currently disabled.
Using the Event Center

Introduction
To access the event center, select Analyze ⇒ Event Center.

The event center provides a deployment-wide view of events that have been logged for resources.

Note: Alerts are automatically logged as events. You can configure SAS Environment Manager to also log events for log messages and resource configuration changes.

The following data is shown for each event:

Date
the date and time that the event happened

Status
for log track events, the level is displayed; for alerts, the word alert is displayed

Resource
the name of the resource that caused the event

Subject
■ for an alert, the alert name
■ for a Nagios check, the plug-in path and name
■ for a configuration tracking event, the type of change (add, delete, modify, or rename)

Detail
information about the event detail or triggering condition.

Note: For a configuration tracking event, the detail displays a limited portion of the raw difference that was detected. For folder changes, the detail displays a list of changed files.

Filtering
You can limit the events that are displayed in the Events section as follows:

Minimum Status
limits by minimum status level (Error, Warning, Info, and Debug).

Type
limits by event type (Log track, Event Track, or Alerts)

Time Range
limits by time period (Last 4 hours, Last 8 hours, Last day, or Last week)

Groups
limits to events that are related to resources that are in specified resource groups

Using the Operations Center

Introduction
To access the operations center, select Analyze ⇒ Operations Center.

The operations center lists resources that are down or have unfixed alerts. You can use filters to scope the content of the page to the resources and problem type of interest. This concise view displays the current number of unavailable resources and unfixed alerts, and a one line problem summary for each resource.
Filtering and Update Frequency

To specify the issues and resources to include, use the Display Filters fields in the upper left of the page.

1. From the Status Type drop-down list, select one of the following settings:
   - **All**
     - list every resource that is currently unavailable or has an unfixed alert
   - **Down Resources**
     - list only resources that are currently unavailable
   - **All Alerts**
     - list all resources that have unfixed alerts
   - **Alerts in Escalation**
     - list resources that have unfixed alerts that are currently in escalation
   - **Alerts not in Escalation**
     - list resources that have unfixed alerts that are not in escalation

2. To also limit the display by hosting platform, enter a string in the Platform Filter field and click Enter to update the page.

3. To also limit the display by group membership, select a group from the Group Filter drop-down list. The list includes resources that belong to the selected group and meet any other specified filtering criteria.

To specify the number of resources that are listed on each page and the frequency with which the page content is updated, use the Table Controls.

Resource Details

Each row in the table in the lower part of the Operations Center represents a resource that is currently down or has an unfixed alert.

The following details are provided:

- **Platform**
  - the platform where the resource runs
- **Resource**
  - the name of the resource that is unavailable or has an unfixed alert
- **Alert Name**
  - for a resource with an alert, the name of the alert definition that triggered the alert
- **Priority**
  - for a resource with an alert, the alert priority
- **Status Type**
  - whether a row is for an unavailable resource or an unfixed alert
- **Last Escalation**
  - for a resource that has an alert in escalation, the timestamp for the last escalation step that has been performed
- **Last Check**
  - for an unavailable resource, shows when metrics for the resource were last collected; for an alert, shows when the alert was last triggered
- **Duration**
  - how long ago the alert was triggered or the resource became unavailable
State
for an alert, an icon indicates the alert is in escalation. A megaphone icon indicates that the alert has been acknowledged.

Status Information
how many times an alert has triggered and the condition that triggered it (if a metric condition triggered the alert, the triggering and current values of the metric are displayed).

Using the Report Center

Introduction
To access the Report Center, select **Analyze ➔ Report Center**. The Report Center is displayed as a separate window or tab in your browser. If your browser blocks pop-up windows, you must disable pop-up blocking for SAS Environment Manager.

The Report Center is a collection of stored process reports that are produced from data in the SAS Environment Manager Data Mart. These reports provide a comprehensive view of the performance and status of your SAS environment and its resources.

The reports and associated stored processes in the Report Center are created when you initialize SAS Environment Manager Extended Monitoring. However, the stored reports operate only on data stored in the SAS Environment Manager Data Mart by the APM or ACM ETL processes. Unless you initialize and enable one of those packages, no reports are produced.

Run a Report
To run a report, expand the folders until you find the report that you want to run, and then click on the report entry. The report is displayed in the viewing pane of the Report Center window.

Some reports contain prompts for you to select the data that you want to display in the report. Use each prompt to select the information required to produce the report. Select the categories of inputs on the left side of the display area to fully customize the report.

When you have specified all of the information required to produce the report, click **Run** to produce the report.

When you select a nightly report, the report is generated using the data currently in the SAS Environment Manager Data Mart and the report is then cached. If you select the same report again, the cached report is displayed, rather than a new report being generated. All of the reports in the Report Center expire at midnight, so displaying a report after midnight displays a new report using current data. The ETL processes that load data into the SAS Environment Manager Data Mart also run at midnight, so reports that you run after midnight use the most current data (from the previous day). However, suppose you create a report, and then run the ETL processes later by using commands. If you run the report again, the cached data will still be used, rather than the data that the ETL process just loaded into the SAS Environment Manager Data Mart.

Native Users and Roles

About Native Users and Roles
SAS Environment Manager has its own registry of users and its own system of roles and permissions, although user definitions in SAS Environment Manager are mapped to user definitions in SAS metadata. SAS Environment Manager uses the same authentication process and authentication provider as the other SAS web applications.
This documentation uses the term *native* to identify features that are internal to this application and distinct from their suite-level counterparts. For example, *native roles* are entirely internal to this application and distinct from metadata-layer roles.

To initiate user, role, and permissions management tasks that are native to SAS Environment Manager, use the Authentication/Authorization section of the Manage page.

### Synchronizing SAS Metadata Users and Native Users

Native user definitions in SAS Environment Manager are mapped to user definitions in SAS metadata. The synchronize function creates a native user definition in SAS Environment Manager for each user assigned to the groups SAS_EV_Super_User, SAS_EV_Guest, and SAS_EV_AppServer_Tier in SAS metadata.

Synchronizing only creates new native user definitions in SAS Environment Manager for user definitions that have been added in SAS metadata. It does not overwrite any existing definitions, either in SAS metadata or in SAS Environment Manager.

To synchronize SAS Environment Manager users with SAS metadata users, click **Sync** in the Authentication/Authorization section of the Manage page.

### List Users

The List Users page includes the basic information for each native user account.

To view or edit a user account, click its user name.

To send e-mail to a user, click an e-mail address.

### User Properties

A user’s General Properties section contains basic information. Here are some tips:

- The Username field contains the user’s account ID.
- The user's password is not displayed. If you have the permission to modify the password, a Change link is displayed.
- The password must contain at least 6 case-sensitive characters and numbers, no spaces, and no quotation marks.
- You can click the user’s e-mail address to send an e-mail to the user.
- The Format field determines the format in which e-mails are sent to the user.
- The SMS Address field contains the e-mail-to-SMS gateway e-mail address for the user’s SMS device.
  
  **Note:** Check with the service provider for details about your email-to-SMS configuration.
  
  **Note:** Basic alert notifications that are sent to this address are in long format, which can result in as many as five separate messages per-notification. We recommend that you use SMS alerting only as a step in an escalations (which use short format).

A user’s Roles Assigned To section lists the roles that the user is assigned to.

### Assign Roles to a User

To assign roles to a user:

1. On the Manage page, click **List Users**.
2. Click the user that you want to assign roles to.
In the Roles Assigned To section, click Add to List.

Use the check boxes and arrows to move roles to the Add to Roles list.

**TIP** You must first select check boxes and then use the arrows to move the selected items.

Click OK.

**Modify a User’s Properties**

To modify a user’s properties:

1. On the Manage page, click List Users.
2. Click the user that you want to modify.
3. Make changes as needed. See User Properties on page 52.
4. Click OK.

**List Roles**

The List Roles page includes basic information for each native role.

To view or edit a role, click its name.

**Add a Role**

To add a role:

1. On the Manage page, click New Role.
2. On the New Role page, enter a name.
3. In the Permissions section, set a permission level in each row. See Role Permissions on page 54.
4. Click OK.

**Role Properties**

**Introduction**

The Permissions section displays the permissions that the role provides. The display is a matrix of permission level by resource type. To modify the role’s permissions, click Edit. See Role Permissions on page 54.

In the Assigned Users section, you can click a user name to view the user’s properties. To add users to the role, click Add to List.

In the Assigned Groups section, you can click the name of a resource group to view that group. A role’s permissions affect access to only those resources that are assigned to it.

The Alert Calendar section defines the time frame in which the role’s users are available for alert notifications. By default, role users are available for notifications all of the time.
Continuous Coverage for Alerts

To provide continuous coverage for alert notifications, create multiple roles that have complementary alert calendars. Assign each user to the role whose alert calendar matches the user’s availability.

When you define an availability calendar, use the first set of From and To drop-down lists to specify a start time and an end time. If you need to exclude a time period, click Except, and use the From and To pull-downs on the right to specify the exclusion.

Role Permissions

Permission Definitions

The following table documents the available permission levels:

### Permission Levels for Native Roles

<table>
<thead>
<tr>
<th>Permission Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Provides no access to instances of the type.</td>
</tr>
<tr>
<td>Read-Only</td>
<td>Provides View access to instances of the type. Also provides View access to alert definitions for certain inventory types (platforms, servers, services, and groups). This permission level does not provide the ability to enable, disable, fix, or acknowledge alerts or control resources. Those capabilities must be explicitly granted.</td>
</tr>
<tr>
<td>Read-Write</td>
<td>Provides the ability to view and edit instances of the type, but does not provide the ability to create or delete instances. Also provides the following capabilities for platforms, servers, services, and groups:</td>
</tr>
<tr>
<td></td>
<td>- Full access to alert definitions for the inventory type.</td>
</tr>
<tr>
<td></td>
<td>- Permission to manage alerts for the inventory type.</td>
</tr>
<tr>
<td></td>
<td>- Permission to perform control operations on resources of the inventory type.</td>
</tr>
<tr>
<td>Full</td>
<td>Provides the ability to create, edit, delete, and view instances of the type. Also provides the following capabilities for platforms, servers, services, and groups:</td>
</tr>
<tr>
<td></td>
<td>- Full access to alert definitions for the inventory type.</td>
</tr>
<tr>
<td></td>
<td>- Permission to manage alerts for the inventory type.</td>
</tr>
<tr>
<td></td>
<td>- Permission to perform control operations on resources of the inventory type.</td>
</tr>
</tbody>
</table>

Permissions by Inventory Type

The following table provides information about how permission levels apply to different types of resources:

<table>
<thead>
<tr>
<th>Inventory Type</th>
<th>Permission Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>To enable role members to create and delete native user accounts, grant Full.</td>
</tr>
<tr>
<td></td>
<td>To enable role members to edit native user accounts, grant Read-Write.</td>
</tr>
<tr>
<td>Inventory Type</td>
<td>Permission Level</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Roles</td>
<td>If you grant Full the role's access to users and resource groups will be at least Read-Only (because to create a role, you need to view users and resource groups)</td>
</tr>
</tbody>
</table>
| Resource Groups| - To enable role members to delete resource groups that were created by other users, grant Full.  
                - To enable role members to modify resource groups that were created by others, grant Read-Write.  
                Note: Any user can create resource groups and delete the groups that they create.       |
| Platforms      | - If you grant Full, the role's permission level for servers and services must also be Full.  
                - If you grant Full or Read-Write, the Can Fix/Ack Alerts? and Can Control? capabilities are automatically selected.  
                - If you grant Read-Only, you can also grant alert management or resource control capabilities (by clicking Can Fix/Ack Alerts? or Can Control?).  
                - If you grant None, you cannot grant alert management or resource control permissions.  |
| Servers        | - If you grant Full, the role's permission level for platforms must be at least Read-Write, and the role's permission level for services must be Full.  
                - If you grant Full or Read-Write, the Can Fix/Ack Alerts? and Can Control? capabilities are automatically selected.  
                - If you grant Read-Only, you can also grant alert management or resource control capabilities.  
                - If you grant None, you cannot grant alert management or resource control permissions.  |
| Services       | - If you grant Full, the role's permission level for servers must be at least Read-Write.  
                - Grant at least Read-Only, if you are going to grant the role Full permission to applications.  
                - If you grant Full or Read-Write, the Can Fix/Ack Alerts? and Can Control? capabilities are automatically selected.  
                - If you grant Read-Only, you can also grant alert management or resource control capabilities.  
                - If you grant None, you cannot grant alert management or resource control permissions.  |
| Applications   | To enable role members to create and delete applications, grant Full.  
                To enable role members to modify applications that were created by others, grant Read-Write.  |
| Alert Escalations| To enable role members to create and delete escalations, grant Full.  
                To enable role members to modify escalations, grant Read-Write.  |
Guidance for Setting Permissions

The following table provides guidance for choosing permission levels:

Permission Recommendations

<table>
<thead>
<tr>
<th>Activities</th>
<th>Permission Level Recommendation</th>
</tr>
</thead>
</table>
| Add resources to inventory and create alert definitions | Either Full or Read-Write  
This enables a role to also process triggered alerts and to perform resource control actions. |
| Monitor resources, respond to alerts and control resources | Read (also grant fix, acknowledge, and control capabilities as needed).  
This enables operations staff to respond to alerts, examine alert definition details, and perform resource control tasks. This permission level does not provide the ability to create, modify, or delete resources and alert definitions. |
| Monitor resources                               | Read.  
This is appropriate for roles that view and monitor resources. This permission level does not provide the ability to create, modify, or delete resources and alert definitions or respond to alerts. |

Dependencies

A role that has Full access to an inventory type must have at least Read access to the parent type (if there is one) and Full access to the child type (if there is one).

For example, Full access to servers requires at least Read access to platforms and Full access to services.

Scope

A role’s permission levels affect only those resources that are assigned to the role. See Assign Resource Groups to Roles on page 57.

Assign Users to Roles

To assign users to a role:

1. Navigate to the role.
2. In the Assigned Users section, click Add to List.
3. On the Assign Users to Role page, use the check boxes and arrows to move users to the Assign To Role list.

**TIP** You must first select check boxes and then use the arrows to move the selected items.

4. Click OK.
Assign Resource Groups to Roles

You define the scope of a role by assigning resource groups to the role. For example, if a role's permission level for platforms is **None**, members of the role cannot access any platforms that are in resource groups that are assigned to the role.

**CAUTION!** Permissions are granted only to groups of individual resources, not to nested groups of resources. Assigning a group of groups or a group of applications to a role does not grant permissions to the individual resources within the nested structure. Groups that you assign to a role for the purpose of granting permissions must contain individual resources, not other groups or applications.

1. Navigate to the role.
2. In the Assigned Groups section of the page, click **Add to List**.
3. On the Assign Groups to Role page, use the check boxes and arrows to move users to the Assign To Role panel.
4. Click **OK**.

---

**Resource Control Actions**

**Resource Control Actions: Overview**

**Introduction**

A resource control action is a command that an agent can perform on an individual managed resource (usually a server) or on a compatible group of resources. For example, a web application server might have **start**, **stop**, and **restart** as available control actions.

A resource’s **Control** page includes the following sections:

- The **Current Status** section displays the currently running control action (if there is one) and provides the following details:
  - **Control Action**: the name of the control action
  - **Command State**: the result of this control action (**Successful** or **Failed**).
  - **Command Status**: what this control action is currently doing (**In Progress**, **Stopped**, **Running**, **Restarting**, or **Stopping**).
  - **Elapsed Time**: how long this control action has been running
  - **Description**: a description of this control action
  - **Date Started**: the day and time on which the server started performing this control action
  - **Date Scheduled**: the day and time on which this control action is scheduled to run

- The **Quick Control** section displays the resource control actions that are available for the current resource.
The Control Action Schedule section lists all of the resource control actions that are currently scheduled for this resource.

**Run a Control Action On-Demand**
To initiate a quick (on-demand) resource control action on the current resource:

1. Select the action in Control Action.
2. Enter any required Control Arguments for the action.
3. Click The control action runs immediately.
   
   **Note:** If other resource control actions are in progress, the action runs after those actions are completed.

**Delete a Scheduled Control Action**
In the Control Action Schedule section, select the check box for the scheduled control action and click Delete. The deleted action will no longer be performed on the resource.

**Schedule a Resource Control Action**
To schedule a resource control action for the current resource:

1. In the Control Action Schedule section, click New
2. On the New Scheduled Control Action page, select an action from the Control Action drop-down list.
3. Specify whether the control action should run immediately or at a specified date and time.

   **TIP** Scheduling a control action to run immediately is the same as running it on-demand as a quick control action.

   **TIP** If you specify a date and time, you can also specify recurrence.

4. Click OK.

**Edit a Scheduled Resource Control Action**
To change the name, description, or schedule of a resource control action:

1. In the resource’s Control Action Schedule section, click the scheduled control action.
2. On the Edit Scheduled Control Action page, adjust values and then click OK.

   **TIP** If you specify a date and time, you can also specify recurrence.

**View a Resource’s Control Action History**
To view a list actions that have been performed on a resource, click History on the resource’s Control tab.
Note: If the Control tab is not present, control actions are not supported for the current resource type.

On the Control History page, the following information is provided:

Control Action
the action that was performed

Arguments
any arguments that were supplied to the control action

Command State
the status of the action (Completed, In Progress, or Failed)

Date Started
the date and time that the control action was initiated

Elapsed Time
how long it took to perform the control action

User
the user ID of the user that initiated or scheduled the control action

Message
any additional information about the control action

To delete a control action, select its check box and click Delete (at the bottom of the page).

---

**tcServer Administration**

**Application Management**

**tc Runtime Application Management**

The Application Management page, available when a tc Runtime instance or a group of tc Runtime instances is selected, enables an authorized user to manage applications deployed that server instance or group.

The super-user can use all the tc Runtime Application Management features of SAS Environment Manager. However, if you sign in to SAS Environment Manager as a non-super-user, then that user must have certain permissions to be able to use the tc Runtime features. See User Permissions Required to Use the tc Runtime Features on page 62 for more information.

A group is not equivalent or similar to a tc Runtime cluster.

A group is a set of other managed resources. An authorized user can create a group and assign resources to it. A group whose members are all of the same resource type is referred to as a compatible group. You can manage and monitor the resources in a compatible group at the group level. Grouping tc Runtime instances allows you manage applications across multiple tc Runtime instances.

A tc Runtime cluster enables session replication. Clustering behavior is defined in a tc Runtime instance's server.xml file.

**Navigating to a tc Runtime Instance or Group**

To navigate to the Application Management page of a tc Runtime instance or group, follow these steps:

1. Click Resources ➔ Browse at the top of the Dashboard.

   To browse to a server instance, select Servers to view a list of the servers to which you have access. tc Runtime instances have the server type "SpringSource tc Runtime 7.0". Apache Tomcat server instances have the server type "Tomcat X.X".
To browse to a group of servers, select **Compatible Groups/Clusters** to view a list all the compatible groups to which you have access. Groups of tc Runtime have the type "SpringSource tc Runtime 7.0".

2 In the table, select the name of the tc Runtime instance or group to which you want to navigate.

3 Select **Views ➪ Application Management**.

### Creating tc Runtime Groups

Grouping tc Runtime instances eases the process of managing server instances and applications. For example, you can deploy an application to group of tc Runtime with a single command, instead of deploying to each instance individually. To create a group of tc Runtime instances:

1 Click **Resources ➪ Browse** at the top of the Dashboard.

2 Click **Servers** to list servers in inventory to which you have access. (Note: Only server instances that have been auto-discovered by SAS Environment Manager and have been added to the inventory appear). tc Runtime instances have the server type "SpringSource tc Runtime 7.0". Apache Tomcat server instances have the server type "Tomcat X.X".

