



SAS® Environment Manager 2.4: User's Guide

The correct bibliographic citation for this manual is as follows: SAS Institute Inc. 2014. *SAS® Environment Manager 2.4: User's Guide*. Cary, NC: SAS Institute Inc.

SAS® Environment Manager 2.4: User's Guide

Copyright © 2014, SAS Institute Inc., Cary, NC, USA

All Rights Reserved. Produced in the United States of America.

For a hard copy book: No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, or otherwise, without the prior written permission of the publisher, SAS Institute Inc.

For a web download or e-book: Your use of this publication shall be governed by the terms established by the vendor at the time you acquire this publication.

The scanning, uploading, and distribution of this book via the Internet or any other means without the permission of the publisher is illegal and punishable by law. Please purchase only authorized electronic editions and do not participate in or encourage electronic piracy of copyrighted materials. Your support of others' rights is appreciated.

U.S. Government License Rights; Restricted Rights: The Software and its documentation is commercial computer software developed at private expense and is provided with RESTRICTED RIGHTS to the United States Government. Use, duplication, or disclosure of the Software by the United States Government is subject to the license terms of this Agreement pursuant to, as applicable, FAR 12.212, DFAR 227.7202-1(a), DFAR 227.7202-3(a), and DFAR 227.7202-4, and, to the extent required under U.S. federal law, the minimum restricted rights as set out in FAR 52.227-19 (DEC 2007). If FAR 52.227-19 is applicable, this provision serves as notice under clause (c) thereof and no other notice is required to be affixed to the Software or documentation. The Government's rights in Software and documentation shall be only those set forth in this Agreement.

SAS Institute Inc., SAS Campus Drive, Cary, NC 27513-2414

February 2018

SAS® and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration.

Other brand and product names are trademarks of their respective companies.

P3:evug

Contents

<i>What's New in SAS Environment Manager 2.4</i>	<i>ix</i>
--	-----------

PART 1 Understanding SAS Environment Manager **1**

Chapter 1 / Introduction to SAS Environment Manager	3
What is SAS Environment Manager?	3
Resource Inventory Model	8
Deciding Which Components to Initialize	11
Chapter 2 / Finding Your Way Around	13
Finding Your Way Around	14
Viewing Important Information at a Glance: the Dashboard	14
Monitoring Platforms, Servers, and Services: the Resources Pages	15
Monitoring Resources: the Analyze Pages	17
Performing SAS Tasks: the Administration Page	23
Configuring SAS Environment Manager: the Manage Page	24
Chapter 3 / Viewing Information at a Glance: Using the Dashboard	27
Using the Dashboard	28
Customizing Your Dashboard	31
Summary Portlet Examples	32
Metric Viewer Portlet Examples	36
Metric Chart Examples	43
Chapter 4 / Finding Resources in Your System	51
Automatically Discovering and Adding SAS Resources	51
Using the Auto-Discovery Portlet	52
Performing an Auto-Discovery Scan	53

Rediscovering Resources	53
Manually Adding a Server	54
Manually Configuring a Service	55
Chapter 5 / Monitoring and Controlling Resources	57
Monitoring Resources	57
Managing SAS Resources	60
Making Resources Easier to Locate	62
Controlling Resources Using Control Actions	65
Chapter 6 / Working with Events and Alerts	69
Creating Resource Events	69
Importing and Exporting Events	72
Working with Resource Alerts	75
Chapter 7 / Controlling Access to SAS Environment Manager	83
Controlling Access to SAS Environment Manager	83
Creating SAS Middle-Tier Administrator IDs	88
<div> PART 2 Operations Integration, Audits, and Performance Analysis 89 </div>	
Chapter 8 / Understanding SAS Environment Manager Service Management Architecture	91
Understanding SAS Environment Manager Service Management Architecture	92
Working with SAS Environment Manager Extended Monitoring	94
Working with APM ETL	96
Working with ACM ETL	97
Working with the Solution Kits Infrastructure	98
Feeding Data from the Data Mart into SAS Visual Analytics	98

Chapter 9 / Initializing and Enabling the Service Management Architecture	101
Initializing SAS Environment Manager Extended Monitoring	101
Enabling and Initializing the APM ETL	104
Enabling ACM ETL	109
Enabling Kits Infrastructure	110
Chapter 10 / Using the Report Center	111
What is the Report Center?	111
Use the Report Center	112
Change Report Parameters	115
Finding the Reports You Need	115
Chapter 11 / Working With Commands	121
Performing Functions by Using a Command Line	121

PART 3 SAS Metadata Administration 135

Chapter 12 / Managing User Access	137
Features in User Administration	138
Introduction to User Administration	139
Access User Management	149
Add a User	150
Add an Administrator	152
Add a Custom Group	152
Add a Custom Role	153
Assign Members to a Group or Role	153
Update the Stored Password in a Login	154
Delete an Identity	154
Store DBMS Credentials	155
Adjust Policies for an Internal Account	156
Chapter 13 / Managing Metadata Access	157
Features in Access Management	158