3 Check the box to the left of each tc Runtime instance that you want to include in the new group.

4 Click **Group**.

5 Enter a name for the group (required) and a description and location as desired.

6 Click **OK**.

### Listing Applications

Navigate to the **Application Management** page for a server instance or group. Deployed applications are listed in the **Manage Deployed Applications** section of the page. For a group, the table lists all applications deployed to all servers in the group. The table shows:

- **Status**
  - The state of the application - either **Running** or **Stopped**. For a group of servers:
    - **Running** or **Stopped** indicates that all instances of the application on all servers in the group have that state.
    - A numeric value indicates the number of servers upon which the application's state is **Running**.

- **Sessions**
  - The number of current active sessions for the application.

**Note:** Only applications on running tc Runtime instances appear. SAS Environment Manager returns an error for application hosts that are not running.

### Starting Applications

Starting an application makes it available to users. You must have previously deployed the application to be able to start it.

1 Navigate to the **Application Management** page of a tc Runtime instance or group.

2 In the **Manage Deployed Applications** section, select the box next to the applications that you want to start.

3 Click **Start**. The status of the application changes to **Running**.

4 See the **Results of the last operation** section for details about the result of starting the application.
Stopping Applications
Stopping an application makes it unavailable to users.

1. Navigate to the Application Management page of a tc Runtime instance or group.
2. In the Manage Deployed Applications section, select the box next to the applications that you want to stop.
3. Click Stop. The status of the application changes to Stopped.
4. See the Results of the last operation section for details about the result of stopping the application.

Reloading Applications
When you reload an existing application, it shuts itself down and then reloads itself.

1. Navigate to the Application Management page of a tc Runtime instance or group.
2. In the Manage Deployed Applications section, select the box next to the applications that you want to reload.
3. Click Reload. The status of the application changes to Running.
4. See the Results of the last operation section for details about the result of reloading the application.

tc Runtime Configuration

Navigating tc Runtime Configuration Pages
To navigate to the Server Configuration page for a tc Runtime instance:

1. Select Resources ➤ Browse.
2. Select Servers to list all of the tc Runtime instances in inventory.
   - tc Runtime instances have the server type "SpringSource tc Runtime 7.0"
   - Apache Tomcat instances have the server type "Tomcat X.X".
3. Click the name of the tc Runtime instance to which you want to navigate.
4. Click the Views ➤ Server Configuration tab.

There are four tc Runtime configuration pages, three of which are beneath the main Server Configuration page:

- **Configuration**
  Configure general tc Runtime options, such as JVM options, JSP behavior, and default options for static content.

- **Resources**
  Create, configure, and delete JDBC data sources.

- **Services**
  Configure the default Catalina service, and create new ones. A tc Runtime service groups together one or more connectors and a single engine. The engine, in turn, groups together one or more virtual hosts.

The Advanced section provides links for reloading, reverting, and uploading server configurations.
## Saving or Undoing Changes

SAS Environment Manager populates the fields of the tc Runtime configuration pages from its configuration files, including:

- `conf/server.xml`
- `conf/context.xml`
- `conf/web.xml`
- `bin/setenv.sh`
- `conf/catalina.properties`
- `conf/logging.properties`

(All relative to `CATALINA_BASE`, which is the root directory of the tc Runtime instance.)

Each configuration page includes a **Save** button for saving the changes made in the user interface to the tc Runtime configuration files. If you try to navigate to a different page without saving any of your updates, you will be prompted to save the updates.

When you click **Save** to save your changes, a dialog box labeled **Changes have been made locally** is displayed until you select either:

**Push**
- to write the configuration changes that you have made to the appropriate tc Runtime configuration file (such as `server.xml`). If you push the changes, SAS Environment Manager overwrites existing configuration, saving a backup of the overwritten configuration. Most saved changes to the tc Runtime configuration require a server restart to take effect. SAS Environment Manager flags these cases and provides a link to restart the tc Runtime.

**Undo**
- to undo all changes that have been made since the last push or undo.

**CAUTION!** If you update the tc Runtime configuration settings from SAS Environment Manager, do not manually update the tc Runtime configuration files at the same time. SAS Environment Manager clears its local memory and reloads the configuration files upon certain events, not continuously.

## User Permissions Required to Use the tc Runtime Features

The SAS Environment Manager super-user can use all of the tc Runtime features of SAS Environment Manager. However, if you sign in as a non-super-user, then that user must have certain permissions to be able to use the tc Runtime features, as described in this section.

In SAS Environment Manager, users are assigned application roles, which in turn are assigned permissions, such as View and Control.

The following table describes the additional effects that some of the SAS Environment Manager permissions have on the tc Runtime features. Use this table to determine which role you should assign a user that will be managing tc Runtime instances.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Additional Effect on tc Server Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>View</td>
<td>Allows the user to:</td>
</tr>
<tr>
<td></td>
<td>- View the deployed web applications in the <strong>Application Management</strong> page.</td>
</tr>
<tr>
<td></td>
<td>- View the current configuration of a tc Runtime instance in the <strong>Server Configuration</strong> page.</td>
</tr>
</tbody>
</table>
Modify

Allows the user to:

- Update the fields in the **Server Configuration** page and then push the data to the configuration files associated with the tc Runtime instance, such as server.xml.
- Use the application lifecycle commands of the **Application Management** page to start, stop, reload, or undeploy a web application.

Control

Allows the user to use the commands in the **Control** page to start, stop, and restart a tc Runtime instance.

### Configuring General tc Runtime Options

The main tc Runtime configuration page includes options to change the shutdown port and shutdown command.

1. Navigate to the **Server Configuration** page for the tc Runtime instance. See [Navigating tc Runtime Configuration Pages on page 61.](#).
2. Click **Configuration**.
3. Select **General**.
4. Make your changes.
5. Click **Save**. The message "Configuration saved successfully" indicates your changes were successfully saved.
6. To write your changes to the tc Runtime configuration files, click **Push** in the Changes have been made locally dialog box. See [Saving or Undoing Changes on page 62.](#)

### Configuring Start Up Options

The page for configuring tc Runtime Start settings includes options for configuring the JVM where the instance runs, including minimum and maximum heap size, garbage collection, and debugging options.

**NOTE:** SAS Environment Manager populates the tc Runtime **Start** page with information from the `CATALINA_HOME/bin/setenv.sh` file of the server instance that you are configuring (specifically the `JVM_OPTS` environment variable.) If you have not set the `JVM_OPTS` environment variable in this file, then the fields in the **Server Start** page are blank.

The page enables you to add your own command line arguments to the JVM; be careful using this option because SAS Environment Manager does not validate the options but simply adds them to the Java command that starts the tc Runtime instance. If you enter them incorrectly, you will get an error starting the tc Runtime instance.

1. Navigate to the tc Runtime configuration page. See [Navigating tc Runtime Configuration Pages on page 61.](#)
2. Click **Configuration**.
3. Select **Server Start**.
4. Make your changes.
5. To add your own JVM command line arguments, select **Advanced** and enter the arguments in the form `-Xoption=value` or `-XX:option=value`, separating options with a space.
6. Click **Save**. The message "Configuration saved successfully" indicates your changes were successfully saved.
To write your changes to the tc Runtime configuration files, click **Push** in the Changes have been made locally dialog box. See Saving or Undoing Changes on page 62.

### Configuring the Context Container

Use this page to configure the context for every web application deployed to this tc Runtime instance.

1. Navigate to the tc Runtime configuration page. See Navigating tc Runtime Configuration Pages on page 61.
2. Click **Configuration**.
3. Select **Context Container**.
4. Make your changes.
5. Click **Save**. The message "Configuration saved successfully" indicates your changes were successfully saved.
6. To write your changes to the tc Runtime configuration files, click **Push** in the Changes have been made locally dialog box. See Saving or Undoing Changes on page 62.

### Configuring JSP Options

SpringSource tc Runtime implements version 2.1 of the Java Server Pages (JSP) specification. Use this page to configure the behavior of the JSPs that are deployed to a tc Runtime instance.

1. Navigate to the tc Runtime configuration page. See Navigating tc Runtime Configuration Pages on page 61.
2. Click **Configuration**.
3. Select **Server Defaults: JSP**.
4. Make your changes. See Server Defaults: JSP on page 72 for a list of possible changes.
5. Click **Save**. The message "Configuration saved successfully" indicates your changes were successfully saved.
6. To write your changes to the tc Runtime configuration files, click **Push** in the Changes have been made locally dialog box. See Saving or Undoing Changes on page 62.

### Configuring Static Content Defaults

Use this page to configure the behavior of static content in web applications that run on tc Runtime.

1. Navigate to the tc Runtime configuration page. See Navigating tc Runtime Configuration Pages on page 61.
2. Click **Configuration**.
3. Select **Server Defaults: Static Content**.
4. Make your changes. See Server Defaults: Static Content on page 74 for a list of possible changes.
5. Click **Save**. The message "Configuration saved successfully" indicates your changes were successfully saved.
6. To write your changes to the tc Runtime configuration files, click **Push** in the Changes have been made locally dialog box. See Saving or Undoing Changes on page 62.
Using the Advanced Server Configuration Options

Overview
The Advanced section of the main Server Configuration tab includes options for reverting or reloading configuration values in the event that you do not want to save any of the recent updates that you have made using SAS Environment Manager. The Advanced section also includes an option to upload a local configuration file in its entirety, such as server.xml. The following sections provide more information about these options.

SpringSource recommends that you use these options with caution.

Reloading Settings from Server
Select Reload Settings From Server if you want to reload the server configuration currently contained in the tc Runtime configuration files. With this option, all local changes to the tc Runtime instance that you have made using SAS Environment Manager that you have not yet pushed to the instance will be lost.

Reverting to a Previously Saved Configuration
Select Revert To a Previously Saved Configuration if you want to revert to the most recent backup copy of the tc Runtime configuration. Each time you push changes from SAS Environment Manager to the tc Runtime configuration files, the application makes a timestamped backup copy of the previous configuration before overwriting the relevant configuration file, such as server.xml. With this option, you can revert back to the most recent backup copy in the event that there was a problem with the most recent changes that you pushed. As with reloading the current configuration, if you revert to a backup copy, any local changes to the tc Runtime instance made using SAS Environment Manager will be lost.

If you have never pushed configuration changes from SAS Environment Manager to the tc Runtime instance, then no backup file will exist to which the application can revert. In this case, if you try to revert, you will get an error.

Uploading a Configuration File
Select Upload a Configuration File to upload a local configuration file, such as server.xml, and copy it to the appropriate tc Runtime instance directory. Use the Configuration File menu to specify the type of configuration file that you are going to upload, and then select Browse to browse for the file on your local computer.

The tc Server plug-in makes a timestamped backup copy of the current configuration file before it overwrites it with the one you uploaded. This means that you can revert to the backup copy in the event that you do not want to use the uploaded configuration file for some reason.

Configuring and Creating JDBC Data Sources
JDBC datasources enable you to access data in a database server. A datasource defines a pool of JDBC connections which in turn connect to a specific database using a specified URL, user name, and so on. Use this page to create and configure datasources.

You can create two types of JDBC data sources:

Database Connection Pool (DBCP) Datasource
The DBCP Datasource is the standard datasource provided by tc Runtime that uses the commons-dbcp package. Although this datasource is adequate for simple applications, it is single-threaded which means that in order to be thread-safe, tc Runtime must lock the entire pool, even during query validation. Therefore, it is not suitable for highly concurrent environments. Also, it can be slow, which in turn can negatively affect the performance of web applications.

Tomcat Datasource
The Tomcat Datasource includes all the functionality of the DBCP datasource, but adds additional features to support highly concurrent environments and multiple core and CPU systems. The Tomcat datasource typically performs much better than the DBCP datasource. Additional features include:
Dynamic implementation of the interfaces, which means that the datasource supports the java.sql and javax.sql interfaces for your run-time environment (as long as your JDBC driver supports it), even when compiled with a lower version of the JDK.

Validation intervals so that tc Runtime does not have to validate every single time the application uses the connection, which improves performance.

Run-Once query, which is a configurable query that the tc Runtime instance runs only once when the connection to the database is established. This is very useful to setup session settings that you want to exist during the entire time the connection is established.

Ability to configure custom interceptors to enhance the functionality of the datasource. You can use interceptors to gather query statistics, cache session states, reconnect the connection upon failures, retry queries, cache query results, and so on. The interceptors are dynamic and not tied to a JDK version of a java.sql/javax.sql interface.

Asynchronous connection retrieval, which means that you can queue your request for a connection and receive a Future response in return.

To create a new JDBC datasource, or edit an existing one:

1. Navigate to the tc Runtime configuration page. See Navigating tc Runtime Configuration Pages on page 61.
2. Click Resources.
3. Select JDBC Data Sources.
4. If you want to edit an existing data source, click its name in the table and make your changes. If you want to create a new data source, select Create a New Tomcat/DBCP Data Source. See tc Runtime JDBC Reference on page 75 for more information.
5. Click Save. The message "Configuration saved successfully" indicates your changes were successfully saved.
6. To write your changes to the tc Runtime configuration files, click Push in the Changes have been made locally dialog box. See Saving or Undoing Changes on page 62.

Configuring and Creating tc Runtime Services

A tc Runtime service represents the combination of one or more connector components that share a single engine component for processing incoming requests. A tc Runtime instance can have one or more services configured. The default service is "catalina".

1. Navigate to the tc Runtime configuration page. See Navigating tc Runtime Configuration Pages on page 61.
2. Click Services.
3. To edit an existing service, such as the default "catalina" service, click its name in the table and then configure or add the following components of the service:
   - Connectors
   - Engine
   - Virtual Host
   - Logging System
4. If you want to create a new service, click New Service. See tc Runtime Services Reference on page 78 for more information.
5. Click Save. The message "Configuration saved successfully" indicates your changes were successfully saved.
Configuring and Creating Connectors
Connectors represent the interface between external clients sending requests to (and receiving responses from) a particular tc Runtime service. A tc Runtime instance can have one or more connectors, one for each supported message protocol. The default connector, configured for each tc Runtime, is the HTTP connector.

Use this page to configure, or create new, connectors for the current tc Runtime service.

1. Navigate to the tc Runtime configuration page. See Navigating tc Runtime Configuration Pages on page 61.
2. Click Services.
3. In the Services table, click the name of the service that you want to configure or for which you want to create a connector.
4. Select Connectors.
5. If you want to edit an existing connector, click its name in the table and make your changes. If you want to create a new connector, select New AJP Connector or New HTTP(S) Connector, depending on the type of connector that you want to create. See Connector Properties on page 78 for more information.
6. Click Save. The message "Configuration saved successfully" indicates your changes were successfully saved.

Configuring and Creating Virtual Hosts
A tc Runtime host represents a virtual host, which is an association of a network name for a server (such as "www.mycompany.com") with the particular computer which hosts the tc Runtime instance. In order to be effective, this name must be registered in the Domain Name Service (DNS) server that manages your Internet domain.

Use this page to configure, or create new, virtual hosts for the current tc Runtime service.

1. Navigate to the tc Runtime configuration page. See Navigating tc Runtime Configuration Pages on page 61.
2. Click Services.
3. In the Services table, click the name of the service that you want to configure or for which you want to create a virtual host.
4. Select Hosts.
5. If you want to edit an existing host, click its name in the table and make your changes. If you want to create a new host, click the New Host link. See Host Properties on page 82 for more information.
6. Click Save. The message "Configuration saved successfully" indicates your changes were successfully saved.

Configuring tc Runtime Logging
Use this page to configure the logging system for the current engine. Note that you can also configure logging for a host by configuring the specific Host component.

1. Navigate to the tc Runtime configuration page. See Navigating tc Runtime Configuration Pages on page 61.
2. Click Services.
3. In the Services table, click the name of the service for which you want to configure logging.
Select Logging.

Make your changes in the table. See HTTP Access Logging on page 83 for more information.

Click Save. The message "Configuration saved successfully" indicates your changes were successfully saved.

## tc Runtime Configuration Reference

### Overview

This page defines the fields on the Configuration page of the Server Configuration page. This is the location where an authorized user can configure a tc Runtime instance.

### General Configuration

#### Server Properties

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Shutdown Port** | The TCP/IP port where the tc Runtime instance listens for a shutdown command. The connection must be initiated from the same server computer that is running this instance of tc Runtime.  
Valid values are -1, 1, 2, ... up to 65535.  
With the default setting, "-1", no shutdown port is enabled, so that the only way the server instance can be shut down is by a local "kill" statement to the server process. |
| **Shutdown Command** | The command to shut down tc Runtime. This command is issued through a TCP/IP connection to the Shutdown Port. |

#### JMX Listener

The JMX Listener section configures the component of the tc Runtime instance that listens for Java Management Extensions (JMX) connections from management tools, such as the agent. By default, tc Runtime enables JMX connectivity.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enabled</strong></td>
<td>Specifies whether the tc Runtime instance's pre-configured JMX listener is enabled. Important: The agent uses JMX to connect to tc Runtime, so if you disable the JMX listener then you will not be able to use it configure tc Runtime instances or groups from SAS Environment Manager, unless you configure JMX for tc Runtime through some other mechanism.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Specifies the port on which tc Runtime listens for JMX/RMI connections. Specify a port number that is not in use by another process.</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>Specifies the IP address on which tc Runtime listens for JMX/RMI connections. If the IP address is on the same as the tc Runtime instance, you can enter 127.0.0.1.</td>
</tr>
<tr>
<td><strong>Protocols</strong></td>
<td>Specifies a comma-separated list of enabled SSL/TLS protocols. If you do not enter a value for this property, the default protocols are enabled.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Authenticate</strong></td>
<td>Specifies whether tc Runtime authenticates users that connect to the server using the JMX port.</td>
</tr>
<tr>
<td></td>
<td>If you enable this field, tc Runtime looks up the user and password in the files specified by the Access File and Password File. If tc Runtime finds the user name and password in the files, then the user is authenticated and allowed JMX access. If you disable this property, all users can access tc Runtime via JMX.</td>
</tr>
<tr>
<td></td>
<td>Configure the JMX user and password in SAS Environment Manager on server instances the Configuration Properties page. The default JMX user and password is configured by default when you install tc Server. However, if you change the name or password of the user in the access and password files, you must also change the configured user/password in SAS Environment Manager.</td>
</tr>
<tr>
<td><strong>Access File</strong></td>
<td>Specifies the full pathname of the tc Runtime file that contains the list of users allowed to access tc Runtime using JMX. Note that this file is on the computer that hosts the tc Runtime instance, not the computer that hosts the server.</td>
</tr>
<tr>
<td></td>
<td>The access file contains one line per user; each line contains a user name and permission level:</td>
</tr>
<tr>
<td></td>
<td>readonly</td>
</tr>
<tr>
<td></td>
<td>user can only view tc Runtime configuration</td>
</tr>
<tr>
<td></td>
<td>readwrite</td>
</tr>
<tr>
<td></td>
<td>user can view and modify tc Runtime configuration. The default name for the access file is jmxremote.access; the default location is the CATALINA_BASE/conf directory of the tc Runtime instance. Each tc Runtime instance is configured by default with an &quot;admin&quot; user with readwrite permission.</td>
</tr>
<tr>
<td><strong>Password File</strong></td>
<td>Specifies the full pathname of the tc Runtime file that contains passwords for the users listed in the Access File. Note that this file is on the computer that hosts the tc Runtime instance, not the computer that hosts the server.</td>
</tr>
<tr>
<td></td>
<td>The password file contains one line for each user listed in the access file; each line contains a user name and password.</td>
</tr>
<tr>
<td></td>
<td>The default name for the password file is jmxremote.password; the default location is the CATALINA_BASE/conf directory of the tc Runtime instance. The password for the pre-configured &quot;admin&quot; user is &quot;springsource&quot;.</td>
</tr>
<tr>
<td><strong>Use SSL</strong></td>
<td>Specifies whether to use secure sockets layer (SSL) for users' JMX connections to tc Runtime.</td>
</tr>
<tr>
<td></td>
<td>To use SSL, you must first set up a digital certificate on the computer that hosts the tc Runtime instance and then configure the SSL settings on this page. You can use a command-line utility keytool to manage digital certificates.</td>
</tr>
<tr>
<td><strong>Client Authentication</strong></td>
<td>Specifies whether client authentication is required when using SSL. If you enable this property, tc Runtime authenticates JMX/SSL clients using certificate authentication rather than file-based authentication; this means that tc Runtime must find the client's certificate in its truststore or it will deny the client JMX access. This implies that only clients with known SSL certificates are allowed access to tc Runtime.</td>
</tr>
<tr>
<td><strong>Use JDK Client Factory</strong></td>
<td>Specifies whether the agent uses the required client libraries from the JDK. The required libraries are used to pass SSL-specific properties (such as the trust store and password) to the tc Runtime instance. If you disable this property, you must manually set up the agent's CLASSPATH to find these client libraries.</td>
</tr>
<tr>
<td><strong>Cipher Suites</strong></td>
<td>Specifies a comma-separated list of enabled SSL/TLS cipher suites. A cipher suite is a combination of cryptographic parameters that define the security algorithms and key sizes used for authentication, key agreement, encryption, and integrity protection. If you do not enter a value for this property, the default cipher suites are enabled.</td>
</tr>
</tbody>
</table>
### Field Name | Description
--- | ---
**Truststore File** | Specifies the full pathname of the truststore file used by SSL.
A truststore is a special type of keystore file that is used when making decisions about what to trust. If you receive some data from an entity that you already trust, and if you can verify that the entity is the one that it claims to be, then you can assume that the data came from that entity. This means that the key of a truststore file typically contains an entity's identity and a public key, as opposed to a private key contained in a more restricted keystore file.