Concepts in Access Management	160
Icons in Access Management	167
Permissions Inspector	170
Permission Origins	171
Access Control Inheritance	175
Permission Condition	178
Best Practices for Permissions	180
Manage Metadata Information	182
Apply an ACT	183
Create an ACT	183
Update an ACT	184
Add an Explicit Grant or Denial	186
Add a Row-Level Permission Condition	187
Provide Fine-Grained Access Using Permission Conditions	187

PART 4 Appendixes 189

Appendix 1 / Troubleshooting	191
Resolving Problems with SAS Environment Manager	191
Resolving Problems with SAS Environment Manager Agents	194
Resolving Problems with SAS Environment Manager Plugins	196
Appendix 2 / Manual Setup Examples	199
Alert Definition Examples	200
Manually Configuring HTTP Components and Applications	202
Appendix 3 / Data Mart Table Reference	211
About SAS Environment Manager Data Mart Tables	212
ACM Tables	213
APM Tables	219
Solution Kits Table	226
Recommended Reading	229

Index **231**

What's New

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 for collecting and storing operational 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 into the SAS Visual Analytics 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 provides information that helps these systems make this determination. The SAS environment requires one external account

ID for each user. The SAS environment uses its copy of this ID to establish a unique SAS identity for each user. All of a user's group memberships, role memberships, and permission assignments are associated with this 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.



Part 1

Understanding SAS Environment Manager

<i>Chapter 1</i>	
<i>Introduction to SAS Environment Manager</i>	3
<i>Chapter 2</i>	
<i>Finding Your Way Around</i>	13
<i>Chapter 3</i>	
<i>Viewing Information at a Glance: Using the Dashboard</i>	27
<i>Chapter 4</i>	
<i>Finding Resources in Your System</i>	51
<i>Chapter 5</i>	
<i>Monitoring and Controlling Resources</i>	57

Chapter 6

<i>Working with Events and Alerts</i>	69
--	-----------

Chapter 7

<i>Controlling Access to SAS Environment Manager</i>	83
---	-----------

Introduction to SAS Environment Manager

<i>What is SAS Environment Manager?</i>	3
<i>Resource Inventory Model</i>	8
Overview	8
Platforms	8
Servers	9
Services	10
<i>Deciding Which Components to Initialize</i>	11

What is SAS Environment Manager?

SAS Environment Manager is a web-based administration solution for a SAS environment. The application enables you to perform these tasks:

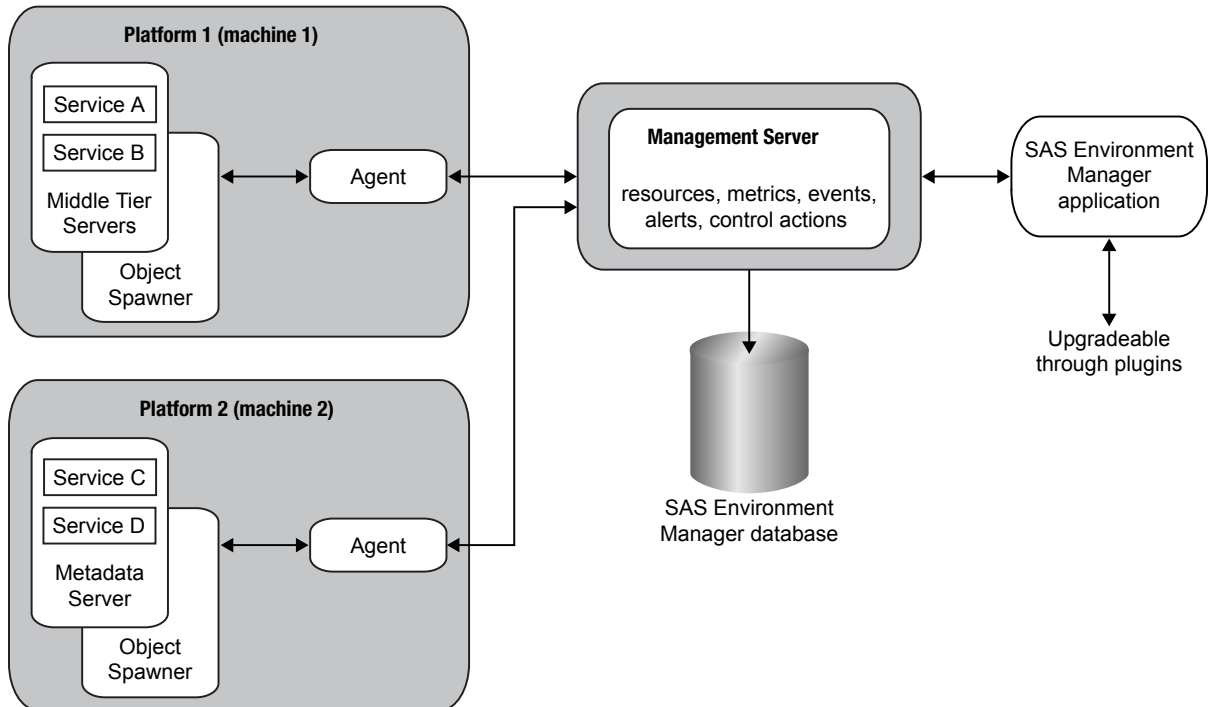
- administer, monitor, and manage SAS resources, including administering the SAS Web Application Server and monitoring SAS foundation servers
- collect and chart data on metrics for monitored SAS resources, which creates a comprehensive view of resource health and operation
- monitor log events and reporting alerts

- manage resources and definitions in SAS metadata, including authorization and user definitions
- Incorporate the monitoring and managing of IT and SAS resources into a service management strategy by using the detailed metric information stored in the SAS Environment Manager Data Mart and the reports provided in the Report Center

SAS Environment Manager agents run on all SAS platforms except for z/OS.

SAS Environment Manager is based on VMWare's Hyperic product, with customizations and plugins to optimize the product specifically for a SAS environment. Some terms and concepts used in SAS Environment Manager are different than in other parts of SAS, but these are noted in this document.

The basic architecture of SAS Environment Manager consists of an agent process running on each platform in a SAS deployment that communicates to a central management server. Agents monitor detected resources and periodically report resource metrics back to the server. The server provides an interface for interacting with those agents, managing the data collected by the agents, distributing plugins, creating alerts and escalation procedures based on collected metrics, and graphing the metrics provided through the installed plugins.



There are five main components to SAS Environment Manager:

agent

An agent is a software process that runs on each platform (middle-tier and server-tier machine) in a SAS deployment. The agent is responsible for tasks such as discovering software components on its platform, gathering metric and availability data for the platform and components, and performing resource control actions. The agents communicate with the management server. Plugins are used to provide the agents with the information needed to discover SAS resources installed on a platform.

management server

The management server is responsible for communicating with the agents. It collects information about items such as discovered resources, metrics, and availability, and issues control actions received from the SAS Environment Manager application. Collected data is stored in the SAS Environment Manager database.

SAS Environment Manager database

The database is a Postgres database that is a repository for all of the information about all of the resources known to SAS Environment Manager. It uses the SAS Web Infrastructure Platform Data Server, which is based on PostgreSQL. After resources are discovered and added to your inventory, the database stores data collected from the agents about the resources.

SAS Environment Manager application

The application is the web-based interface to the SAS Environment Manager system. Resources discovered by the agents and added to the inventory are displayed and monitored. Metric and availability data collected by the agents and stored in the database is displayed and charted. Events and metric data are used to generate alerts. Control actions are sent back through the management server to the agents to control resources on the platforms. The application also includes a framework to add functions specific to SAS, such as server, library, and user administration.

plugins

Plugins enable agents to discover and monitor resources in a SAS environment. Each plugin is associated with a specific resource, and provides the agents with the instructions needed to recognize the resource during auto-discovery and to monitor and collect metrics for the resource.

Although open-source plugins are available for VMWare Hyperic, these plugins are not supported by SAS Environment Manager. You should use only plugins provided by SAS.

Beginning with SAS Environment Manager 2.4, the component SAS Environment Manager Data Mart Performance and Usage Reporting is also included. Extract, transform and load (ETL) processes obtain metric information from the SAS Environment Manager agent and from SAS logs, standardize the data, and store the data in the SAS Environment Manager Data Mart. From there, the data is used to produce predefined reports in the Report Center.

The basic framework for SAS Environment Manager Service Management Architecture is provided by SAS Environment Manager Extended Monitoring. In addition to providing the infrastructure for the SAS Environment Manager Data Mart and the Report Center, the Extended Monitoring package includes predefined alerts, groups, and logging

configurations. Initializing Extended Monitoring automates the task of setting up SAS Environment Manager, and enables you to start using the application right away.

SAS Environment Manager is based on VMware's Hyperic product, with customizations and plugins to optimize the product specifically for a SAS environment. Some terms and concepts used in SAS Environment Manager are different than in other parts of SAS, but these are noted in this document.

SAS Environment Manager is licensed for and restricted to the monitoring and management of SAS Technologies, solutions, and the necessary associated supporting infrastructures. SAS Environment Manager agents can be installed on any machines that host software or data on which your SAS environment depends. However, agents installed on machines that do not host SAS software are restricted to monitoring basic hardware and operating system resource metrics. Although SAS Environment Manager is based on VMware's Hyperic product, only plugins and customizations specifically delivered with and deployed by SAS software may be installed in SAS Environment Manager. See the [SAS Environment Manager Plugins page on support.sas.com](https://support.sas.com/sas-environment-manager-plugins) for a complete listing of supported plugins. Other SAS Environment Manager uses are restricted in accordance with your SAS Master License Agreement.