**Truststore Pass** | Specifies the password used to access the truststore file.

**Keystore File** | Specifies the full pathname of the keystore file.
A keystore is a database of key material. Key material is used for a variety of purposes, including authentication and data integrity. There are various types of keystores available, including "PKCS12" and "JKS" from Sun. Typically, the key of a keystore consists of an entity's identity and its private key.

**Keystore Pass** | Specifies the password used to access the keystore file.

### Server Start Configuration

**Notes**
SAS Environment Manager populates these fields with information contained in the CATALINA_HOME/bin/setenv.sh file of the tc Runtime instance that you are configuring, specifically argument values defined in the JVM_OPTS environment variable.

If setenv.sh does not exist, or does not define JVM_OPTS, the Server Start fields are blank.

Edits that you make to Server Start fields in SAS Environment Manager are written back to the setenv.sh file.

### General

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Java Home</strong></td>
<td>Specifies the full pathname to the JDK or JRE used by the tc Runtime instance.</td>
</tr>
<tr>
<td><strong>Use Server HotSpot VM</strong></td>
<td>Check to use the Java HotSpot Virtual Machine.</td>
</tr>
<tr>
<td><strong>Min Heap Size</strong></td>
<td>Specifies the initial size, in MB, of the memory allocation pool.</td>
</tr>
<tr>
<td><strong>Max Heap Size</strong></td>
<td>Specifies the maximum size, in MB, of the memory allocation pool.</td>
</tr>
<tr>
<td><strong>Thread Stack Size</strong></td>
<td>Specifies the amount of memory, in KB, allocated to a single JVM thread.</td>
</tr>
</tbody>
</table>

### Sun Specific JVM Options
The options in the following table are specific to Sun JVMs. Modify the option values with caution. If you use a non-Sun VM, altering the values might have unintended side effects.

### Memory
### Field Name

<table>
<thead>
<tr>
<th><strong>Min Young Generation Size</strong></th>
<th>Specifies the default size, in MB, of the new generation.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Max Young Generation Size</strong></td>
<td>Specifies the maximum size, in MB, of the new generation.</td>
</tr>
<tr>
<td><strong>Min Perm Gen Size</strong></td>
<td>Specifies the initial size, in MB, of the permanent generation.</td>
</tr>
<tr>
<td><strong>Max Perm Gen Size</strong></td>
<td>Specifies the maximum size, in MB, of the permanent generation.</td>
</tr>
</tbody>
</table>

### Garbage Collection

<table>
<thead>
<tr>
<th><strong>Field Name</strong></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Max GC Pause</strong></td>
<td>Sends a hint to the virtual machine that pause times of the specified milliseconds or less are desired. The VM will adjust the Java heap size and other GC-related parameters in an attempt to keep GC-induced pauses shorter than the specified value.</td>
</tr>
<tr>
<td>Note: Using this field might cause the VM to reduce overall throughput, and in some cases the VM will not be able to meet the desired pause time goal.</td>
<td></td>
</tr>
<tr>
<td><strong>Max GC Minor Pause</strong></td>
<td>Similar to Max GC Pause, but for minor pauses.</td>
</tr>
</tbody>
</table>

### Debug

<table>
<thead>
<tr>
<th><strong>Field Name</strong></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Heap Dump on Out of Memory Error</strong></td>
<td>Directs the JVM to generate a heap dump when an allocation from the Java heap or the permanent generation cannot be satisfied.</td>
</tr>
<tr>
<td><strong>Print Message at GC</strong></td>
<td>Specifies whether the JVM should print messages to the GC log file every time it performs a garbage collection.</td>
</tr>
<tr>
<td><strong>Print Heap at GC</strong></td>
<td>Specifies whether the JVM should print detailed information, including heap occupancy before and after a garbage collection, to the GC log file.</td>
</tr>
<tr>
<td><strong>Print GC Application Stopped Time</strong></td>
<td>Specifies whether the JVM should print the amount of time an application is stopped during a garbage collection to the GC log file.</td>
</tr>
<tr>
<td><strong>Print GC Timestamps</strong></td>
<td>Specifies whether the JVM should print timestamps relating to garbage collection to the GC log file.</td>
</tr>
<tr>
<td><strong>Print GC Details</strong></td>
<td>Specifies whether the JVM should print detailed information relating to garbage collection to the GC log file.</td>
</tr>
<tr>
<td><strong>GC Log File</strong></td>
<td>Specifies the name of the GC log file to which all garbage collection information is printed. Default value is CATALINA_BASE/logs/gc.log.</td>
</tr>
</tbody>
</table>
Advanced

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Command Line Arguments        | Enter additional options to the CATALINA_OPTS environment variables if they are not available as text fields on this configuration page. Use one of these forms:  

  -X:OptionValue  
  or  
  -XX:Option=Value  
  with a space between options.  
  For example:  
  -Xms512M -Xmx512M -XX:NewSize=128M |

Context Container

Notes

The fields described in the following table configure the context for every web application deployed to this tc Runtime instance. SAS Environment Manager loads and updates the values from the CATALINA_BASE/conf/context.xml file for this tc Runtime instance.

Static Resource Cache

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Caching</td>
<td>If checked, specifies that tc Runtime uses the cache for static resources.</td>
</tr>
<tr>
<td>Max Cache Size</td>
<td>Maximum size, in KB, of the static resource cache. Default value is 10240 (10 megabytes).</td>
</tr>
<tr>
<td>Cache TTL</td>
<td>Amount of time, in milliseconds, between cache entries revalidation. Default value is 5000 (5 seconds).</td>
</tr>
</tbody>
</table>

Web Application Logger

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Swallow Output</td>
<td>If checked, specifies that tc Runtime will redirect the bytes outputted by the web application to System.out and System.err to the web application logger.</td>
</tr>
</tbody>
</table>

Server Defaults: JSP

The fields described in the following table configure JSP-related initialization parameters for every web application deployed to this tc Runtime instance. SAS Environment Manager loads and updates the values from the CATALINA_BASE/conf/web.xml file for this tc Runtime instance.
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recompile Check Interval (s)</td>
<td>Specifies the interval, in seconds, at which tc Runtime checks to see whether a JSP and its dependent file need to be recompiled. Default value is 0. If you set this field to a value greater than zero, and the Development Mode field is unchecked, then tc Runtime performs the compilation in the background.</td>
</tr>
<tr>
<td>Development Mode</td>
<td>Specifies that tc Runtime is working in development mode. When this value is checked, you can specify the frequency at which JSPs are checked for modification using the Modification Test Interval field.</td>
</tr>
<tr>
<td>Modification Test Interval (s)</td>
<td>Specifies the interval, in seconds, that tc Runtime should wait before checking JSPs and their dependent files for modifications. If you set this field to 0, then tc Runtime checks the JSPs every time they are accessed. Default value is 4 seconds. This feature is enabled only when Development Mode is checked.</td>
</tr>
<tr>
<td>Compiler</td>
<td>Specifies the JSPs compiler used by tc Runtime. If not set, then tc Runtime uses the default Eclipse JDT Java compiler.</td>
</tr>
<tr>
<td>Compiler Target VM</td>
<td>Specifies the JDK version with which the generated files are compatible. Default value is JDK 1.4.</td>
</tr>
<tr>
<td>Compiler Source VM</td>
<td>Specifies the JDK version with which the source files are compatible. Default value is JDK 1.4</td>
</tr>
<tr>
<td>Compile Class With Debug Information</td>
<td>Specifies whether the JSP class should be compiled with debugging information.</td>
</tr>
<tr>
<td>Classpath</td>
<td>Specifies the CLASSPATH that tc Runtime should use when compiling the generated servlets. tc Runtime creates the default CLASSPATH dynamically based on the current web application.</td>
</tr>
<tr>
<td>Fork JSP Page Compile to Separate JVM</td>
<td>Specifies whether tc Runtime should fork the compilation of JSPs so that they are performed in a separate JVM than the tc Runtime.</td>
</tr>
<tr>
<td>Enable Tag Handler Pooling</td>
<td>Enables tag handler pooling.</td>
</tr>
<tr>
<td>Internet Explorer class-id for <a href="">jsp:plugin</a></td>
<td>Specifies the class-id value that tc Runtime sends to Internet Explorer when using the tags. Default value is clsid:8AD9C840-044E-11D1-B3E9-00805F499D93.</td>
</tr>
<tr>
<td>Tags</td>
<td></td>
</tr>
<tr>
<td>Java File Encoding</td>
<td>Specifies the Java file encoding to use for generating Java source files. Default value is UTF8.</td>
</tr>
<tr>
<td>Keep Generated Source Code</td>
<td>Specifies whether tc Runtime should keep the generated source code for each page rather than deleting it.</td>
</tr>
<tr>
<td>Generate One Print Statement Per Input Line</td>
<td>Specifies whether tc Runtime should generate static content with one print statement per input line, to ease debugging.</td>
</tr>
<tr>
<td>Trim Spaces In Template Text</td>
<td>Specifies whether tc Runtime should trim white spaces in template text between actions or directives.</td>
</tr>
<tr>
<td>Suppress SMAP Information</td>
<td>Specifies whether tc Runtime should suppress the generation of SMAP information for JSR-45 debugging.</td>
</tr>
</tbody>
</table>
### Field Name
### Description

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dump SMAP Information</td>
<td>Specifies whether tc Runtime should dump SMAP information for JSR-45 debugging to a file. If you want to set this field to true (checked), then be sure to also uncheck Suppress SMAP Information.</td>
</tr>
<tr>
<td>Generate Strings as Char Arrays</td>
<td>Specifies whether strings should be generated as character arrays. Checking this field will sometimes increase the performance of JSPs.</td>
</tr>
<tr>
<td>Issue Error For Invalid useBean Class Attribute</td>
<td>Specifies whether tc Runtime should issue an error when the value of the class attribute in a useBean action is not a valid bean class.</td>
</tr>
<tr>
<td>Scratch Directory</td>
<td>Specifies the scratch directory that tc Runtime should use when compiling JSP pages. Default value is the work directory for the current web application.</td>
</tr>
<tr>
<td>Add X-Powered-By Response Head</td>
<td>Specifies whether generated servlet adds the X-Powered-By response header.</td>
</tr>
</tbody>
</table>

### Server Defaults: Static Content

Server Defaults: Static Content

The fields described in the following table configure static content-related initialization parameters for every web application deployed to this tc Runtime instance. SAS Environment Manager loads and updates the values from the `CATALINA_BASE/conf/web.xml` file for this tc Runtime instance.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Debug Level</td>
<td>Specifies the level of detail contained in the debugging messages from the current servlet. Default value is 0 (no debugging.)</td>
</tr>
<tr>
<td>File Encoding</td>
<td>Specifies the encoding that tc Runtime uses when reading static resources. The default value is the same as the file encoding of the platform on which tc Runtime is running.</td>
</tr>
<tr>
<td>Input Buffer Size</td>
<td>Specifies the size, in bytes, of the input buffer that tc Runtime uses when reading resources to be served. Default value is 2048.</td>
</tr>
<tr>
<td>Output Buffer Size</td>
<td>Specifies the size, in bytes, of the output buffer that tc Runtime uses when writing resources to be served. Default value is 2048.</td>
</tr>
<tr>
<td>Min Sendfile Size</td>
<td>Specifies the minimal file size, in KB, that tc Runtime uses with &quot;sendfile&quot;. This field only works if the connector supports sendfile. Default value is 48.</td>
</tr>
<tr>
<td>Show Directory Listings</td>
<td>Specifies whether tc Runtime should produce a directory listing if there is no welcome file in the directory. Directory listings that include many entries can be slow and consume significant proportion of the tc Runtime resources.</td>
</tr>
<tr>
<td>Readme File Name</td>
<td>Filename to display with the directory contents. No default value.</td>
</tr>
<tr>
<td>Read Only</td>
<td>Specifies whether the current context is read-only, which means that it rejects HTTP commands such as PUT and DELETE.</td>
</tr>
</tbody>
</table>
**tc Runtime JDBC Reference**

**Overview**
This page provides reference information about the fields on the Resources page of the Server Configuration page. These fields are used to configure and create JDBC data sources.

SpringSource tc Runtime provides two types of JDBC datasources: the standard DBCP one and a Tomcat datasource for highly concurrent environments. See tc Runtime Configuration Reference on page 68.

### General Properties

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>JNDI Name</strong></td>
<td>The JNDI path to which this data source is bound. By default, the JNDI name is the name of the data source.</td>
</tr>
</tbody>
</table>

### Connection Properties

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Username</strong></td>
<td>The user name that the JDBC driver uses to establish a connection to the database server.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The password that the JDBC driver uses to establish a connection to the database server.</td>
</tr>
</tbody>
</table>
| **URL**        | The connection URL that the JDBC driver uses to establish a connection to the database server. This URL varies for each type of database driver. An example for the MySQL database is:  
> jdbc:mysql://localhost:3306/javatest?autoReconnect=true |
| **Driver Class Name** | The fully qualified name of the JDBC driver class used to create the physical database connections in the connection pool. The driver class name varies for the type of JDBC driver. An example of the driver class name for connecting to a MySQL database server is:  
> com.mysql.jdbc.Driver |
| **Connection Properties** | The connection properties that tc Runtime sends to the JDBC driver when establishing new connections. Format of the string must be [propertyName=property;]  
**Note:** tc Runtime passes the “user” and “password” properties explicitly, so do not include them in this field. |

### Tomcat and DBCP Connection Pool Properties

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default Auto Commit</strong></td>
<td>Specifies whether connections created by this pool are by default in an auto-commit state.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Default Read Only</td>
<td>Specifies whether connections created by this pool are by default read only.</td>
</tr>
<tr>
<td>Default Transaction Isolation</td>
<td>Specifies the default transaction isolation state for connections created by this pool. Values can be:</td>
</tr>
</tbody>
</table>
|                                 | NONE  
|                                 | Transactions are not supported  
|                                 | READ_COMMITTED  
|                                 | Dirty reads are prevented; non-repeatable reads and phantom reads can occur.  
|                                 | READ_UNCOMMITTED  
|                                 | Dirty reads, non-repeatable reads and phantom reads can occur.  
|                                 | REPEATABLE_READ  
|                                 | Dirty reads and non-repeatable reads are prevented; phantom reads can occur.  
|                                 | SERIALIZABLE  
|                                 | Dirty reads, non-repeatable reads and phantom reads are prevented. Default value depends on the database driver. |
| Default Catalog                 | Specifies the default catalog of connections created by this pool.           |
| Initial Number of Connections   | Specifies the initial number of connections that are created when tc Runtime starts this connection pool. Default value is 0 (DBCP datasource) or 10 (Tomcat datasource). |
| Max Active Connections          | Specifies the maximum number of active connections that tc Runtime can allocate from this pool at the same time. Specify a negative number for no limit. Default value is 8 (DBCP datasource) or 100 (Tomcat datasource). |
| Max Idle Connections            | Specifies the maximum number of connections that can remain idle in the pool without any extra ones being released. Specify a negative number for no limit. Default value is 8 (DBCP datasource) or 100 (Tomcat datasource). |
| Min Idle Connections            | Specifies the minimum number of connections that can remain idle in the pool without any extra ones being created. Specify 0 to create none. Default value is 0 (DBCP datasource) or 10 (Tomcat datasource). |
| Max Wait Time For Connection Borrow | The maximum number of milliseconds that the connection pool waits (when there are no available connections) for a connection to be returned before throwing an exception. Specify -1 to wait indefinitely. Default value is -1 (DBCP datasource) or 30000 (Tomcat datasource). |
| Validation Query                | The SQL query that the driver uses to validate connections from this pool before returning them to the caller. If specified, this query MUST be an SQL SELECT statement that returns at least one row. |
| Test on Borrow                  | Specifies whether tc Runtime validates objects before being borrowed from the pool. If the object fails to validate, tc Runtime drops it from the pool and attempts to borrow another.  
<p>|                                 | Note: for a value in this field to have any effect, you must set the <strong>Validation Query</strong> field to a non-null string. |
| Test on Return                  | Specifies whether tc Runtime validates objects before returning them to the connection pool. |</p>
<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test While Idle</td>
<td>Specifies whether the idle object evictor validates objects. If an object fails to validate, tc Runtime drops it from the connection pool. <strong>Note:</strong> for a value in this field to have any effect, you must set the Validation Query field to a non-null string.</td>
</tr>
<tr>
<td>Time Between Eviction Runs</td>
<td>The number of milliseconds to sleep between runs of the idle object evictor thread. When non-positive, tc Runtime does not run an idle object evictor thread. Default value is -1 (DBCP datasource) or 5000 (Tomcat datasource).</td>
</tr>
<tr>
<td>Test Per Eviction Runs</td>
<td>The number of objects to examine during each run of the idle object evictor thread (if any). Default value is 3.</td>
</tr>
<tr>
<td>Min Evictable Idle Time</td>
<td>The minimum amount of time, in milliseconds, that an object can sit idle in the pool before it is eligible for eviction by the idle object evictor (if any).</td>
</tr>
<tr>
<td>Pool Prepared Statements</td>
<td>Enables prepared statement pooling for this connection pool.</td>
</tr>
<tr>
<td>Max Opened Prepared Statements</td>
<td>The maximum number of open statements that can be allocated from the statement pool at the same time. Set this field to 0 for no limit. Default value is 0.</td>
</tr>
<tr>
<td>Allow Access to Underlying Connection</td>
<td>Specifies whether the PoolGuard allows access to the underlying connection.</td>
</tr>
<tr>
<td>Remove Abandoned Connections</td>
<td>Specifies whether tc Runtime should remove abandoned connections if they exceed the value of the Remove Abandoned Timeouts field. If checked, a connection is considered abandoned and eligible for removal if it has been idle longer than the value of Remove Abandoned Timeouts. Checking this field can recover database connections from poorly written applications which fail to close a connection.</td>
</tr>
<tr>
<td>Remove Abandoned Timeouts</td>
<td>Specifies the amount of time, in seconds, before tc Runtime can remove an abandoned connection. Default value is 300 seconds.</td>
</tr>
<tr>
<td>Log Abandoned Statements and Connections</td>
<td>Specifies whether tc Runtime should log stack traces for application code that abandoned a Statement or Connection. <strong>Note:</strong> Logging of abandoned statements and connections adds overhead for every connection open or new statement, because a stack trace has to be generated.</td>
</tr>
<tr>
<td>Validation Interval (ms)</td>
<td>Tomcat datasource only. Specifies the time, in milliseconds, that tc Runtime waits before running a validation check to ensure that the JDBC connection is still valid. Too frequent validation checks can slow performance. Default value for this field is 30000 (30 seconds).</td>
</tr>
<tr>
<td>Fair Queue</td>
<td>Tomcat datasource only. Specifies that calls to getConnection() should be treated fairly in a true FIFO (first in, first out) fashion. You are required to enable this feature if you want to use the asynchronous connection retrieval feature, which is the ability to queue your connection request.</td>
</tr>
<tr>
<td>JMX Enabled</td>
<td>Tomcat datasource only. Specifies whether the connection pool is registered with the JMX server.</td>
</tr>
<tr>
<td>Use equals comparison</td>
<td>Tomcat datasource only. Specifies whether the ProxyConnection class should use String.equals() instead of == when comparing method names. Does not apply to added interceptors as those are configured individually.</td>
</tr>
</tbody>
</table>
Init SQL

Tomcat datasource only. Specifies an initial SQL statement that is run only when a connection is first created. You can use this feature to set up session settings that you want to exist during the entire time the connection is established.