SAS Environment Manager, its reports, and supporting data are provided to assist in the troubleshooting and performance tuning of SAS environments. Although audit, access, and connectivity data and reports are provided, SAS does not provide a guarantee as to their completeness. If you require more extensive and comprehensive audit, access, and connectivity data, please contact SAS Professional Services for assistance.

Note: SAS Environment Manager and the SAS Environment Manager Service Architecture use a collection of data sets to store collected metric data and information that is used to create reports. If you notice that a data set that is associated with SAS Environment Manager is not being updated, this is not necessarily an indication of an error. A data set might not be updated because it is no longer being used, or because the event that it is collecting data for has not occurred.

Resource Inventory Model

Overview

The SAS Environment resource inventory model contains three levels:

platform

A container such as an operating system or a SAS server tier that holds servers and services

server

Software product or process, such as a SAS Metadata Server, that runs on a platform

service

A task-specific software component, such as a SAS logical server, that runs on a server or platform

Platforms

Platforms are the highest level of resource type in SAS Environment Manager. They are containers that host other software and services. There are three major categories of platforms:

- operating system platforms
- SAS Application Server Tier
- virtual and network platforms

An operating system platform consists of a computer (physical or virtual) and the operating system that runs on it. The SAS Environment Manager uses the system plugin to teach the agent how to auto-discover the operating system platform. You cannot manually add an operating system platform to inventory. SAS Environment Manager supports most of the operating systems on which SAS is supported.

The SAS Application Server Tier platform is an instantiation of a SAS deployment and a collective store of deployment-wide information such as license information and clustering. Resources in the SAS Application Server Tier platform include SAS Metadata Server and SAS Application Server and their logical servers (such as SAS Workspace Servers, SAS OLAP Servers, and SAS Stored Process Servers). The agent automatically discovers and creates the SAS Application Server through direct communication with the SAS metadata server as a platform resource.

Virtual and network platforms include a variety of platform types that do not map to an individual physical machine running a traditional operating system and are managed by an agent proxy. These include the following:

- resources that an agent monitors remotely over the network, such as network hosts and devices
- virtual resources such as VMware vSphere hosts and virtual machines
- distributed sets of resources, such as GemFire Distributed Systems

The agent does not automatically discover platforms other than the host operating system and the SAS Application Server Tier. You must manually create other platforms or supply resource properties data that enable the agent to manage them. Below are the virtual and network platform types that SAS Environment Manager supports:

- Cisco IOS
- GemFire Distributed System
- Network Device
- Network Host
- VMware vSphere Host
- VMware vSphere VM

Servers

In SAS Environment Manager, a server is commonly a software product or process that runs on a platform. Servers provide a communication interface and perform specific tasks upon request. The Monitoring Defaults page on the **Manage** tab lists all of the

server types (along with platform and service types) that SAS Environment Manager supports.

Most server types are auto-discovered by a server type-specific SAS Environment Manager plugin. If the plugin that manages a server does not support auto-discovery, or if auto-discovery of a server fails, you might need to manually create a server. See [“Manually Adding a Server” on page 54](#).

Examples of server types include the following:

- SAS Metadata Server
- SAS Object Spawner
- Postgres server
- SAS Home Directory Service

Services

In SAS Environment Manager, a service is a software component dedicated to a particular task that runs on a server or platform. A service that runs on a server is a service, and a service that runs on a platform is a platform service.

The resource plugin that discovers a platform or server also discovers key services, such as CPUs, network interfaces, and file systems that are running on the platform.

You can also configure a platform service that serves as a proxy for a resource that the SAS Environment Manager agent can monitor over the network. Examples include

- DNS service
- POP3 service
- Fileserver mount
- Windows service
- Network host storage

For more information, see [“Manually Configuring a Service” on page 55](#).

Services that run on a server can be either an internal component of the server or a deployed item. Logical SAS servers are considered to be services that run on SAS server resources. Examples of services that run on servers include the following:

- PostgreSQL database
- SAS Object Spawner
- SAS Logical Workspace Server
- SpringSource tc Runtime Cache

The Monitoring Defaults page on the **Manage** tab lists the supported platform service types (along with platform types and server types) provided by the installed plugins.

Deciding Which Components to Initialize

After you have used the SAS Deployment Wizard to install SAS Environment Manager, you must perform additional steps to configure resources (either automatically or manually), create the dashboard, and enable SAS Environment Manager Service Management Architecture. The following steps outline the process.