JDBC Interceptors

Tomcat datasource only. Semi-colon separated list of classnames that tc Runtime inserts as interceptors in the chain of operations on the java.sql.Connection object. The interceptor classes must extend the abstract class:

org.apache.tomcat.jdbc.pool.JdbcInterceptor

SpringSource tc Runtime provides a JDBC Interceptor called SlowQueryReportJmx that keeps a report of slow JDBC queries, or JDBC queries that did not complete below a configured time threshold. If you want AMS to display this report in its Console, then you must add the SlowQueryReportJmx interceptor to this text field. For example, to add it to the default interceptors, enter this value:

ConnectionState;StatementFinalizer;SlowQueryReportJmx

The default threshold for the SlowQueryReportJmx interceptor is 5000 milliseconds. If you want to change the default value, include it as a parameter to the interceptor, as shown:

ConnectionState;StatementFinalizer;SlowQueryReportJmx(threshold=6000)

After you have configured the SlowQueryReportJmx interceptor, AMS creates and auto-discovers a service called "JDBC Query Report" that contains information about slow JDBC queries.

tc Runtime Services Reference

Overview

This page defines the fields on the Services page on the Server Configuration page that are used to configure and create tc Runtime services.

A tc Runtime service represents the combination of one or more Connector components that share a single Engine component for processing incoming requests. A tc Runtime consists of one or more services. The default tc Runtime service which is always present in newly created tc Runtime instance is called "catalina."

General Service Properties

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the name of this tc Runtime service. Within the scope of a tc Runtime, the service name must be unique. This is the name that appears in the tc Runtime log messages.</td>
</tr>
</tbody>
</table>

Connector Properties

General

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Protocol</td>
<td>Specifies the protocol that handles incoming and outgoing messages for this connector. This field can have the following values: org.apache.coyote.http11.Http11Protocol (same as HTTP/1.1)</td>
</tr>
<tr>
<td></td>
<td>This is the default value. Note that if you want to use HTTPS, you do not specify &quot;HTTPS/1.1&quot;, but rather, set the secure field to true.</td>
</tr>
<tr>
<td></td>
<td>non-blocking Java connector</td>
</tr>
<tr>
<td></td>
<td>the APR connector.</td>
</tr>
<tr>
<td>IP Address</td>
<td>For tc Runtime instances with more than one IP address, this attribute identifies a single address, upon which the listen port defined in the Port attribute will be opened for connections. If a specific IP address is not specified, server sockets will be created on all IP addresses associated for the server, on the port specified in the Port attribute.</td>
</tr>
<tr>
<td>Port</td>
<td>Specifies the TCP port number on which this connector will create a server socket and await incoming connections. Your operating system allows only one server application to listen to a particular port number on a particular IP address, which means that multiple tc Runtime instances running on the same computer must have unique ports. Default value is 8080.</td>
</tr>
<tr>
<td>Accept Count</td>
<td>HTTP(S) Connectors only. Specifies maximum queue length for incoming connection requests when all possible request processing threads are in use. Any requests received when the queue is full will be refused. The default value is 10.</td>
</tr>
<tr>
<td>Max Keep Alive Requests</td>
<td>HTTP(S) Connectors only. Specifies the maximum number of HTTP requests that can be pipelined until the connection is closed by the server. A value of 1 disables HTTP/1.0 keep-alive, as well as HTTP/1.1 keep-alive and pipelining. A value of -1 allows an unlimited amount of pipelined or keep-alive HTTP requests. The default value of this field is 100.</td>
</tr>
</tbody>
</table>
| Proxy Host        | If this connector is being used in a proxy configuration, specifies the server name that is returned from calls to request.getServerName().
| Proxy Port        | If this connector is being used in a proxy configuration, specifies the server port that is returned from calls to request.getServerPort(). |
| Redirect Port     | Specifies the port to which a user is redirected if they require a secure connection. If this connector supports non-SSL requests, and a request is received for which a matching requires SSL transport, tc Runtime automatically redirects the request to the port number specified here. |
| Scheme            | Specifies the name of the protocol that you want to have returned by calls to request.getScheme(). For example, set this field to "https" for an SSL Connector. The default value is "http". |
| Connection Timeout | Specifies the number of milliseconds this connector waits, after accepting a connection, for the request URI line to be presented. The default value is 60000 (60 seconds). |
| Max Threads       | Specifies the maximum number of request processing threads that this connector creates, which in turn determines the maximum number of simultaneous requests that can be handled. If an executor is associated with this connector, tc Runtime ignores this attribute as the connector will execute tasks using the executor rather than an internal thread pool. The default value of this field is 40. |
| Request Secret Keyword | Specifies that only requests from workers with this secret keyword will be accepted.                                                                                                               |
Use Request Secret Keyword

Specifies whether tc Runtime should generate a random value for the Request Secret Keyword field.

Security and SSL

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure</td>
<td>Specifies whether you want user calls to request.isSecure() to return true for requests received by this connector. Check this field for connectors (both SSL and non-SSL) that receive data from an SSL accelerator, like a cryptographic card, an SSL appliance or even a web server.</td>
</tr>
<tr>
<td>Enable SSL</td>
<td>Enables SSL traffic (handshake/encryption/decryption) for this connector. When enabled, be sure to also set the &quot;scheme&quot; and &quot;secure&quot; attributes so that correct values are returned to user calls to request.getScheme() and request.isSecure().</td>
</tr>
<tr>
<td>Certificate Encoding Algorithm</td>
<td>Specifies the certificate encoding algorithm. The default value is the Sun implementation (SunX509). For IBM JVMs use the value IbmX509. For other vendors, consult the JVM documentation for the correct value.</td>
</tr>
<tr>
<td>Keystore File</td>
<td>Specifies the pathname of the keystore file that contains the server certificate to be loaded. By default, the pathname is the file &quot;.keystore&quot; in the operating system home directory of the user that starts the tc Runtime instance.</td>
</tr>
<tr>
<td>Keystore Password</td>
<td>Specifies the password used to access the server certificate from the specified keystore file. The default value is &quot;changeit&quot;.</td>
</tr>
<tr>
<td>Key Alias</td>
<td>Specifies the alias that tc Runtime uses when accessing the server certificate in the keystore. If not specified, tc Runtime uses the first key read in the keystore.</td>
</tr>
</tbody>
</table>

APR SSL Settings

These settings are relevant only for APR-based connectors that also use SSL.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL Protocol</td>
<td>Specifies the protocol that tc Runtime might use to communicate with clients. Valid values are &quot;SSLv2&quot;, &quot;SSLv3&quot;, &quot;TLSv1&quot;, and &quot;SSLv2+SSLv3&quot;. Default value is &quot;all&quot;.</td>
</tr>
<tr>
<td>SSL Cipher Suite</td>
<td>Specifies the ciphers that tc Runtime might use to communicate with clients. Valid values is a list of ciphers, separated by a colon. Default value is &quot;all&quot;. See the OpenSSL website for the list of valid ciphers.</td>
</tr>
<tr>
<td>SSL Certificate File</td>
<td>Specifies the name of the file that contains the server certificate. The format is PEM-encoded.</td>
</tr>
<tr>
<td>SSL Certificate Key File</td>
<td>Specifies the name of the file that contains the server private key. The format is PEM-encoded. The default value is the value of the SSL Certificate File field, which implies that both the certificate and the private key are in the same file. For security reasons, this is not recommended.</td>
</tr>
<tr>
<td>SSL Password</td>
<td>Specifies the password for the encrypted private key. If this field is left blank, the callback function prompts for the password.</td>
</tr>
</tbody>
</table>
SSL Verify Client
Specifies whether tc Runtime should ask client for certificate. The default value is "none", which means that the client will not have the opportunity to submit a certificate. Other valid values include "optional", "require" and "optionalNoCA".

SSL Verify Depth
Specifies the maximum verification depth for client certificates. The default value is "10".

SSL CA Certificate File
Specifies the single file where you assemble the certificates of Certification Authorities (CA) for the clients that you authenticate. The file is the concatenation of the various PEM-encoded Certificate files, in order of preference.

SSL CA Certificate Path
Specifies the directory where you keep the Certificates of Certification Authorities (CAs) for the clients that you authenticate. These are used to verify the client certificate on Client Authentication.

The files in this directory must be PEM-encoded and are accessed through hash filenames. Typically, you cannot place Certificate files in this directory, but you also have to create symbolic links named hash-value.N. And you should always make sure this directory contains the appropriate symbolic links. Use the Makefile, which comes with mod_ssl, to accomplish this task.

SSL Certificate Chain File
Specifies the optional all-in-one file where you can assemble the certificates of Certification Authorities (CA) which form the certificate chain of the server certificate. This starts with the issuing CA certificate of the server certificate and can range up to the root CA certificate. Such a file is simply the concatenation of the various PEM-encoded CA Certificate files, usually in certificate chain order.

SSL CA Revocation File
Specifies the directory where you keep the Certificate Revocation Lists (CRL) of Certification Authorities (CAs) whose clients you deal with. These are used to revoke the client certificate on Client Authentication.

SSL CA Revocation Path
Specifies the directory where you keep the Certificate Revocation Lists (CRL) of Certification Authorities (CAs) whose clients you deal with. These are used to revoke the client certificate on Client Authentication.

Engine Properties
A tc Runtime engine represents the entire request processing machinery associated with a particular service. It receives and processes all requests from one or more connectors, and returns the completed response to the connector for ultimate transmission back to the client.

Each Service must be associated with exactly one engine.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the name of this service. This is the name used in tc Runtime logging messages. Each service name must be unique within the scope of a tc Runtime instance.</td>
</tr>
<tr>
<td>Default Host</td>
<td>Specifies the default host name. This name corresponds to the name of a Host component that processes requests directed to host names on this server, but which are not explicitly configured for this tc Runtime instance.</td>
</tr>
<tr>
<td>JVM Route</td>
<td>Specifies the identifier that must be used in load balancing scenarios to enable session affinity. The identifier, which must be unique across all tc Runtime instances that participate in a cluster, is appended to the generated session identifier, therefore allowing the front end proxy to always forward a particular session to the same tc Runtime instance.</td>
</tr>
</tbody>
</table>
Thread Diagnostics

When you deploy and start a web application on a tc Runtime instance, and then clients begin connecting and using the application, you might find that the clients occasionally run into problems such as slow requests or even failed requests. Although tc Runtime by default logs these errors in the log files, it is often difficult to pinpoint where exactly the error came from and how to go about fixing it. By enabling thread diagnostics, tc Runtime provides additional information to help you troubleshoot the problem.

A failed request is one that simply did not execute; a slow request is defined as a request that takes longer than the configured threshold. The default threshold is 500 milliseconds.

When you enable thread diagnostics, you can view the following contextual information about a slow or failed client request:

- The time and date on which the slow or failed request happened.
- The exact URL invoked by the client that resulted in a slow or failed request.
- The exact error returned by the request.
- The database queries that were executed as part of the request and how long each one took.
- Whether any database connection failed or succeeded.
- Whether the database had any other connectivity problems.
- Whether the database connection pool ran out of connections.
- Whether any garbage collection occurred during the request, and if so, how long it took.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Thread Diagnostics</td>
<td>Enables the gathering of thread diagnostic information. To view this information after you have enabled thread diagnostics, go to the Monitor tab of a particular tc Runtime instance and then click on servername Thread Diagnostics in the Services window.</td>
</tr>
<tr>
<td>History</td>
<td>Specifies the maximum number of requests that have met the threshold condition that tc Runtime keeps as historical data. The default value is 1000. You can query this historical data using JMX; it is not presented in SAS Environment Manager.</td>
</tr>
<tr>
<td>Threshold</td>
<td>Specifies the threshold, in milliseconds, after which a client request is considered slow. The default value is 5000 milliseconds.</td>
</tr>
</tbody>
</table>

Host Properties

A tc Runtime Host represents a virtual host, which is an association of a network name for a tc Runtime (such as "www.mycompany.com" associated with the particular tc Runtime). To be effective, the network name must be registered in the Domain Name Service (DNS) server that manages the Internet domain to which you belong.

A tc Runtime engine must be associated with one or more hosts. One of the hosts must be the default host, or the one pointed to by the Default Host field of the Engine configuration.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the network name of this virtual host, as registered in your Domain Name Service (DNS) server. One of the hosts associated within a tc Runtime engine MUST have a name that matches the Default Host field for that engine.</td>
</tr>
</tbody>
</table>
**Application Base Directory**
Specifies the application base directory for this virtual host. The application base directory can contain web applications to be deployed on this virtual host. You can specify an absolute pathname for this directory, or a pathname that is relative to the $CATALINA_BASE directory.

**Auto Deploy Web Applications**
Specifies whether new web applications that are copied to the application base directory while tc Runtime is running should be automatically deployed.

**Deploy Applications on Startup**
Specifies whether web applications from this host should be automatically deployed when the tc Runtime instance starts.

**Unpack WARs**
Specifies whether tc Runtime should unpack web applications that are copied to the application base directory as web application archive (WAR) files into a corresponding disk directory structure. If unchecked, tc Runtime runs the web applications directory from a WAR file.

**Deploy XML**
Specifies whether tc Runtime should parse the "context.xml" file embedded inside the web application (located at /META-INF/context.xml). Security conscious environments should set this to false (uncheck) to prevent applications from interacting with the container's configuration. The administrator will then be responsible for providing an external context configuration file, and put it in $CATALINA_BASE/conf/enginename/hostname/.

**Work Directory**
Specifies the pathname to a scratch directory used by applications for this host. Each application will have its own sub directory with temporary read-write use. Configuring a Context work directory overrides use of the Host work directory configuration. This directory will be made visible to servlets in the web application by a servlet context attribute (of type java.io.File) named javax.servlet.context.tempdir as described in the Servlet Specification. If not specified, a suitable directory underneath $CATALINA_BASE/work will be provided.

**HTTP Access Logging**
The tc Runtime logging subsystem creates log files in the same format as those created by standard web servers. These logs can later be analyzed by standard log analysis tools to track page hit counts, user session activity, and so on. The logging files are rolled over nightly at midnight.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Logging</td>
<td>Specifies whether you want to enable logging on this engine or virtual host.</td>
</tr>
<tr>
<td>Directory</td>
<td>Specifies the absolute or relative pathname of a directory in which tc Runtime creates the log files log files. If you specify a relative pathname, it is relative to $CATALINA_BASE. The default value is $CATALINA_BASE/logs.</td>
</tr>
<tr>
<td>Pattern</td>
<td>A formatting layout identifying the various information fields from the request and response to be logged, or the word &quot;common&quot; or &quot;combined&quot; to select a standard format. Note that the optimized access does only support &quot;common&quot; and &quot;combined&quot; as the value for this attribute.</td>
</tr>
<tr>
<td>File Name Prefix</td>
<td>Specifies the prefix added to the start of each log file's name. The default value is &quot;access_log.&quot; Leave the field blank if you do not want a prefix.</td>
</tr>
<tr>
<td>File Name Suffix</td>
<td>Specifies the suffix added to the end of each log file's name. Leave the field blank if you do not want a suffix (default behavior).</td>
</tr>
</tbody>
</table>
File Date Format

Specifies a customized date format in the access log filename. The date format also specifies how often the file is rotated. For example, if you want the log files to rotate every hour, then set this value to: yyyy-MM-dd.HH

tc Server Client

To go to the download page for the tc Server Command-line Interface (CLI), click tc Server Command-line Interface in the Plugins section of the SAS Environment Manager Administration.

You can use the CLI to perform configuration and application deployment tasks on individual or groups of tc Server instances that are managed by SAS Environment Manager.

Advanced Topics

Plug-ins: Introduction

To initiate plug-in management tasks for SAS Environment Manager, use the Plugins section of the Manage page.

TIP This documentation uses the term native to identify features that are internal to this application but could be confused with their suite-level counterparts. For example, native roles are wholly internal to this application and distinct from metadata-layer application roles.

The following links provide access to detailed information and instructions.

See Also

Relationship to VMware Hyperic on page 2

Plug-ins: Management

Introduction

To access the Plug-in Manager page, open the Manage page and click Plug-in Manager (in the Server Settings section).

This page provides deployment-wide management of product plug-ins. It displays all of the plug-ins that are deployed to the server. For all up-to-date agents that are reporting to the server, a summary of deployment status is provided.

You can use this page to deploy new or updated plug-ins and to remove plug-ins from agents.

Note: You can administer plug-ins only on agents that are the same or later version than the server.

Page Contents

This page lists all of the resource plug-ins that are deployed to the server.

In the upper right corner, a message indicates how many of the agents reporting to the server support the Server Agent Plug-in Synchronization (SAPS) feature, and the total number of agents reporting to the server.

For any agents that do not support SAPS, the message is a link.
The following information is listed for each plug-in:

**Plug-in**
The name of the plug-in. You cannot change or remove system plug-ins.

A **File Not Found** message in this column indicates that the plug-in file or archive has been manually removed from the server's plug-ins directory. To remove the resources that were defined by the plug-in, select the plug-in’s check box, and click **Remove Selected Plugin**

**TIP** The best practice approach to removing plug-ins is to use the Plug-in Manager page, because this also removes the resources that are managed by the plug-in.

**Version**
The version of the server in which the plug-in was distributed.

**Filename**
The name of the archive or file that contains the plug-in.

**Added Time**
When the plug-in was first deployed to the server.

**Updated Time**
When the plug-in was most recently redeployed to the server.

**Agent Sync Status**
Summarizes the deployment status of the plug-in on up-to-date agents that are reporting to the server. Deployment status can be any of the following:

- ![checkmark] If this icon is present, the value next to it indicates the number of agents to which the plug-in is deployed.
- ![cloud] If this icon is present, the value next to it indicates the number of agents on which deployment has been initiated and is still in progress.
- ![warning] if this icon is present, the value next to it indicates the number of agents on which deployment failed

**Agents That Are Not Synchronizing**
If one or more agents that are reporting to the server are not synchronizing plugs, click the link in the upper right of the page (the link that indicates how many agents are synchronizing). See Plug-ins: Troubleshooting on page 86.

**Agent Synchronization Details**
If plug-in deployment is in progress or failed for one or more agents, the **Agent Sync Status** links to the **Agent Status** page. That page lists the agents upon which deployment is in progress or failed, and indicates the status of each.

If deployment of a plug-in to an agent fails, check the server's log file (at ServerHome/logs/server.log) for the following message:

```
agent-id=<id>, address=<addr>, port=<port> has checked in the exact same plug-in set twice in a row. To avoid any potential issues on the agent which may cause it to continuously restart the Server will sync the agent's plugin repository but will not restart it. Depending on the state of the agent it may take up to two successful agent restarts in order for the agent's plugin to be successfully synced with the Server.
```
If the preceding message appears in `ServerHome/logs/server.log`, restart the agent twice. Upon the second restart, plug-in deployment should succeed.