- 1 After the installation process has completed, sign on to SAS Environment Manager. The application autodiscovers the resources in your environment.
- 2 Decide whether you want to enable SAS Environment Manager Extended Monitoring. If you enable Extended Monitoring, SAS Environment Manager is automatically set up by using tuned resource configurations, alert definitions, and metrics. The SAS Environment Manager Data Mart infrastructure is also configured, so if you plan to use the Data Mart, you must enable Extended Monitoring. If you choose to not enable Extended Monitoring, you must configure resources and define alerts manually.
- 3 If you choose to use Extended Monitoring, run the command to enable Extended Monitoring. See [“Initializing SAS Environment Manager Extended Monitoring” on page 101](#) for more information..

- 4** If you choose not to use Extended Monitoring, you must manually configure the resources in SAS Environment Manager and manually define alerts. See [Appendix 2, “Manual Setup Examples,” on page 199](#) for examples.
- 5** Set up your dashboard. See [“Using the Dashboard” on page 28](#).
- 6** If you decided to use SAS Environment Manager Service Management Architecture, you must decide what type of data you want to populate the SAS Environment Manager Data Mart with. APM ETL provides forensic data from SAS logs, ACM ETL provides real-time data from the computing resources in your environment, and solution kits ETL provide data specific to individual SAS solutions. If you initialize and enable Extended Monitoring and all three ETL components, you will obtain the most complete and comprehensive view of your system. However, initializing all of these components does consume more resources and impact performance.
- 7** If you are populating the SAS Environment Manager Data Mart with forensic data from SAS logs, initialize and enable APM ETL. See [“Enabling and Initializing the APM ETL” on page 104](#). You can perform this step at any time, not just during the initial setup.
- 8** If you are populating the SAS Environment Manager Data Mart with current data from the computing resources in your SAS environment, enable ACM ETL. See [“Enabling ACM ETL” on page 109](#). You can perform this step at any time, not just during the initial setup.
- 9** If you are using solution kits, enable the solution kits ETL. See [“Enabling Kits Infrastructure” on page 110](#). You can perform this step at any time, not just during the initial setup.

Finding Your Way Around

<i>Finding Your Way Around</i>	14
<i>Viewing Important Information at a Glance: the Dashboard</i>	14
<i>Monitoring Platforms, Servers, and Services: the Resources Pages</i>	15
<i>Monitoring Resources: the Analyze Pages</i>	17
Overview	17
Alert Center	18
Event Center	19
Operations Center	20
Environment Snapshot	21
Report Center	21
<i>Performing SAS Tasks: the Administration Page</i>	23
<i>Configuring SAS Environment Manager: the Manage Page</i>	24
Overview	24
Authentication/Authorization	24
Server Settings	24
Plugins	25
License Usage Status	25

Finding Your Way Around

The SAS Environment Manager interface is organized around five main areas, as illustrated in this figure:

The following table describes the main functional areas of SAS Environment Manager:

Main Page	Contents
Dashboard	Configurable collections of portlets; this is the initial view when starting SAS Environment Manager.
Resources	Resource-level monitoring and management.
Analyze	Deployment-wide views of events and alerts.
Administration	Metadata folders, basic properties of metadata objects, security and access controls
Manage	Native users, roles, permissions, plugins.

Viewing Important Information at a Glance: the Dashboard

The Dashboard is the starting point when you sign in to SAS Environment Manager. The page consists of a collection of views (called portlets) of resources and metrics that are the most important to your environment. The Dashboard is customizable, so you can specify how many portlets are displayed, which metrics and functions they present, and which resources they cover. For example, your Dashboard could contain a portlet to display recently auto-discovered resources, a portlet to display recent alerts, or a portlet to display the availability of a group of selected servers. Selecting an entry (such as a resource or an alert) in a portlet takes you to detailed information about the entry.

Each user can access their own personal Dashboard as well as a Dashboard for each of the native roles of which the user is a member. Each Dashboard can be customized to meet the needs of the user or role. For more information about roles, see [“About Native Roles and Users”](#) on page 83.

An example Dashboard page is displayed in this figure.

Figure 2.1 Example Dashboard

The screenshot displays the SAS Environment Manager interface. At the top, the header includes the SAS logo, 'Environment Manager', and navigation links like 'Welcome, i10', 'Sign Out', and 'Help'. Below the header is a navigation bar with tabs: 'Dashboard', 'Resources', 'Analyze', 'Administration', and 'Manage'. The main content area is divided into several sections:

- Select a Dashboard:** A dropdown menu set to 'Super User Role' and a 'Make Default' button.
- Auto-Discovery:** A section indicating 'No resources to display'.
- Recent Alerts:** A table listing alerts with columns for Date / Time, Alert Name, Resource Name, Fixed, and Ack. The table shows three alerts: 'Supervisor Failure' (02/28/2013 11:10 AM), 'I/O Subsystem' (02/28/2013 11:00 AM), and 'Log Monitoring' (02/27/2013 02:01 PM and 02/27/2013 01:33 PM). Buttons for 'Fixed' and 'Acknowledge' are at the bottom.
- Problem Resources:** A section indicating 'No resources to display'.
- Recently Added:** A section indicating 'No resources to display'.
- Add content to this column:** A dropdown menu set to 'Select Portlet' and a plus icon.
- Control Actions:** A table listing control actions with columns for Resource Name, Control Action, Date / Time, and Message. The table shows two actions: 'Resume' (02/25/2013 11:56 AM) and 'Pause' (02/25/2013 11:56 AM).
- Quick Control Frequency:** A table listing the frequency of control actions with columns for Resource Name, # of Control Actions, and Most Frequent Control Action. The table shows two entries: 'Resume' (2 actions) and 'Pause' (2 actions).

Monitoring Platforms, Servers, and Services: the Resources Pages

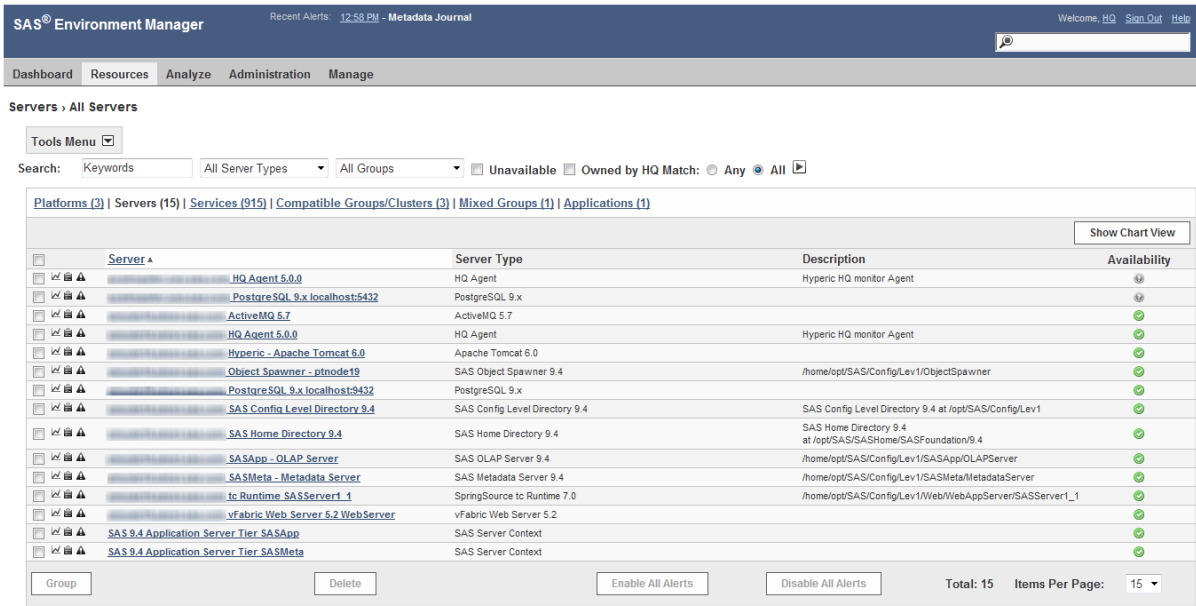
Use the **Resources** pages to monitor, configure, and manage inventory resources. The main Resources page lists the inventory of resources, organized by type:

- Platforms
- Servers
- Services

- Compatible Groups/Clusters
- Mixed Groups
- Applications

Other selections under Resources enable you to view only resources that are currently down or to select from recently viewed resources. This figure shows a server resource list.


Figure 2.2 Resource List



The icons on the left of the resource name enable you to quickly jump to the Monitor, Inventory, or Alerts page for the resource. Selecting the resource name displays the Monitor page for the resource. A lock icon indicates that, because of your permissions, a particular feature is not available for a particular resource.

Use these strategies to locate resources on the **Resources** page:

- Only one inventory type is displayed at a time. To access resources of a different inventory type, click a link in the table header.

- To further limit the display, you can 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 you own, select the **Owned by** check box.
- There might be multiple pages of resources in the list. Use the controls below the list to navigate.
- You can use **Resources** ► **Recently Viewed** ► *the page name* to quickly return to a page that you recently viewed.
- As an alternative to browsing and filtering on the **Resources** page, you can use the search field (on the right side of the application banner) to quickly locate a resource by its name.
- To view a list of resources that are not currently available, select **Resources** ► **Currently Down**.
- You can initiate resource management tasks from the **Resources** page.

Monitoring Resources: the Analyze Pages

Overview

The **Analyze** pages contain the Alert Center, the Event Center, the Operations Center and the Environment Snapshot. If you have enabled SAS Environment Manager Data Mart Performance and Usage Reporting, the Report Center is also included. These pages enable you to quickly view and work with alerts, events, system status, and performance and usage reporting throughout your system.

An event is any sort of activity in a resource that you are monitoring. Alerts are a user-defined type of event that acknowledges a critical condition in a selected resource. You can configure SAS Environment Manager to also log events for log messages and resource configuration changes.

Alert Center

The Alert Center page provides a deployment-wide view of alerts and alert definitions.