**Uploading Plug-ins**

**Note:** You can upload only plug-ins that are less than 5 megabytes and that comply with plug-in naming conventions.

When you upload a plug-in, the following results occur:

- The plug-in is deployed to custom plug-in directory on the server.
- The plug-in is deployed to each up-to-date agent that is reporting to the server.
- Any agents to which the plug-in is deployed are automatically restarted.

To upload a new plug-in (or a new version of a plug-in):

1. On the **Plugin Manager** page, click **Add/Update Plugin**.
2. On the **Upload** page, click **Browse** to browse the file system for the plug-in `.jar` or `.xml` file.
3. Click **Upload**.

**Removing Plug-ins**

When you remove a plug-in, the following results occur:

- The plug-in is deleted from its plug-in directory on the server.
- All resources that were defined and managed by the plug-in are removed from inventory.
- The plug-in is removed from the plugin directory of each up-to-date agent that is reporting to the server. Any agents from which the plug-in is removed are automatically restarted.

To remove plug-ins:

1. On the **Plugin Manager** page, select the check box of each plug-in that you want to remove.
2. Click **Remove Selected Plugin(s)**.
3. On the **Confirm Remove** page, click **Remove**.

**See Also**

- About the Manage Page on page 122
- Plug-ins: Introduction on page 84

**Plug-ins: Troubleshooting**

The **Out-of-date installed Agents** popup lists the name and version of each agent that is reporting but not synchronizing plug-ins.

There are two main reasons an agent might not synchronize with the server:

- The agent is an older version than the server. Agents should be the same version as the server (or more current than the server). Agents that are out of date are listed in the first table in the **Out-of-date installed Agents** popup. To solve the problem, upgrade the agent.
- The agent is not available. For example, the agent start up might be incomplete or might have failed. Agents that are up-to-date but not synchronizing are listed in the second table on the **Out-of-date installed Agents** popup. If an agent remains on this list for more than a few minutes, restart it.
Groovy Console

This page enables you to run Groovy code directly in the server. This provides low-level interactions (for example, doing advanced scripting, clearing caches, and diagnosing issues). The Groovy console is available to administrators only.

To run a Groovy script:

1. Enter the script in the text box or click the name of a script template (just above the text box).

   **Script Templates**

<table>
<thead>
<tr>
<th>Script Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>database_locks</td>
<td>Indicates what is happening in the database (what queries are currently being run)</td>
</tr>
<tr>
<td>aiApprove</td>
<td>Adds all the platforms that are in the auto-inventory queue (auto-discovery) to the inventory. This is a batch approach to a task that is performed interactively in the Auto-Discovery portlet. See Auto-Discovery Portlet on page 9. This provides an easy and quick method for adding multiple platforms to the inventory.</td>
</tr>
</tbody>
</table>

2. Click **Execute**.

   The script is executed in the same process as the server code and the results are displayed immediately below.

Web Services API

HQApi is SAS Environment Manager's built-in web services API. This API enables programmatic and command line access to SAS Environment Manager Server features and data.

To download HQApi, click **Web Services API** in the **Plug-ins** section of the **Manage** page.

The HQApi package includes the following items:

- The hqapi-client-n.n.n.jar client library and support JAR files.
- The XSD that defines the web service.
- Javadoc documentation for HQApi.

The HQApi supports the following methods of interaction:

- Programmatic access through the Java API.
- Script-based access using command line tools.

System Commands

**Introduction and Queries**

The **Live Exec** view enables you to run system commands on a managed platform or a group of platforms.
This view uses SIGAR (an API for gathering system information in real time).
The following table describes the queries that you can run:

**Queries**

<table>
<thead>
<tr>
<th>Command</th>
<th>Data That is Returned</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpuinfo</td>
<td>All CPUs on a platform.</td>
</tr>
<tr>
<td>cpuperc</td>
<td>Usage percentages on each CPU and related data. Equivalent to the <code>uptime</code> command.</td>
</tr>
<tr>
<td>df</td>
<td>All filesystems on a platform. This does not list disk-usage percentages.</td>
</tr>
<tr>
<td>ifconfig</td>
<td>Network statistics on each of the platform's network interfaces</td>
</tr>
<tr>
<td>netstat</td>
<td>Active socket connections on the platform</td>
</tr>
<tr>
<td>top</td>
<td>All processes (that the SAS Environment Manager Agent can see) running on the platform. If a process is not listed, it is most likely because the Agent does not have permission to see it.</td>
</tr>
<tr>
<td>who</td>
<td>Logged-in users</td>
</tr>
</tbody>
</table>

**Instructions**

To run Live Exec:

1. On the **Resource** page, navigate to a platform or a group of platforms.
2. On the **Views** tab, click **Live Exec**.
3. Select a command from the Please select a query to run drop-down list.

Command results are displayed on the right side of the page.

If the resource is a group:

- If a member of the group has not previously been selected, click 🗝 next to a specific platform. That platform will be displayed first by default for subsequent commands.
- If a member of a group is not available, 🛠 is displayed next to the resource. Click the icon to view the reason why it is unavailable.
- To view the real-time data for another platform in the group, click 🗝 next to that platform. The platform for which data is currently being displayed is highlighted at the left.

**Note:** If the agent cannot reach the platform, an error message is displayed.

**SAS Health**

The SAS Health view enables you to view information about the hardware and services on your system.

To access the SAS Health view, select a SAS Application Server Tier platform from the Resources page. On the Details page for the platform, select Views ➔ **SAS Health**.
On the SAS Health View page, select a platform from the menu. The page contains this information for the selected platform:

**Hardware**
- contains a summary of the hardware characteristics, such as CPU speed, free memory, and average load.

**Top**
- lists information about the processes that are consuming the most resources on the SAS system.

**System**
- contains a summary of operating system parameters, such as maximum user processes, data segment size, and stack size.

**Network**
- contains network addresses for the default gateway, IP address, primary DNS and secondary DNS.

**Mounts**
- lists information about the file and NFS mounts on the system.

**Servers**
- Contains a list and count of each server type on the platform.

**Services**
- Contains a list and count of each service type on the servers on the platform.

**Logs**
- contains the log file location for each server type on the platform. If log tracking has not been enabled or a log location has not been set for a server, that information is noted instead of the log location.

**Control Actions**
- contains a list of the most recent control actions that have been attempted in response to resource alerts. The table lists information about the action, whether it was successful, and any messages that were issued. The Control Schedule tab lists any control actions that are scheduled.

**SAS**
- contains properties and corresponding values for IOM and mid-tier servers and information about the time remaining until the SAS license expires and terminates on the platform.

Click **Snapshot System** to save the system information to a file.

Select the **Include Setinit** check box to set the product license information.

**JMX Mbean Browser**

**Using JMX MBean Query**
The JMX MBean Query tool enables you to search for MBeans, display their attributes, and invoke selected MBean operations on them.

When SAS Environment Manager alerts you of availability or health issues with a JVM resource or service, you can use the JMX MBean Query tool to troubleshoot and resolve the problem.

The MBean attributes displayed in the JMX MBean Query tool are read-only; the console does not support attribute editing. In this version of SAS Environment Manager, support for MBean operations is limited to operations with one or no arguments of primitive or simple type.

The JMX MBean Query tool is available on the Views tab when you have a JVM selected in SAS Environment Manager. These instructions assume that your JVM is in the inventory.

Note that JVMs are not auto-discovered by SAS Environment Manager. You must add a JVM to inventory and configure it for monitoring.
Entering Query Options

To access specific MBean attributes and operations, you enter search patterns in the text boxes in the JMX MBean Query tool page:

Object Name Pattern
To specify the MBean or MBeans of interest, enter a valid MBean object name pattern. For information about object name patterns, see http://download.oracle.com/javaee/1.4/api/javax/management/ObjectName.html.

Attribute Regex Filter
To restrict the attributes returned, enter a valid Java regular expression. For information about Java regex patterns, see http://download.oracle.com/javase/1.4.2/docs/api/java/util/regex/Pattern.html.

Operation Regex Filter
To restrict the MBean operations returned, enter a valid Java regular expression.

Click Query MBeans to execute the search.

For MBeans whose object name matches the Object Name Pattern, attributes and operations that match your filter criteria will be listed.

Enabling Automatic Refresh

If you want the console to periodically refresh the attribute values, select an interval from the Refresh Interval pulldown.

Defining Saved Mbean Searches

If you expect to perform the same search frequently, you can create an XML file that specifies the search criteria. You name the file according to a predefined convention, and store it in a specific directory in your SAS Environment Manager Server installation. Each saved search will appear in the MBean Query page's Preset Searches menu.

When you run a saved search, the values that you defined for the search Object Name Pattern, Attribute Regex Filter, and Operation Regex Filter appear in the text boxes at the top of the view.

Create a saved search and save it using the naming convention SearchID-filter.xml

SearchID is a meaningful name for the search to which you append "-filter.xml" to identify the search

The filters values defined in this file will then appear in the Preset Searches menu and will be named according to the filter ID. Save the file in the ServerHome/hq-engine/hq-server/webapps/ROOT/hqu/jmx/conf directory.

The following topics defines the XML schema for saved MBean searches.

Schema for JMX Search Criteria

A saved MBean search criteria consists of a top-level filters element, containing at least one filter sub-element. Each filter sub-element consists of:

- An ID attribute containing an identifier for the search. This string will appear in the Preset Searches menu. Each search that you define and save on an SAS Environment Manager server must have a unique ID attribute.
- An objectName sub-element, whose value is the object name pattern used for the MBean query.
- An attributeRegex sub-element, whose value is the Java regular expression used to filter the attributes returned from the MBean query.
- An operationRegex sub-element, whose value is the Java regular expression used to filter the operations returned from the MBean query.
For example:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<filters>
  <filter id="JVM Memory MBean">
    <objectName>java.lang:type=Memory</objectName>
    <attributeRegex>.*Usage</attributeRegex>
    <operationRegex>.*</operationRegex>
  </filter>
  <filter id="JVM Platform MBeans">
    <objectName>java.lang:*</objectName>
    <attributeRegex>.*</attributeRegex>
    <operationRegex>.*</operationRegex>
  </filter>
</filters>
```

## Diagnostics for Auto-Discovery

### Introduction

The **Health** page is available from the **Plug-ins** section of the **Manage** page. It displays real-time server diagnostics.

### Key Statistics

The top of the page displays standard health statistics for a server.

### Diagnostics Tab

This tab contains the information that SAS Environment Manager prints to log files every 15 minutes. You can choose the following diagnostics from the drop-down list:

- **Agent Synchronizer**
  - Lists the agents (up to 10 of them) that have done the most metric scheduling, unscheduling, and plugin synchronization jobs since the most recent restart of the server. The number of jobs of each type that the agent has run is shown.

- **Batch Aggregate AvailabilityInserter**
  - Status of the queue that contains resource availability data to be stored in the database.

- **Batch Aggregate DataInserter**
  - Status of the queue that contains resource metrics to be stored in the SAS Environment Manager database.

- **EhCache**
  - Size, hits, and misses for SAS Environment Manager cache regions.

- **Enabled Metrics Not Coming In**
  - Lists up to 10 platforms for which enabled metrics (for the platform, or resources running on the platform) were not reported during the past 60 minutes. For each such platform, the number of unreported metrics is listed, along with the internal ID for the metric, metric name (if known), the internal ID for the resource with the unreported metric, and the resource name. Only metrics for resources that (1) have been configured for monitoring, if necessary, and (2) are currently available, will be included in this diagnostic.

- **Metric Reports Stats**
  - A running average of how fast metrics are being pushed into the database.

- **ZEvents**
  - Status of the internal BUS.
**Cache Tab**
This tab displays the detailed status of cache regions, including total memory usage of all cached objects. For each region, size, hits, misses, limit and memory usage information is provided.

**Load Tab**
This tab displays the current load on the SAS Environment Manager server, including the following:
- Metrics collected per minute
- Platforms
- CPUs
- Agents
- Active Agents
- Servers
- Services
- Applications
- Roles
- Users
- Active Alert Defs
- Resources
- Resource Types
- Groups
- Escalations
- Active Escalations

**Database Tab**
The Database tab contains an Actions menu with database cleanup commands, and a Query menu with queries that return information about resources in the auto-inventory queue and resources that are orphaned.

You can perform the following database cleanup commands from the Actions menu:

**Purge AIQ Data**
Deletes the contents of the auto-discovery queue. This is useful if the queue contains resources that for some reason cannot be imported. Deleting resources from the queue will cause the agent to rediscover them.

**Purge Stalled Executions**
Deletes escalations that are stalled.

You can run the following queries from the Queries menu:
- AutoInventory IPs
- AutoInventory Platforms
- AutoInventory Servers
- Database Character Set
- Orphaned Alert Definition Count
- Orphaned Audit Count
- Orphaned (Stalled) Escalations
- Orphaned Group Count (deprecated)
- Orphaned Platform Count
- Orphaned Resource Group Count
- Orphaned Resource Count (deprecated)
- Orphaned Server Count
- Orphaned Service Count
- Postgres Locks
- Postgres Activity
- Active But Disabled Resource Alert Defs
- Database Version Information

**Agents Tab**

For each SAS Environment Manager Agent connected to the SAS Environment Manager Server, the following information is listed:

**FQDN**
- of the machine that it runs on; this is the identifier of the monitored platform in SAS Environment Manager.

**Address**
- The IP address upon which the agent listens for server communications.

**Port**
- The port on the agent's listen address upon which it listens for server communications. By default, the listen port is 2144. The value "-1" indicates that the agent is configured for unidirectional communications.

**Version**
- SAS Environment Manager version

**Bundle Version**

**Creation Time**
- When the platform where the agent runs was first added to SAS Environment Manager inventory.

**# Platforms**
- The number of platforms the agent is monitoring. Typically, this value is "1", indicated that the agent is monitoring only the platform where it runs. The value is greater than 1 if the agent is also monitoring an agentless device (such as an SNMP device).

**# Metrics**
- This is the number of metrics the agent collects. SAS Environment Manager recommends balancing the metric collection load across agents. For example, do not use a single agent to monitor every SNMP devices in your network - this would constitute a single point of failure, and the metric load might downgrade the performance of other services running on the host.

**Time Offset (ms)**
- The system time offset between SAS Environment Manager Server and SAS Environment Manager Agent. Time synchronization on SAS Environment Manager Server and SAS Environment Manager Agents is very important to determine the availability of platforms and services correctly. Single or double digit values are okay. Higher values indicate a problem. In this case, set up NTP-daemons on your server and agent hosts. You can monitor the NTP-daemons and set an alert on the offset value

**License count**
Maintenance Tab

The Maintenance tab has commands for listing and removing orphaned resources. Interrupted database updates can result in orphaned rows in the SAS Environment Manager database. Orphaned rows can cause SAS Environment Manager exceptions. For example, if the SAS Environment Manager database contains alert definitions that are no longer associated with a resource, attempting to edit a resource type alert can result in a stack trace that is similar to the following:

```org.hyperic.hq.events.AlertConditionCreateException:
org.hyperic.hq.measurement.MeasurementNotFoundException: No measurement found
for 10288 with template 33434 at ...
```

Cleanup Orphaned Nodes

Removes orphaned resources from the SAS Environment Manager database. For example, a service whose relationships to its metadata or related resources are broken.

List Orphaned Nodes

List orphaned resources in the SAS Environment Manager database.

You can see the number of orphaned resources of a particular type by running the queries available on the Database tab of the HQ Health page.

Inventory Summary Tab

The Inventory Summary tab lists the resource types in inventory and the number of each type.

Server Settings

E-mail Configuration

Server e-mail configuration properties are used to form notifications that are sent for a triggered alert.

Base URL

The address and port where the server listens for web application requests. The initial value of Base URL is the web application listen port that is configured when the server is installed (for example: `http://server-machine.company.com:7080`)

From E-mail Address

The e-mail address that is listed as the sender of the alert e-mails (for example, `server@demo2.company.net`).

Announcements

The Version and Security Announcements setting controls what security and version announcements are sent to administrators.

Data Manager

These properties control how the contents of the inventory database are condensed and merged. Regardless of these settings, two years of compressed metric history is preserved. You control how long detailed metric data is retained. Retaining fewer days of detailed metric data and deleting alerts and other events on a timely basis can improve performance.
### Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run Database Maintenance Every</td>
<td>Controls how frequently detailed metric data that is older than the specified age is compressed and archived</td>
<td>By default, database maintenance is performed every hour.</td>
</tr>
<tr>
<td>Delete Detailed Metric Data Older Than</td>
<td>Controls how many days of detailed metric data are retained before compressing it into hourly averages with highs and lows and archiving those values.</td>
<td>The default setting is 2 days. The maximum setting is 7 days.</td>
</tr>
<tr>
<td>Reindex Metric Data Tables Nightly</td>
<td>Controls whether metric data tables are reindexed every night. If configured to re-index nightly, the tables are re-indexed around midnight.</td>
<td></td>
</tr>
<tr>
<td>Delete Alerts Older Than</td>
<td>Controls how long alert event data is stored.</td>
<td>The default value is 31 days.</td>
</tr>
<tr>
<td>Delete Events and Logs Older Than</td>
<td>Controls how long other event and log data is stored.</td>
<td>The default value is 31 days.</td>
</tr>
</tbody>
</table>

**Note:** Data management changes take effect when you restart the server.

### Global Alerts

The following properties enable immediate and global control of alert processing:

- **Alerts**
  - Enables or disables all alert definitions for all resources immediately. Disabling stops any alerts from triggering. Notifications that are defined in escalations that are currently in progress will be completed.

- **Alert Notifications**
  - Enables or disables alert notifications for all resources immediately. Disabling stops all notifications, including those for alerts with escalations currently in progress.

- **Hierarchical Alerting**
  - Controls whether alerts are evaluated using the hierarchical alerting method. When hierarchical alerting is enabled, before firing an alert for a resource, SAS Environment Manager considers the availability and alert status of the resource's parent. The purpose of hierarchical alerting is to avoid firing alerts for every resource affected by a single root cause.

**Note:** You can extend the effect of hierarchical alerting in SAS Environment Manager by configuring the relationship between a network device or virtual host and the platforms that depend on it. Use the Network and Host Dependency Manager that is available in the Plug-ins section of the Manage page.

### Notification Throttling

You can use notification throttling to limit the number of alert e-mail actions (notifications that are sent by e-mail for a triggered alert) that are issued in a 15-second interval. When the threshold that you specify is reached, SAS Environment Manager stops sending e-mail alert notifications and instead sends a summary of alert activity every ten minutes to the recipients that you specify.

After starting to throttle, SAS Environment Manager re-evaluates notification volume for fired alerts every 10 minutes. When it determines that the per-interval volume of individual notifications that fired alerts would
generate is less than the configured threshold, SAS Environment Manager resumes sending individual
notifications.

To enable notification throttling:

1. Click the **Notification Throttling ON** control.
2. In the **Threshold** field, enter the maximum number of notifications that you want sent in a 15-second interval. Valid values are 1 through 5.
3. Enter one or more e-mail addresses in the **Notification Email(s)** field.

### Automatic Baseline Configuration Properties

These properties control the baselining process. Changing the data set used to calculate baselines can affect baseline accuracy.

**Properties**

<table>
<thead>
<tr>
<th>Server Setting</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baseline Frequency</td>
<td>The frequency with which SAS Environment Manager calculates a baseline for each metric.</td>
<td>3 days</td>
</tr>
<tr>
<td>Baseline Dataset</td>
<td>The time range of metric data used in calculating the baseline.</td>
<td>7 days</td>
</tr>
<tr>
<td>Baseline Minimum Data Points</td>
<td>The minimum number of data points used in calculating a baseline.</td>
<td>40</td>
</tr>
<tr>
<td>Track Out-of-Bounds Metrics</td>
<td>Controls whether SAS Environment Manager tracks out-of-bounds metrics measurements that are greater than expected high range for a metric, or less than the expected low range for a metric.</td>
<td>off</td>
</tr>
</tbody>
</table>

### SNMP Configuration

Configure the Server for SNMP v1

Select "v1" from the SNMP Protocol Version pulldown and supply values for the properties defined in the table below.

The table below defines the properties for configuring the server for SNMP V1 communications with an NMS.

<table>
<thead>
<tr>
<th>Configuration Option</th>
<th>Description</th>
<th>Allowable Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Trap OID</td>
<td>The OID of the notification to be sent. Supplies the value of snmpTrapOID.0 - the second varbind in a trap or inform that the server generates. (The first varbind is SysUpTime.0.)</td>
<td></td>
</tr>
<tr>
<td>Configuration Option</td>
<td>Description</td>
<td>Allowable Values</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Default Notification Mechanism</td>
<td>Your selection governs the notification type that will appear as the default notification type option in the &quot;Notification Mechanism&quot; pulldown list that is presented in configuration dialog boxes when user configures an SNMP notification as an alert action, or as a step in an escalation.</td>
<td>For v1 of the SNMP protocol, choose V1 Trap. This is the only trap type that you can generate for SNMP v1.</td>
</tr>
<tr>
<td>Community</td>
<td>The community name to be sent with the trap.</td>
<td></td>
</tr>
</tbody>
</table>
| Generic ID                     | Single digit identifier of the trap type.                                                                                                                                                                                                                                                                                                    | 0 - coldStart  
1 - warmStart  
2 - linkDown  
3 - linkUp  
4 - authenticationFailure  
5 - egpNeighborLoss  
6 - enterpriseSpecific  |
| Specific ID                    | The specific trap code for an enterprise-specific trap (when Generic ID is set to 6).                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                |
| Enterprise OID                 | Enterprise OID.                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                |
| Agent Address                  | Address of the managed object that generates the trap.                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                |

### Configure the Server for SNMP v2c

<table>
<thead>
<tr>
<th>Configuration Option</th>
<th>Description</th>
<th>Allowable Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Trap OID</td>
<td>The OID of the notification to be sent. Supplies the value of snmpTrapOID.0 - the second varbind in a trap or inform that the server generates. (The first varbind is SysUpTime.0.)</td>
<td></td>
</tr>
</tbody>
</table>
| Default Notification Mechanism| Specifies the default notification type that will appear in configuration dialog boxes when an authorized user configures an SNMP notification as an alert action, or as a step in an escalation. This choice simply defines the default option - the user configuring an alert action or escalation can choose a different message type. | V1 Trap  
V2c Trap  
Inform  |
| Community                    | The community name to be sent with the trap.                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                |
### Configure the Server for SNMP v3

This section lists the properties for enabling the server to send SNMP notifications to an NMS. When this is enabled, you can use SNMP notifications in alert definitions as alert actions and escalation steps.

<table>
<thead>
<tr>
<th>Configuration Option</th>
<th>Description</th>
<th>Allowable Values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SNMP Trap OID</strong></td>
<td>The OID of the notification to be sent. Supplies the value of snmpTrapOID.0 - the second varbind in a trap or inform that the server generates. (The first varbind is SysUpTime.0.)</td>
<td></td>
</tr>
<tr>
<td><strong>Default Notification Mechanism</strong></td>
<td>Specifies the default notification type that will appear in configuration dialog boxes when an authorized user configures an SNMP notification as an alert action, or as a step in an escalation. This choice simply defines the default option - the user configuring an alert action or escalation can choose a different message type.</td>
<td>V1 Trap, V2c Trap, Inform</td>
</tr>
<tr>
<td><strong>Security Name</strong></td>
<td>The user name that the SNMP agent should use when sending notifications to the NMS.</td>
<td>Required</td>
</tr>
<tr>
<td><strong>Local Engine ID</strong></td>
<td>ID of the SNMP agent; this value appears automatically, and is not user-configurable.</td>
<td></td>
</tr>
<tr>
<td><strong>Authorization Protocol</strong></td>
<td>The SNMP authentication protocol that the server should use for communications with the NMS.</td>
<td>none, MD5, SHA</td>
</tr>
<tr>
<td><strong>Authorization Passphrase</strong></td>
<td>The SNMP authorization passphrase configured for use when communication with the NMS.</td>
<td></td>
</tr>
<tr>
<td><strong>Privacy Protocol</strong></td>
<td>The SNMP Privacy Protocol that the server should use for communication with the NMS.</td>
<td>none, DES, 3DES, AES-128, AES-192, AES-256</td>
</tr>
<tr>
<td><strong>Privacy Passphrase</strong></td>
<td>The SNMP privacy passphrase configured for use when communication with the NMS.</td>
<td></td>
</tr>
<tr>
<td><strong>Context Engine ID</strong></td>
<td>The EngineID of the NMS. This, along with Context Name, identifies the SNMP context for accessing management data.</td>
<td>Required for V1 and V2c traps. Do not supply for Inform.</td>
</tr>
</tbody>
</table>
### Monitoring Defaults

#### Overview

To display the **Monitoring Defaults** page, click **Monitoring Defaults** in the **Server Settings** section of the **Manage** page.

#### Page Contents

The **Monitoring Defaults** page lists all of the resource types that SAS Environment Manager can monitor. The page is organized in the following three sections:

- **Platforms Types** section lists the platform types that SAS Environment Manager can monitor.
- **Platform Service Types** section lists the platform service types that SAS Environment Manager can monitor.
- **Server Types** section lists the servers types and service types that SAS Environment Manager can monitor. This list is arranged hierarchically. Each server type in the list is followed by an indented list of associated services.

#### Page Navigation

The following links are available for each resource type:

- The name of each resource type (such as "Linux" or "Win32") links to a list of all resources of that type. Changes that are made to the metric template for the resource type update the monitoring settings for each resource that is displayed.
- To view or update a resource's metric collection settings, click its **Edit Metric Template** link. See **Metric Collection Settings for Resource Types on page 99**.
- To view or create alert definitions for a resource type, click its **Edit Alerts** link. See **Alert Definitions for a Resource Type on page 34**.

### Metric Collection Settings for Resource Types

#### Introduction

Metric collection settings for each resource type are configured on the **Monitoring Defaults** page for that resource type. This configuration affects all instances of resources for the specified resource type.

**CAUTION!** Changes made using these instructions overwrite per-resource custom metric collection configuration. Changes that you make to the metric collection settings for a resource type (on the **Monitoring Defaults** page) apply to all resources of that type. Such changes overwrite any custom metric collection configuration for resources of that type (per-resource changes that can be set on a particular resource's **Metric Data** tab).
Note: The preceding caution does not apply to indicator metrics. If a user has chosen a different set of indicator metrics for a resource instance (on the resource’s Indicators tab in the Resource Hub), changing the indicator metrics for a resource type on the Monitoring Defaults page does not overwrite or override the user’s selections.

To access a resource type’s Monitoring Defaults page, select the Manage page and click the Monitoring Defaults link in the Server Settings section. On the Monitoring Defaults page, click Edit Metric Template in the row of the resource type that you want set monitoring defaults for.

Enable Collection of a Metric
To enable the collection of a metric, follow the directions in Change a Metric Collection Interval on page 100. Collection of the metric is now enabled by default with the specified collection interval on every resource of this type.

Disable Collection of a Metric
To disable the collection of a metric, select the check box for the metric name (on the left) and click Disable Collection (at the bottom of the page).

Change a Metric Collection Interval
1 Select the check box for the metric name (on the left).
2 In Collection Interval for Selected (at the bottom of the page), enter a time value and select a unit of time measure for the collection interval.
3 Click the Collection Interval for Selected control (at the bottom of the Monitoring Defaults page).

Set Indicator Metrics
Indicator metrics are the metrics that are charted on a resource’s Indicators tab on the Resource page.

To specify indicator metrics for a resource type, select the check box for each metric that you want to use as an indicator. Then click the Set Selected Metrics as Indicators control (at the bottom of the Monitoring Defaults page).

The metrics that you select become the default indicators for the resource type.

Changes to indicator metrics apply to all existing resources, except for users that have explicitly changed the default indicator page for particular resources of the specified resource type.

APIs for Metric Collection Settings
As an alternative to the updating metric collection settings from within SAS Environment Manager, you can use APIs to perform updates from the command line or from scripts.
Resource Reference

GemFire

Introduction
GemFire is a distributed caching system. A GemFire Distributed System (DS) is a logical entity—a set of servers that are configured to communicate with one another. The servers in a DS are referred to as members or nodes.

Distributed System
The GemFire View for a Distributed System displays the following information:

Servers in the DS
The number of cache servers, gateway hubs and application peers in the distributed system.

Gateways in the DS
If the distributed system is part of a multi-site deployment, the number of gateways in the distributed system's Gateway Hub.

Clients connected to the DS
The number of clients (cache servers, gateways, or application peers) in other distributed systems that are connected to the distributed system.

The table in the middle of the GemFire view for a distributed system displays inventory properties and last reported metric values for each server (including Cache Servers, Gateway Hubs and Application Peers) in the distributed system.

Cache Server or Application Peer
The GemFire View for a Cache Server or Application Peer displays the following server and region inventory properties and metrics:

Server metrics
The single row table presents last reported metric values for the cache server or application peer.

Region metrics
The multi-row table presents inventory properties and the Entry Count metric for each region that the server contains.

Gateway Hub
The GemFire View for a Gateway Hub displays inventory data and live measurements for the gateway hub, the hubs and regions that it contains, and for any clients connected to the hub.

Nagios

View Nagios Service Detail
From the Resources page, select Nagios Availability.

The page displays the most recent results of the Nagios checks. This is the same information that is displayed on the Nagios Service Details page.
Host
the host that the Nagios check is monitoring

Service
the Nagios plug-in that is used to perform the check

Status
the return code from execution of the check

Last Check
when the check was last run

Event Log
the output of the plug-in

Each line is color-coded as follows:

- pink indicates that the monitored service is down
- yellow indicates that the monitored service has triggered an alert (based on the threshold that is defined in Nagios)
- green indicates that the monitored service is OK

View a Nagios Check

To view a Nagios check:

1. Browse to the Nagios server resource (Resources ⇒ Browse ⇒ Servers ⇒ Nagios).
2. Choose the Nagios server from the list of servers.
3. On the Nagios server’s Indicators tab, click the Nagios Plug-in auto-group.
4. The first chart on the Indicators tab shows the average execution time for all of the checks in the group.
   Note: Charts of average result values and return codes are also displayed, but this data is not meaningful for a group.
5. Click an item in the Group Members list.
6. On the Indicators tab for the Nagios service, click the blue icons (above the time range bar at the bottom of the page) to view log messages output.

See Also
Resource Management: Overview on page 22

Spring Insight

Understanding Application Metrics

Overview
The Spring Insight Applications page displays multiple metrics that indicate how well an application is running (for example, the percentage of application requests that had an unacceptable response time and the number of requests that returned errors).
The **Health** tab displays metrics for all applications that report to dashboards that are monitored by SAS Environment Manager. The **Performance** tab displays metrics for **Insight** dashboards and **Insight** applications.

**Application Health**

The **Application Health** metric for an application is the health value that **Insight** calculates for the application. This metric is based on the percentage of **Insight** traces that complete without error. The values, indicators, and thresholds for the **Application Health** metric are as follows:

<table>
<thead>
<tr>
<th>Value</th>
<th>Indicator</th>
<th>Percentage of Successful Insight Traces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Excellent</td>
<td>Excellent</td>
<td>94% or more</td>
</tr>
<tr>
<td>Good</td>
<td>Good</td>
<td>85% - 93%</td>
</tr>
<tr>
<td>Fair</td>
<td>Fair</td>
<td>70% - 84%</td>
</tr>
<tr>
<td>Poor</td>
<td>Poor</td>
<td>50% - 83%</td>
</tr>
<tr>
<td>Unacceptable</td>
<td>Unacceptable</td>
<td>0% - 49%</td>
</tr>
</tbody>
</table>

**Application Vitals**

The **Vitals** metric for an application is calculated by SAS Environment Manager. It is based on the Application Health metric (described above), and also takes into account the SAS Environment Manager metrics and events for the application and for resources that the application depends on, including:

- Number of unfixed alerts for the application in SAS Environment Manager.
- Availability of the managed resources that the application depends on: application servers, database servers (if applicable), and platforms.
- Number of unfixed alerts for the resources that the application depends on: application servers, database servers (if applicable), and platforms.

If an application has no unfixed alerts in SAS Environment Manager and the resources that it depends on are available and have no unfixed alerts, the application's value of the applications Vitals metric is equal to the value of its Application Health metric.

**Unfixed Alert Count**

The number of unfixed alerts during the timeframe.

**Error Rate**

The percentage of **Insight** traces that resulted in an HTTP error status code (500 to 600).

**Response Time Levels**

The "Invocations" metric tells you what percentage of traces had response times in each of three response time levels. The response time thresholds for each level are configurable in Spring Insight, and by default are:

- **Satisfied**
  - Response time 200 ms or less.
- **Tolerated**
  - Response time more than 200 ms but less than 800 ms.
Frustrated
  Response time 800 ms or higher.

For example
  19.8%/7.4%/72.7%

indicates that over the selected interval:
  - 19.2% of the traces had response time 200 ms or less.
  - 7.5% had response time more than 200 ms but less than 800 ms.
  - 73.4% had response time 800 ms or higher.

Contents of the Spring Insight Applications Page

Dashboards Tab

The **Dashboards** pane on the left side of the Spring Insight Applications page is a tree control whose nodes are **Insight Dashboards** and **Insight Applications**.

The color of the bar to the left of a **Dashboard** node indicates the worst **Vitals** metric among the applications reporting to the Dashboard.

You use the **Dashboards** pane to browse a hierarchy of performance data. Depending on your need and interest, you view filter your view to include health information for:

- All applications reporting to all SAS Environment Manager-managed **Insight Dashboards**
  
  This is the view that appears when neither a dashboard or application is selected in the tree control. To return to this view, click the **Dashboards** link above the tree control. See **Health Tab for All Applications on page 104**.

- Just the applications reporting to a particular **Insight Dashboards**
  
  To display this view, click the dashboard of interest in the tree control. See **Performance Tab for a Dashboard on page 105**.

- Just one particular application
  
  To display this view, select the application of interest in the tree control. See **Performance Tab for an Application on page 106**.

Health Tab for All Applications

The **Health** tab summarizes the health of all of the applications reporting to SAS Environment Manager-managed Insight Dashboards. This tab is present when you first open the Spring Insight Applications page.

After navigating to a dashboard or an application, you can redisplay the **Health** tab by clicking **Dashboards** at the top of the left pane.

The **Health** tab contains the following data and metrics:

**Applications Health Trend chart**

By default, this chart plots the health of the five applications that currently have the poorest vitals. You can add and remove applications to the chart by checking and unchecking the box next to it. See **Application Health on page 103**.

**Worst Vitals**

The **Vitals** indicator in the **All Applications** bar reflects the worst value reported among all applications reporting to all Dashboards. See **Application Vitals on page 103**.

**Application Metrics**

Below the **Applications Health Trend** chart is a list of all applications under management, ordered by the applications’ **Vitals** metric, starting with the worst. The following data and metrics are displayed for each application:
Application
The name of the application is a link. If you click it, the Performance tab for the dashboard appears. See Performance Tab for an Application on page 106.

Vitals

Alerts
See Unfixed Alert Count on page 103.

Errors
See Error Rate on page 103.

Invocations (F/T/S)
See Response Time Levels on page 103.

Performance Tab for a Dashboard
To display the Performance tab for an Insight Dashboard, click the dashboard's name in the Dashboards tab. In the list of applications reporting to the dashboard, the list is ordered by application health, from worst to best. You can mouse over the application name to highlight the line for it in the Application Health Trend chart.

You can click the application name to display the Performance tab for it. See Performance Tab for an Application on page 106.

The Performance tab for a Dashboard contains:

Applications Health Trend chart
By default, this chart plots the health of the five applications (reporting to the Dashboard) that currently have the poorest vitals. You can add and remove applications to the chart by checking and unchecking the box next to it. See Application Health on page 103.

Dashboard Vitals
The Vitals indicator in the Dashboard bar is a composite health indicator that takes into account:

- The Vitals for the applications reporting to the currently selected Insight Dashboard.
- Availability of the managed resources that the Insight Dashboard depends on: application server (tc Server) and platform.
- Number of unfixed alerts for the resources that the Insight Dashboard depends on: application server (tc Server) and platform.

Application Metrics