The default view of the Alert Center is the **Alerts** tab, which displays a table with information about currently active alerts. You can use the filter controls to filter by criteria such as status, type, and priority. Clicking on an entry in the **Alert Definition** column in the table displays detailed information about the alert.

To access the Alert Center, select **Analyze ► Alert Center**.

Alert Center

AlertsDefinition

Alert Filter

Show:

☐ Not Fixed

☐ In Escalation

☒ All

Alert type:

Resource

Minimum priority:

Low

In the last:

day

Group:

-- All Groups --

Resource Alerts

PreviousPage 1Next

<input type="checkbox"/>	Date	Alert Definition	Resource	Platform	Fixed	Ack	Priority
<input type="checkbox"/>	3/25/13 9:55 AM	Host Credentials	Object Spawner - ptnode20		No		Med
<input type="checkbox"/>	3/25/13 3:47 AM	Stored Process Canceled	Object Spawner - ptnode20 SASApp - Stored Process Server		No		Med
<input type="checkbox"/>	3/24/13 7:45 PM	Server Not Running	Object Spawner - ptnode20 SASApp - Pooled Workspace Server		No		Med
<input type="checkbox"/>	3/24/13 4:45 PM	Server Launch	Object Spawner - ptnode20		No		Med

Fixed

Acknowledge

Click the icon to acknowledge an alert

Although you can select the check box next to an alert and click **Fixed** to identify the problem as having been corrected, the Detail page for the alert enables you to not only mark the alert as fixed, but also to enter information about the resolution of the alert.

Object Spawner - ptnode20 SASApp - Stored Process Server: Stored Process Canceled: Alert Detail

[<< Resource Alert List](#)

Alert Properties	
Name: Stored Process Canceled	Priority: II - Medium
Resource: Object Spawner - ptnode20 SASApp - Stored Process Server	Alert Date: 03/25/2013 03:47 AM
Description: Stored process has been canceled at the user's request	Alert Status: Not Fixed

Condition Set
If Condition: Event/Log Level(ERR) and matching substring "Stored process canceled at user's request" Actual Value: mayhem /home/opt/SAS/Config/Lev1/SASApp/StoredProcessServer/Logs/SASApp_STPServer_mayhem.log: Stored process canceled at user's request. Enable Action(s): Each time conditions are met.

Control Type: none

Notification Actions
Notify Roles: (none)
Notify Users: (none)

Fix

Resolution for Fix:

Click the "Fixed" button to mark alert condition as fixed

[<< Resource Alert List](#)

The **Definition** tab in the Alert Center contains a table listing all of the defined alerts. Clicking on an alert takes you to the definition page for the alert, where you can view more detailed information or edit the alert.

Event Center

The Event Center page provides a deployment-wide view of all events that have been logged for resources. Alerts are automatically logged as events. You can configure SAS Environment Manager to also log events for log messages, resource configuration changes, and resource metric triggers.

To access the Event Center, select **Analyze ► Event Center**.

SAS® Environment Manager

Recent Alerts: 02/21/16 - Stored Process Cancelled
02/21/16 - Access Denied

Welcome, HQ 288.0M 100%

Dashboard Resources Analyze Administration Manage

Event Center

Filter

Minimum Status

Any

Type

All

Time Range

Last 4 hours

In Groups

Unselect All

File Mounts
Key Web Applications
RPC Socket Response
SAS Spawnd Servers

Events

Date	Status	Resource	Subject	Detail
3/4/15 2:09 PM	Error	SASMeta - Metadata Server	mayhem.homeopt\SAS\Config\Lev1\SASMeta MetadataServer Log\SASMeta_MetadataServer_mayhem.log	The SAS Metadata Supervisor failed to initialize
3/4/15 2:09 PM	Alert	SASMeta - Metadata Server	Supervisor Failure	mayhem.homeopt\SAS\Config\Lev1\SASMeta MetadataServer Log\SASMeta_MetadataServer_mayhem.log The SAS Metadata Supervisor failed to initialize
3/4/15 2:07 PM	Error	SASMeta - Metadata Server	mayhem.homeopt\SAS\Config\Lev1\SASMeta MetadataServer Log\SASMeta_MetadataServer_mayhem.log	The SAS Metadata Supervisor failed to initialize
3/4/15 2:07 PM	Alert	SASMeta - Metadata Server	Supervisor Failure	mayhem.homeopt\SAS\Config\Lev1\SASMeta_MetadataServer Log\SASMeta_MetadataServer_mayhem.log The SAS Metadata Supervisor failed to initialize
3/4/15 2:03 PM	Alert	Object Spawner - gphode19 SASApp - Stored Process Server	Stored Process Cancelled	mayhem.homeopt\SAS\Config\Lev1\SASApp\StoredProcessServer Log\SASApp_STPServer_mayhem.log Stored process cancelled at user's request.
3/4/15 2:03 PM	Error	Object Spawner - gphode19 SASApp - Stored Process Server	mayhem.homeopt\SAS\Config\Lev1\SASApp StoredProcessServer Log\SASApp_STPServer_mayhem.log	Stored process cancelled at user's request.
3/4/15 2:03 PM	Error	Object Spawner - gphode19 SASApp - Stored Process Server	mayhem.homeopt\SAS\Config\Lev1\SASApp StoredProcessServer Log\SASApp_STPServer_mayhem.log	Access is denied. File: mayhem0_secrets.txt
3/4/15 2:03 PM	Alert	Object Spawner - gphode19 SASApp - Stored Process Server	Access Denied	mayhem.homeopt\SAS\Config\Lev1\SASApp\StoredProcessServer Log\SASApp_STPServer_mayhem.log Access is denied. File: mayhem0_secrets.txt