Below the Applications Health Trend chart is a list of the applications reporting to the Dashboard. The following metrics are displayed for each application:

Vitals
See Application Vitals on page 103.

Alerts
See Unfixed Alert Count on page 103.

Errors
See Error Rate on page 103.

Invocations (F/T/S)
See Response Time Levels on page 103.

Application Server Performance
To view health data for the application server that the Insight Dashboard runs on, click the control in the Application Server bar. See Application Server Performance on page 106.

Platform Performance
To view health data for platform on which the Insight Dashboard runs, click the control in the Platforms bar. See Platform Performance on page 106.
Application Server Performance

The **Application Server** section charts a selected application server metric for all, or selected application servers where the applications in the Dashboard run.

The **Metric Low/Avg/Peak** menu lists all of the available metrics for the application server and shows the low, average, and peak values for the metric over the current time range. Choose a metric from the list to graph it.

Below the chart, the following information is listed for each application server:

- **name**
  - The name of the resource in SAS Environment Manager.
- **AVAIL**
  - Current availability of the resource
- **ALERTS**
  - Current number of unfixed alerts
- **LOW**
  - Low value during current display range.
- **AVG**
  - Average value during current display range.
- **PEAK**
  - High value during current display range.

Platform Performance

The **Platform** section charts a selected platform metric for all, or selected platforms where the applications in the Dashboard run.

The **Metric Low/Avg/Peak** menu lists all of the available platform metrics and shows the low, average, and peak values for the metric over the current time range. Choose a metric from the list to graph it.

Below the chart, the following information is listed for each platform:

- **name**
  - The name of the resource in SAS Environment Manager.
- **AVAIL**
  - Current availability of the resource
- **ALERTS**
  - Current number of unfixed alerts
- **LOW**
  - Low value during current display range.
- **AVG**
  - Average value during current display range.
- **PEAK**
  - High value during current display range.

Performance Tab for an Application

To display the **Performance** tab for an Insight Application, click the application’s name in the **Dashboards** tab.

The **Performance** tab has four sections:

- **Applications**
  - The application name is a link. Clicking the link opens Insight Operations, which displays more detailed resource health and performance metrics for the current display range.
The **Vitals** health bar to the right of the application name indicates the current Vitals for the application. See *Application Vitals* on page 103.

The **Health Trend** chart plots the application's Health and Error Rate metrics for the display range. See *Application Health* on page 103.

The **Invocations** chart plots the distribution of request response times across the three response time levels defined in *Response Time Levels* on page 103.

**Application Server**

- This section is expanded if one or more application servers to which the application is deployed is unhealthy. Otherwise, the section is collapsed.
- See *Application Server Performance* on page 106.

**Data Service**

- This section is present if the application accesses a SAS Environment Manager managed database server. See *Data Service Performance* on page 107.
- This section is expanded if the database that the application uses is unhealthy. Otherwise, the section is collapsed.
- See *Data Service Performance* on page 107.

**Platform**

- This section is expanded if one or more platforms where the application runs is unhealthy. Otherwise, the section is collapsed.
- See *Platform Performance* on page 106.

**Data Service Performance**

The **Data Service** section is present if the currently selected application accesses a database managed by SAS Environment Manager.

The **Metric Low/Avg/Peak** menu lists all of the available platform metrics and shows the low, average, and peak values for the metric over the current display range. Choose a metric from the list to graph it.

Below the chart, the following information is listed for each platform:

- **name**
  - The name of the resource in SAS Environment Manager.

- **AVAIL**
  - Current availability of the resource

- **ALARMS**
  - Current number of unfixed alerts

- **LOW**
  - Low value during current display range

- **AVG**
  - Average value during current display range

- **PEAK**
  - High value during current display range

**Jump to Insight Operations**

You can jump from the Spring Insight Applications page into the Insight application to investigate problems. Click the application name link on the application's **Performance** tab. Insight will open in a new window, with the application selected in the **Browse Resources** tab, where you can view more detailed application health data for display range currently selected in the SAS Environment Manager user interface.
vSphere

Introduction
The vSphere page enables you to monitor and manage vSphere hosts and the virtual machines (VMs) that run on them.

To display the vSphere page, select vSphere from the Resources page.

Note: The vSphere option is available only if you have vSphere components under management.

Permissions
In SAS Environment Manager, a user can access only those resources that are assigned to groups to which the user's roles provide access. The accessible resources are further limited by role permissions to inventory types.

In other words, you can see PlatformA in Browse dialog boxes and navigate to it if PlatformA is a member of a group assigned to your role, and that role grants access to platforms.

The vSphere user interface behaves somewhat differently. If you have View access to platforms, you can see all of the vSphere Hosts and vSphere VMs in the deployment whether they belong to a group assigned to your role.

Note: Even if your role does not grant View permission to servers, vCenter servers are visible on the vSphere page. A vCenter server is the root of the vSphere resource hierarchy and is visible regardless of role permissions. The only resource data that is exposed for the vCenter server is its name.

Inventory Tab
The Inventory tab on the vSphere page is a tree of the vSphere resources under management, organized in the resource type hierarchy shown below. The lowest level appears for a VM that has an SAS Environment Manager Agent running and monitoring resources running in the VM.

The contents of the Inventory tab are updated once per minute.

You can use the Inventory tab to view the virtual resource hierarchy and to navigate among resources. When you select a resource, the tab or tabs on the right side of the page contain resource data, performance charts, and resource control commands, as appropriate to the resource type.

The table below shows the vSphere resource type hierarchy; the right column indicates the inventory level for a type in the SAS Environment Manager inventory model.

<table>
<thead>
<tr>
<th>vSphere Resource Hierarchy</th>
<th>Inventory Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vCenter server</td>
<td>server</td>
</tr>
<tr>
<td>VMware vSphere Host platform</td>
<td>platform</td>
</tr>
<tr>
<td>VMware vSphere VM platform</td>
<td>platform</td>
</tr>
<tr>
<td>SAS Environment Manager Agent-managed resource in VM</td>
<td>server</td>
</tr>
</tbody>
</table>

The following table lists the icons in the vSphere Inventory tab. The icon to the left of an item in the resource tree indicates the type of the resource, and for a VM, its availability status.

| vCenter Server |
vSphere Host

VM whose availability is Up

VM whose availability is Paused

VM whose availability is Powered Off

VM whose availability status is Down

VM whose availability status is Unknown

A SAS Environment Manager-managed resource running in a VM that has an SAS Environment Manager Agent running in it.

Summary Tab

Overview
The Summary tab, available when any resource in the Inventory tab is selected, displays properties for the selected resource, and its parent resource, as applicable.

To view a vSphere resource in the SAS Environment Manager Resource view, click the view resource link to the right of the resource name.

Summary Tab for vCenter
When a vCenter Server instance is selected in the vSphere page, the Summary tab contains the name of the vCenter instance. You can view inventory and configuration properties for the vCenter instance in the Resource view click view resource next to the resource name to view it in the Resource Hub.

Summary Tab for vSphere Hosts
The Summary tab for a vSphere Host displays the following properties:

Host Information
- Hostname
- Location
- Manufacturer
- Model
- VMware Version

Processor Details
- Type - of the processor
- CPUs - Processor sockets and cores per socket

Network Details
- IP Address
- Default Gateway
- DNS - primary and secondary DNS server
Summary Tab for vSphere VM

The Summary tab for a vSphere VM displays the following VM properties:

VM Information

Hostname
of the vSphere Host (ESX platform) where the VM runs

Guest OS
operating system running in the VM

vCPU(s)
number of virtual processors in the VM

Memory
VM memory, in MB

MAC Address

IP
IP address of the virtual machine

VM Version
virtual machine hardware version

Tools Version
version of VMware Tools on the VM.

Config Details

ESX Host
IP address of the vSphere Host (ESX platform) where the VM runs

Resource Pool
resource pool with which the VM is associated

Config File
path to the VM configuration (.vmx) file, expressed using the symbolic link path to the VMFS volume where the file is stored

Properties for the vSphere Host where the VM runs are shown below the VM properties.

If the VM does not have an SAS Environment Manager Agent running in it, the Summary tab displays "Performance data not available" near the top of the page.

Summary Tab for a Managed Resource in the VM

When you select a managed resource running in a VM, the Summary tab displays the vSphere Host and VM properties.

The contents of the Summary tab are updated once per minute.

To view inventory properties for the managed resource itself, click the view resource link next to the resource name to view the resource in the Resource view.

Note: This information applies to a VM with a running SAS Environment Manager Agent that is managing resources in the VM. Otherwise, resources running in the VM do not appear in the vSphere page.

Performance Tab

Overview

The Performance tab appears when a vSphere Host is selected, and, if the VMs running on the host have SAS Environment Manager Agents running, for each VM, and for the managed resources running in the VMs.
The contents of the **Performance** tab are updated once per minute.

If a VM does not have an agent running in it, no **Performance** tab appears. You can view the VM metrics in its Monitor page in the Resource view. Click **view resource** next to the **Hostname** property on the VM’s **Summary** tab.

**View Metrics**

The **Performance** tab displays an **Availability** bar and a chart for each metric currently enabled for the selected resource type.

Twelve hours history is displayed by default. You can use the **Data Range** menu to set the display range to the most recent:

- 1, 4, or 12 hours
- 1 or 2 days,
- 1 week, or
- 1 month

**Correlate Metrics**

On the **Performance** tab for a VM or an SAS Environment Manager Agent-managed resource running in the VM, you can use the **Compare** menu to correlate the selected resource’s performance with its parent or grandparent. You can:

Compare each VM metric with its vSphere Host equivalent. For example, you can compare the VM's "Disk Usage (Average)" metric to its host's "Disk Usage (Average)" metric; the VM's "CPU Usage (Average)" metric to its host's "CPU Usage (Average)" metric; and so on.

Compare each VM metric to a selected vSphere Host metric. For example, you can compare each VM metric to the "Disk Usage (Average)" metric of its vSphere host.

Compare metrics for a managed resource in the VM with performance of the VM or the vSphere host. Use the **Compare** menu to select a VM or Host metric. The charts for the managed resource metrics are overlaid with the line for the selected VM or host metric.

**Control Tab**

The **Control** tab appears when a VM is selected (if there is an SAS Environment Manager Agent running in the VM) and enables you to issue a control command to the VM.

If a VM does not have an agent running in it, no **Control** tab appears. You can run control actions from the "Control" page for the VM in the Resource view. Click **view resource** next to the **Hostname** property on the VM's **Summary** tab.

**VMware vSphere Metrics**

**Host Metrics**
### Host Metrics

<table>
<thead>
<tr>
<th>Name</th>
<th>Alias</th>
<th>vCenter Statistics Level</th>
<th>Definition</th>
<th>Units</th>
<th>Category</th>
<th>Default On</th>
<th>Default Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>Availability</td>
<td>n/a</td>
<td>The plugin determines a vSphere Host's availability by querying vCenter for the host's power state, once per minute, by default. Availability takes these values: If the power state is:</td>
<td>percentage</td>
<td>AVAILABILITY</td>
<td>true</td>
<td>1 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Up if vSphere Host power state is poweredOn.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Paused if vSphere Host power state is standby.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Powered Off if vSphere Host power state is poweredOff.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Down if the vSphere Host power state is none of the above.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Uptime</td>
<td>sys.uptime.late st</td>
<td></td>
<td>The plugin determines a vSphere Host's availability by querying vCenter for the host's power state, once per minute, by default. Uptime takes these values: If the power state is:</td>
<td>sec</td>
<td>AVAILABILITY</td>
<td>false</td>
<td>1 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Up if vSphere Host power state is poweredOn.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPU Usage (Average)</td>
<td>cpu.usage.average</td>
<td>1</td>
<td>CPU usage as a percentage during the interval.</td>
<td>percent</td>
<td>UTILIZATION</td>
<td>true</td>
<td>5 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Actively used CPU of the host, as a percentage of the total available CPU. Active CPU is approximately equal to the ratio of the used CPU to the available CPU.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>available CPU = # of physical CPUs clock rate</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>100% represents all CPUs on the host. For example, if a four-CPU host is running a virtual machine with two CPUs, and the usage is 50%, the host is using two CPUs completely.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk Usage (Average)</td>
<td>disk.usage.average</td>
<td>1</td>
<td>Aggregated disk I/O rate. For a vSphere host, this includes the rates for all virtual machines running on the host during the collection interval.</td>
<td>KB per second</td>
<td>UTILIZATION</td>
<td>true</td>
<td>5 min</td>
</tr>
<tr>
<td>Highest Disk Latency</td>
<td>disk.maxTotalLatency.latest</td>
<td>1</td>
<td>Highest latency value across all disks used by the host. Latency measures the time taken to process a SCSI command issued by the guest OS to the virtual machine. The kernel latency is the time VMkernel takes to process an IO request. The device latency is the time it takes the hardware to handle the request. Total latency = kernelLatency + deviceLatency</td>
<td>ms</td>
<td>UTILIZATION</td>
<td>true</td>
<td>5 min</td>
</tr>
<tr>
<td>Name</td>
<td>Alias</td>
<td>vCenter Statistics Level</td>
<td>Definition</td>
<td>Units</td>
<td>Category</td>
<td>Default On</td>
<td>Default Interval</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------------------------------</td>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>-------------------</td>
<td>------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Memory Usage (Average)</td>
<td>mem.usage.average</td>
<td>1</td>
<td>memory usage = memory consumed · host configured memory size</td>
<td>percent</td>
<td>UTILIZATION</td>
<td>true</td>
<td>5 min</td>
</tr>
<tr>
<td>Network Usage (Average)</td>
<td>net.usage.average</td>
<td>1</td>
<td>Sum of the data transmitted and received during the collection interval. Sum of data transmitted and received across all physical NIC instances connected to the host.</td>
<td>KB</td>
<td>UTILIZATION</td>
<td>true</td>
<td>5 min</td>
</tr>
<tr>
<td>CPU Reserved Capacity</td>
<td>cpu.reservedCapacity.average</td>
<td>2</td>
<td>Total CPU capacity reserved by the virtual machines.</td>
<td>none</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>CPU Throttled (1 min. Average)</td>
<td>rescpu.maxLimited1.latest</td>
<td>3</td>
<td></td>
<td>percent</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>CPU Throttled (5 min. Average)</td>
<td>rescpu.maxLimited5.latest</td>
<td>3</td>
<td></td>
<td>percent</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>CPU Throttled (15 min. Average)</td>
<td>rescpu.maxLimited15.latest</td>
<td>3</td>
<td></td>
<td>percent</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>CPU Running (1 min. Average)</td>
<td>rescpu.runav1.latest</td>
<td>3</td>
<td></td>
<td>percent</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>CPU Running (5 min. Average)</td>
<td>rescpu.runav5.latest</td>
<td>3</td>
<td></td>
<td>percent</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>CPU Running (15 min. Average)</td>
<td>rescpu.runav15.latest</td>
<td>3</td>
<td></td>
<td>percent</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>Name</td>
<td>Alias</td>
<td>vCenter Statistics Level</td>
<td>Definition</td>
<td>Units</td>
<td>Category</td>
<td>Default On</td>
<td>Default Interval</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------</td>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
<td>-------------</td>
<td>-------------</td>
<td>------------------</td>
</tr>
<tr>
<td>CPU Active (1 min. Average)</td>
<td>rescpu.actav1.latest</td>
<td>3</td>
<td>3</td>
<td>percent</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>CPU Active (5 min. Average)</td>
<td>rescpu.actav5.latest</td>
<td>3</td>
<td>3</td>
<td>percent</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>CPU Active (15 min. Average)</td>
<td>rescpu.actav15.latest</td>
<td>3</td>
<td>3</td>
<td>percent</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>Memory Swap In</td>
<td>mem.swapin.average</td>
<td>2</td>
<td>Sum of memory swapin of all powered on VMs on the host.</td>
<td>KB</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>Memory Swap Out</td>
<td>mem.swapout.average</td>
<td>2</td>
<td>Sum of Memory Swap Out of all powered on VMs on the host.</td>
<td>KB</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>Memory Swap Used</td>
<td>mem.swapused.average</td>
<td>2</td>
<td>Amount of memory that is used by swap. Sum of Memory Swapped of all powered on virtual machines and vSphere services on the host.</td>
<td>KB</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>Memory Balloon</td>
<td>mem.vmmemct.average</td>
<td>1</td>
<td>Sum of Memory Balloon (Amount of memory allocated by the virtual machine memory control driver) of all powered on virtual machines and vSphere services on the host. If the balloon target value is greater than the balloon value, the VMkernel inflates the balloon, causing more virtual machine memory to be reclaimed. If the balloon target value is less than the balloon value, the VMkernel deflate the balloon, which allows the virtual machine to consume additional memory if needed.</td>
<td>KB</td>
<td>UTILIZATION</td>
<td>true</td>
<td>5 min</td>
</tr>
<tr>
<td>Memory Unreserved</td>
<td>mem.unreserved.average</td>
<td>2</td>
<td>Amount of memory that is unreserved. Memory reservation not used by the Service Console, VMkernel, vSphere services and other powered on VMs' user-specified memory reservations and overhead memory.</td>
<td>KB</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>Memory Heap</td>
<td>mem.heap.average</td>
<td>2</td>
<td>Amount of VMkernel virtual address space dedicated to VMkernel main heap and related data.</td>
<td>KB</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>Name</td>
<td>Alias</td>
<td>vCenter Statistics Level</td>
<td>Definition</td>
<td>Units</td>
<td>Category</td>
<td>Default On</td>
<td>Default Interval</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------</td>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Memory Heap Free</td>
<td>mem.heapfree.average</td>
<td>2</td>
<td>Amount of free address space in the VMkernel's main heap. Heap Free varies, depending on the number of physical devices and various configuration options. There is no direct way for the user to increase or decrease this statistic.</td>
<td>KB</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>Memory Overhead</td>
<td>mem.overhead.average</td>
<td>1</td>
<td>Total of all overhead metrics (Amount of additional machine memory allocated to a virtual machine for overhead. The overhead amount is beyond the reserved amount), for powered-on virtual machines, plus the overhead of running vSphere services on the host.</td>
<td>KB</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>Memory Zero</td>
<td>mem.zero.average</td>
<td>2</td>
<td>Amount of memory that is zeroed out (contains only 0s). This statistic is included in Memory Shared. For a vSphere Host, Sum of Memory Zero of all powered on VMs and vSphere services on the host.</td>
<td>KB</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>Memory Reserved Capacity</td>
<td>mem.reserved Capacity.average</td>
<td>2</td>
<td>Total amount of memory reservation used by powered on VMs and vSphere services on the host. Includes overhead amount.</td>
<td>MB</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>Memory Active</td>
<td>mem.active.average</td>
<td>2</td>
<td>Amount of memory actively used, as estimated by VMkernel. Active memory is based on the current workload of the virtual machine or host. For a vSphere Host, sum of the active guest physical memory of all powered on virtual machines on the host, plus memory used by basic VMKernel applications on the host.</td>
<td>KB</td>
<td>UTILIZATION</td>
<td>true</td>
<td>5 min</td>
</tr>
<tr>
<td>Memory Shared</td>
<td>mem.shared.average</td>
<td>2</td>
<td>Sum of the shared memory values of all powered-on virtual machines, plus the amount for the vSphere services on the host. The host’s Memory Shared might be larger than the amount of machine memory if memory is overcommitted (the aggregate virtual machine configured memory is much greater than machine memory). The value of this statistic reflects how effective transparent page sharing and memory overcommitment are for saving machine memory.</td>
<td>KB</td>
<td>UTILIZATION</td>
<td>true</td>
<td>5 min</td>
</tr>
<tr>
<td>Memory Granted</td>
<td>mem.granted.average</td>
<td>2</td>
<td>The total of all granted metrics for all powered-on virtual machines, plus memory for vSphere services on the host.</td>
<td>KB</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>Name</td>
<td>Alias</td>
<td>vCenter Statistics Level</td>
<td>Definition</td>
<td>Units</td>
<td>Category</td>
<td>Default On</td>
<td>Default Interval</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------------</td>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Memory Consumed</td>
<td>mem.consume.d.average</td>
<td>1</td>
<td>Amount of machine memory used on the host. Consumed memory includes memory used by virtual machines, the service console, VMkernel, and vSphere services, plus the total consumed memory for all running virtual machines. Host consumed memory = total host memory - free host memory</td>
<td>KB</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>Memory State</td>
<td>mem.state.latest</td>
<td>2</td>
<td>Amount of free machine memory on the host. VMkernel has four free-memory thresholds that affect the mechanisms used for memory reclamation. 0 (High) - Free memory &gt;= 6% of machine memory - service console memory 1 (Soft) - Free memory &gt;= 4% of machine memory - service console memory 2 (Hard) - Free memory &gt;= 2% of machine memory - service console memory 3 (Low) - Free memory &gt;= 1% of machine memory - service console memory For 0 and 1, swapping is favored over ballooning. For 2 and 3, ballooning is favored over swapping.</td>
<td>none</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>Memory Shared Common</td>
<td>mem.sharedcommon.average</td>
<td>2</td>
<td>Amount of machine memory that is shared by all powered-on virtual machines and vSphere services on the host. Memory Shared - Memory Shared Common = Host memory saved by sharing</td>
<td>KB</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>Memory Used by vmkernel</td>
<td>mem.sysUsage.average</td>
<td>2</td>
<td>Amount of memory used by the VMkernel. Amount of machine memory used by the VMkernel for &quot;core&quot; functionality (such as its own internal uses or device drivers). It does not include memory used by VMs or by vSphere services.</td>
<td>KB</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
</tbody>
</table>

* Availability is determined by SAS Environment Manager; it is not a vCenter statistic.
VM Metrics
<table>
<thead>
<tr>
<th>Name</th>
<th>Alias</th>
<th>vCenter Statistics Level</th>
<th>Definition</th>
<th>Units</th>
<th>Category</th>
<th>Default On</th>
<th>Default Interval</th>
</tr>
</thead>
</table>
| Availability         | Availability           | n/a                      | The plugin determines a VM's availability by querying vCenter for a VM power state, once per minute, by default. Availability takes these values: If the power state is:  
<p>|                      |                        |                          | - Up if VM power state is poweredOn.                                       | percentage | AVAILABILITY | true       | 1 min            |
|                      |                        |                          | - Paused if VM power state is standby.                                     |            |              |            |                  |
|                      |                        |                          | - Powered Off if VM power state is poweredOff.                             |            |              |            |                  |
|                      |                        |                          | - Unknown if the VM power state is none of the above.                      |            |              |            |                  |
|                      |                        |                          | - Down if VM availability was not reported for a duration equal to, or greater than, twice the configured collection interval, which is 1 minute, by default. |            |              |            |                  |
| Uptime               | sys.uptime.latest      | 1                        | CPU usage as a percentage during the interval. This value is reported with 100% representing all processor cores on the system. For example, a 2-way VM using 50% of a four-core system is completely using two cores. | percent    | UTILIZATION  | true       | 5 min           |
| CPU Usage (Average)  | cpu.usage.average      | 1                        | Aggregated disk I/O rate.                                                 | KB per second | UTILIZATION | true       | 5 min           |
| Disk Usage (Average) | disk.usage.average     | 1                        | The percentage of memory used as a percent of all available machine memory. | percent    | UTILIZATION  | true       | 5 min           |
| Memory Usage (Average) | mem.usage.average    | 1                        | Sum of the data transmitted and received during the collection interval.   | KB         | UTILIZATION  | true       | 5 min           |
| Network Usage (Average) | net.usage.average    | 1                        |                                                                           |            | UTILIZATION  | false      | 5 min           |
| CPU Throttled (1 min. Average) | rescpu.maxLimited1.latest | 3                        |                                                                           | percent    | UTILIZATION  | false      | 5 min           |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Alias</th>
<th>vCenter Statistics Level</th>
<th>Definition</th>
<th>Units</th>
<th>Category</th>
<th>Default On</th>
<th>Default Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Throttled (5 min. Average)</td>
<td>rescpu.maxLimited5.latest</td>
<td>3</td>
<td></td>
<td>percent</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>CPU Throttled (15 min. Average)</td>
<td>rescpu.maxLimited15.latest</td>
<td>3</td>
<td></td>
<td>percent</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>CPU Running (1 min. Average)</td>
<td>rescpu.runav1.latest</td>
<td>3</td>
<td></td>
<td>percent</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>CPU Running (5 min. Average)</td>
<td>rescpu.runav5.latest</td>
<td>3</td>
<td></td>
<td>percent</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>CPU Running (15 min. Average)</td>
<td>rescpu.runav15.latest</td>
<td>3</td>
<td></td>
<td>percent</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>CPU Active (1 min. Average)</td>
<td>rescpu.actav1.latest</td>
<td>3</td>
<td></td>
<td>percent</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>CPU Active (5 min. Average)</td>
<td>rescpu.actav5.latest</td>
<td>3</td>
<td></td>
<td>percent</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>CPU Active (15 min. Average)</td>
<td>rescpu.actav15.latest</td>
<td>3</td>
<td></td>
<td>percent</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>Memory Swap In</td>
<td>mem.swapin.average</td>
<td>2</td>
<td>Average memory Swap In. A large number here represents a problem with lack of memory and a clear indication that performance is suffering as a result.</td>
<td>KB</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td>Name</td>
<td>Alias</td>
<td>vCenter Statistics Level</td>
<td>Definition</td>
<td>Units</td>
<td>Category</td>
<td>Default On</td>
<td>Default Interval</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------</td>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>------------</td>
<td>------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Memory Swap Out</td>
<td>mem.swapout.</td>
<td>2</td>
<td>Average Memory Swap Out. A large number here represents a problem with lack of memory and a clear indication that performance is suffering as a result.</td>
<td>KB</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td></td>
<td>average</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Memory Balloon</td>
<td>mem.vmmemct.l.</td>
<td>1</td>
<td>Sum of Memory Balloon (Amount of memory allocated by the virtual machine memory control driver)</td>
<td>KB</td>
<td>UTILIZATION</td>
<td>true</td>
<td>5 min</td>
</tr>
<tr>
<td></td>
<td>average</td>
<td></td>
<td>If the balloon target value is greater than the balloon value, the VMkernel inflates the balloon, causing more virtual machine memory to be reclaimed. If the balloon target value is less than the balloon value, the VMkernel deflate the balloon, which allows the virtual machine to consume additional memory if needed.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Memory Balloon Target</td>
<td>mem.vmmemct</td>
<td>2</td>
<td></td>
<td>KB</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td></td>
<td>ltarget.average</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Memory Zero</td>
<td>mem.zero.</td>
<td>2</td>
<td>Amount of memory that is zeroed out (contains only 0s). This statistic is included in Memory Shared. For a vSphere Host, Sum of Memory Zero of all powered on VMs and vSphere services on the host.</td>
<td>KB</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td></td>
<td>average</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Memory Active</td>
<td>mem.active.</td>
<td>2</td>
<td>Amount of memory actively used, as estimated by VMkernel. Active memory is based on the current workload of the virtual machine or host. For a vSphere Host, sum of the active guest physical memory of all powered on virtual machines on the host, plus memory used by basic VMKernel applications on the host.</td>
<td>KB</td>
<td>UTILIZATION</td>
<td>true</td>
<td>5 min</td>
</tr>
<tr>
<td></td>
<td>average</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Memory Shared</td>
<td>mem.shared.</td>
<td>2</td>
<td>The average amount of shared memory. Shared memory represents the entire pool of memory from which sharing savings are possible. The amount of memory that this has been condensed to is reported in shared common memory. So, total saving due to memory sharing equals shared memory minus shared common memory.</td>
<td>KB</td>
<td>UTILIZATION</td>
<td>true</td>
<td>5 min</td>
</tr>
<tr>
<td></td>
<td>average</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Memory Granted</td>
<td>mem.granted.</td>
<td>2</td>
<td>The amount of memory that was granted to the VM by the host. Memory is not granted to the host until it is touched one time and granted memory can be swapped out or ballooned away if the VMkernel needs the memory.</td>
<td>KB</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
<tr>
<td></td>
<td>average</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Alias</td>
<td>vCenter Statistics Level</td>
<td>Definition</td>
<td>Units</td>
<td>Category</td>
<td>Default On</td>
<td>Default Interval</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------</td>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>-------------</td>
<td>-------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Memory Consumed</td>
<td>mem.consume d.average</td>
<td>1</td>
<td>The amount of machine memory that is in use by the VM. While a VM might have been configured to use 4 GB of RAM, as an example, it might have only touched half of that. Of the 2 GB left, half of that might be saved from memory sharing. That would result in 1 GB of consumed memory.</td>
<td>KB</td>
<td>UTILIZATION</td>
<td>false</td>
<td>5 min</td>
</tr>
</tbody>
</table>

* Availability is determined by SAS Environment Manager; it is not a vCenter statistic.
The Sign In Page
This is the sign in page. Enter a valid user ID and password.

Resource Selection
To select which resources are displayed in a particular portlet:
1 Filter the list of resources:
   a From the View drop-down list, select an inventory type.
   b From the All Types drop-down list, select a value.
      Note: Not all inventory types support filtering by value.
   c In the Filter By Name field, enter part of the resource’s name.
   d Click (directly to the right of the Filter By Name field).
2 Use the check boxes and arrows to move items between the Resources and the Add Resources lists.
3 Click OK.

Platform: Scan
To initiate a platform scan, select New Auto-Discovery from the platform’s Tools menu. For detailed instructions, see Scan a Platform on page 30.

Resource: Assign to Groups
To assign a resource to resource groups, use the check boxes and arrows to move groups to the Add To Groups list. For detailed instructions, see Assign a Resource to Resource Groups on page 27.

Service Dependencies
The Service Dependency page is not used by SAS Environment Manager.

About the Manage Page

Introduction
Use the Manage page to perform administrative tasks that are specific to maintaining SAS Environment Manager.

The following topics provide information about the three sections of the Manage page.

Authentication and Authorization
This section enables administrators to view and interactively manage user accounts and role for SAS Environment Manager.

Although it shares the same authentication provider as the rest of a SAS deployment, SAS Environment Manager has its own user registry.
SAS Environment Manager user definitions and roles are mapped to user definitions created in SAS metadata. SAS Environment Manager users are created by first creating the user definition in metadata and then synchronizing the user information with SAS Environment Manager. You cannot create user definitions in SAS Environment Manager directly.

Users in SAS Environment Manager are mapped to users created in SAS metadata. During installation, three user groups are created in SAS metadata to contain SAS Environment Manager users. Users that are members of these groups are mapped to user definitions in SAS Environment Manager with corresponding roles. The user groups and their corresponding roles are as follows:

<table>
<thead>
<tr>
<th>Group name in SAS metadata</th>
<th>Role in SAS Environment Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAS_EV_Super_User</td>
<td>Super User Role</td>
</tr>
<tr>
<td>SAS_EV_Guest</td>
<td>Guest Role</td>
</tr>
<tr>
<td>SAS_EV_AppServer_Tier</td>
<td>SAS App Tier Role</td>
</tr>
</tbody>
</table>

For example, users added to the group SAS_EV_Guest are added as users in SAS Environment Manager under the Guest role when the users are synchronized.

After you have defined new users in SAS metadata, sign on to SAS Environment Manager, and select Manage Synchronize Users. User definitions are created for all users that are defined in the three SAS_EV groups in metadata. Any SAS Environment Manager users that are not associated with user definitions in metadata are deleted.

If you sign on to SAS Environment Manager using a user ID that is defined in metadata, is a member of one of the SAS_EV groups, but is not defined in SAS Environment Manager, then a user definition is automatically created in SAS Environment Manager and assigned to the correct role.

To create a new SAS Environment Manager user, use an application such as SAS Management Console to define the user and assign it to the appropriate SAS_EV user group, and then select Manage Synchronize Users to create the user in SAS Environment Manager and assign the user to the proper role.

Server Settings
This section provides access to the following functionality:

Server Settings
includes settings for e-mail, announcements, data compression, and database maintenance. See Server Settings on page 94.

Monitoring Defaults
defines monitoring and alerting policies for the entire environment

**Note:** Metric collection settings that are defined here can be over-written for an individual resource. However, such changes do not persist when type-level defaults are updated. Each time you update the monitoring configuration for a resource type, the settings for each individual resource of that type are updated. See Monitoring Defaults on page 99.

Escalation Schemes Configuration
defines global escalation schemes that can be applied to individual alerts. See Alert Escalations on page 43.

Plug-in Manager
provides deployment-wide management of plug-ins.

Plug-ins
Plug-ins are Groovy-based extensions that can be incorporated into SAS Environment Manager as follows:
A plug-in can be a view within the Views page for a particular resource type.

A plug-in can be a menu item on a top-level page (such as Resources)

A plug-in can be an addition to the Plugins section of the Manage page.

The following table introduces SAS Environment Manager’s built-in plug-ins:

<table>
<thead>
<tr>
<th>Plug-in</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network and Host Dependency Manager</td>
<td>Defines the relationship between platforms and network hosts or devices. See Define Platform Dependencies on page 32.</td>
</tr>
<tr>
<td>Groovy Console</td>
<td>Enables users to run Groovy code directly. See Groovy Console on page 87.</td>
</tr>
<tr>
<td>Health</td>
<td>Provides real-time diagnostic data (used by technical support for troubleshooting). See Diagnostics for Auto-Discovery on page 91.</td>
</tr>
<tr>
<td>Web Services API</td>
<td>Provides programmatic and command-line access</td>
</tr>
<tr>
<td>tc Server Command-line Interface</td>
<td>Provides a command-line interface to tc Server configuration and application deployment tasks. See tc Server Client on page 84.</td>
</tr>
</tbody>
</table>

**Licenses Usage Status**

This section lists the license information for the SAS Environment Manager server:

**Platform usage**

The number of platforms that are currently managed by SAS Environment Manager compared to the number of platforms the license allows SAS Environment Manager to manage.

Typically, a single agent consumes a single license. If an agent manages a vSphere vCenter instance, it consumes a license for the platform that hosts vCenter, a license for each vSphere vHost administered by the vCenter instance, and if an agent is installed in each VM a license for each vSphere VM on each vHost.

**Platform Properties**

To change a platform’s properties, click Edit in the **Type and Network Properties** section of the platform’s Inventory page.

Platform properties are as follows:

**Platform Type**

- type of platform

  **Note:** You cannot change a platform’s type.

**Agent Connection**

The IP address:port pair that the inventory server uses to connect to the agent on the platform device. In the case of a platform type that is monitored by an agent on a different platform (such as a network or virtual host), this property identifies the agent that manages the platform.

**Fully Qualified Domain Name**

- the platform’s FQDN
IP Address, MAC Address, Netmask

One or more sets of identifiers for the platform. There is at least a minimum one set for the loop back (local) IP address 127.0.0.1 and then additional sets for each network interface on the device.

Server Inventory Page

Server Inventory Page Header

Map Control for a Server

Click the Map control in the page header to view the server's child services and its parent platform. Click the name of a child or parent resource to view its Monitor page.

Tools Menu for a Server

For a server, the Tools menu has the following commands:

Configure Server

Opens the Configuration Properties page for the server, where you can edit the resource's configuration properties.

Delete Server

Delete the server and all its child services from inventory. The server itself is not deleted, but is only removed from inventory. You can rediscover it later if you want to return it to inventory.

New Service

Displays the New Service page, where you can manually add a new child service to the server. (For example, a service that was not auto-discovered.)

Add to Dashboard Favorites

Adds the server to the Favorite Resources portlet on the currently selected dashboard.

Add to Group

Opens the Group Manager page, which lists any compatible groups of the same type as the server.

Schedule Downtime

Opens the Schedule Downtime window, which enables you to schedule the date and time range for when the server should be taken down.

General Properties for a Server

The General Properties section of the Inventory page for a server lists the description, resource type, date created, date modified, and modified by for the server. The Type and Host properties section lists the install path and the host platform.

Services for a Server

The Services section of the Inventory page for a server lists all of the services running on the server, their types, and their availability.

Groups for a Server

The Groups containing this resource section of the Inventory page for a server lists all of the groups that contain the server.

Configuration Properties

The Configuration Properties section of a server's Inventory tab contains three sections:
Shared properties that relate to more than one management function

Monitoring properties that related to log tracking, configuration tracking, and auto-discovery of child services

Control any configuration properties that are required to enable any supported resource control actions (for example, the path of the start script to use to start a server)

Note: For some types of resources, you might need to supply configuration property values to enable monitoring.

See Also
- Add a Server on page 24
- Resource Management: Overview on page 22

Application Inventory
The Service Counts section displays the total number of services in the application and the number of services of each type.
The Services section lists key information for each service in the application.

See Also
- Add an Application on page 26
- Assign Services to an Application on page 27
- Resource Management: Overview on page 22

Resource Group Inventory Page
The Roles Assigned To section lists the roles to which the group is assigned. These assignments affect access to the resources within the group.

See Also
- Add a Resource Group on page 26
- Assign a Resource Group to Roles on page 27
- Resource Management: Overview on page 22

Resource: Name and Description
To edit a resource’s name or description.

1. On the resource’s Inventory tab, in the General Properties section, click Edit.
2. Make changes as needed.
3. Click OK.
Resource: Views Page

The Views page for a resource is the attachment point for plug-ins for a resource type. This page has a link for each plug-in that is attached to the current resource type.

If there are no plug-ins available for the type of resource that is currently selected, the Views page has no links.

Service Inventory Page

See the following links:
- Add a Service on page 24
- Assign Services to an Application on page 27
- Resource Management: Overview on page 22

Platform Inventory Page

See the following links:
- Add a Platform on page 24
- Clone a Platform on page 31
- Resource Management: Overview on page 22

Resource Properties

Introduction

On a resource’s Inventory page, the Configuration Properties section contains the configuration options and currently selected values for the resource. The following list provides details:

Shared
- these properties relate to more than one management function (for example, a property might affect both monitoring and control actions)

Monitoring
- these properties set options that are related to log tracking, configuration tracking, auto-discovery of child services for servers

Control
- if resource control actions are supported for the currently selected resource type, any configuration properties that are required to enable resource control are listed here (for example, the path of a start script to use to start a server)

To open the Edit Configuration Properties page for the currently selected resource, click Edit.

Note: If a resource type requires user-supplied configuration property values, configuration instructions should be available at the bottom of the Configuration Properties for a resource of that type.

Control Properties

If enables control actions are supported for a resource, a Control section of the Configuration Properties page lists any properties that are required or supported for those actions. For example, if SAS Environment Manager
can perform a **start** command for a server type, there is usually an optional property that you can use to supply command arguments.

**See Also**
Resource Management: Overview on page 22

### Application Properties

To edit an application's properties, click **Edit** in the **Application Properties** section of the application's **Inventory** page. Enter or update contact information and click **OK**.

**See Also**
Resource Management: Overview on page 22

### Server Properties

To change a server's properties, click **Edit** in the **Type & Host Properties** section of its **Inventory** page.

**Note:** The installation path for each server instance that is of the same type and on the same platform must be unique. For auto-discovered servers, the plug-in sets the value of the **Install Path** property and uses it as the basis for the resource's auto-inventory identifier.

**TIP** The install path for a manually created server does not have to be the actual installation path for the server. The only requirement is that all servers that are of the same resource type and on the same platform have unique install path property values.

**See Also**
Resource Management: Overview on page 22

### Edit an Alert

On the **Alert Definition** page, you can edit an alert definition's properties, conditions, and actions.

For details, see:

### Alert Details

A triggered alert's **Alert Detail** page displays the underlying alert definition, indicates what actions have been performed, and shows any comments that were supplied when the alert was acknowledged or fixed.

The following list provides details:

**Alert Properties**
- the name of the alert definition, the resource for which the alert fired, the priority of the alert, when it fired, and whether it has been fixed. You can click the alert definition name to view or edit it, or click the resource name to see its **Indicators** page.

**Condition Set**
- the metric value or event that triggered the alert

**Control Action**
- if a resource control action was performed when the alert triggered, that action is listed
Notification Actions
the recipients for notifications

Escalation
if the alert has an escalation, lists the actions that have been defined for the escalation and a log of any steps that are performed (including any acknowledgment notes)

Fix
if the alert has been marked as fixed, lists the user that fixed it and any comments that were entered. If the alert was fixed by a recovery alert, this section indicates that the problem fixed itself.

To fix an unfixed alert, enter comments about the alert resolution and click **Fixed** at the bottom of the page.
To acknowledge an unacknowledged escalated alert, click the **Acknowledge** icon in the **Escalation** section.

Environment Snapshot
The Environment Snapshot plugin enables you to quickly view system information and take snapshots of the displayed information. It collects and displays performance measurement data and configuration parameters from the SAS Environment Manager database, and also executes and gathers information from various live-exec commands such as Top, Who, and Df. The plugin also displays information about the SAS Environment Manager Data Mart.

Before using the plugin, use the Auto-Discovery portlet to add the System Info resources to your inventory. These resources are supplied with the plugin. They are configured for each platform in your environment and collect additional system data.

Use the **Select a System** menu to choose the platform whose performance data you want to view.
Click **Snapshot Environment** to save all of the environment data to a text file. By default, live system queries, events, and alerts are not included in the snapshot file. To add them to the file, select the checkboxes beside the items you want to include, then click "Snapshot Environment."

**Note**: Because the plugin queries the SAS Environment Manager database, taking a snapshot might take several minutes, depending on the size of the installation and the number of machines being monitored by your environment.

After you create a snapshot file, the location of the file is displayed in the plugin.

APM Static Reports
The Audit, Performance and Measurement reports enable you to analyze auditing and usage information for a SAS Business Intelligence environment. The reports are divided into two groups:

**Audit Reports**
enable you to analyze SAS Metadata Server authentication patterns, user sign in behaviors, authorizations changes and authentication or permission errors. You can also use these reports to detect fraudulent attempts to access analytic services.

**Performance Reports**
enable you to perform fine-grained analysis of various performance metrics for the analytic servers. Metrics include the ability to identify the most active users of the system, processor utilization, memory utilization and response time for the servers. Reports are also provided to analyze access data for SAS procedures, SAS stored processes and SAS data libraries.

To view a report, click on an entry in the **Report URL** column.

Register User
If the metadata for a particular user does not include values for display name or email address, the Register User window appears when you first sign into SAS Environment Manager as that user.
Specify the requested information. Information that is required is marked by a red asterisk. When you click **Save Changes**, the information is stored, and you will not be prompted for it again.

After to enter the information and click **Save Changes**, the Dashboard appears and you can use SAS Environment Manager normally.

**Help Not Yet Available**

This is a feature that has been added between releases of SAS Environment Manager. Help is not yet available for this page, but will be added during the next release of the product. Go to [http://support.sas.com/md/emi/index.html](http://support.sas.com/md/emi/index.html) for current information for this feature.