Previous Page 1 Next

Operations Center

The Operations Center lists resources that are down or have active alerts. You can use filters to find resources and problem types of interest. This concise view displays the current number of unavailable resources and active alerts, and a one line problem summary for each resource.

To access the Operations Center, select **Analyze ► Operations Center**.

Operations Center

Display Filters

Status Type: All Alerts

Platform Filter:

Group Filter: None

Current Filter Totals

Resources

Down Platforms: N/A

Down Resources: N/A

Alerts

Low

Medium

High

Total

Unfixed Alerts: 4 9 0 13

Alerts in Escalation: 0 0 0 0

Table Controls

Items per page: 50

Refresh interval: 1 minute

Updated at 11:06:41, population took 151 ms

Resource Details for All Hosts

Platform	Resource	Alert Name	Priority	Status Type	Last Escalation	Last Check	Duration	State	Status Information
atnode21plex1.sas.com	atnode21plex1.sas.com	ICP Attempt Fails	1	Alert		5/28/14 11:05 AM	11:01:41		21 occurrences. If Top Attempt Fails per Minute > 20.0% of Baseline (actual value = 0.2), Current value = 0.0.
atnode21plex1.sas.com	SAS Meta - Metadata Server	Metadata Time in Calls per Minute	1	Alert		5/28/14 11:05 AM	156:31.41		23 occurrences. Last event: sas - Carilog1416ASMetaMetadataServer_AggsASAMeta_MetadataServer_2014-05-20_11:05:00_12944 log: New client connection (186606) received from server port 8061 for user sasadm@plex1.sas.com. Per address and port is 186606 from 10.10.10.10 for APPRIAMS-Login Manager 9.4 Time in Calls per Minute > 300.0% of Baseline (actual value = 13.226), Current value = 6.2126.
atnode21plex1.sas.com	Postgres SQL	pg: Memory Size changed	1	Alert		5/28/14 11:00 AM	191:08.41		2 occurrences. If Memory Size > 90.0% of Baseline (actual value = 3.9 GB), Current value = 31.9 GB.
atnode21plex1.sas.com	Obsest - Metadata Server - Obsest - SASApp - Pooled Workspace Server	Pooled Workspace Server ERROR message in log	1	Alert		5/18/14 2:24 PM	307:42:32		23 occurrences. Last event: sas - _Aem1ASAppPooledWorkspaceServer_AggsASApp_PooledWorkspaceServer_2014-05-15_11:05:00_5381 log: ERROR: Errors printed on page 2. If EventLog Lvl=ERROR and matching substring "ERROR" Log entry - _Aem1ASAppPooledWorkspaceServer_AggsASApp_PooledWorkspaceServer_2014-05-15_11:05:00_5381 log: ERROR: Errors printed on page 2.
atnode21plex1.sas.com	S&B	HQ Time Agent - Spends Estimating Metrics	1	Alert		5/28/14 11:05 AM	454:26.41		145 occurrences. If Task Time Spent Fetching Metrics per Minute > 1x (actual value = 36.0s), Current value = 607.91s.
atnode21plex1.sas.com	Obsest - SASApp - Obsest - SASApp - Object Scanner - Major Object(s) Faults	Object Scanner Major Object(s) Faults	1	Alert		5/28/14 11:05 AM	455:01.41		1 occurrence. Last event: sas: bobSASCarilog141KObjScanner_AggsObjScanner_2014-05-15_11:05:00_5383 log: The server is not running (unexpectedly stopped this mode). If Process Major Faults per Minute > 10.0% of Baseline (actual value = 0.2), Current value = 0.0.
atnode21plex1.sas.com	atnode21plex1.sas.com - HQ Agent S&B	HQ Agent Memory	1	Alert		5/28/14 11:05 AM	644:11.41		1 occurrence. If JVM Free Memory > 14.3 MB (actual value = 13.4 MB), Current value = 56.1 MB.
atnode21plex1.sas.com	atnode21plex1.sas.com	ICP Attempt Fails	1	Alert		5/28/14 11:05 AM	10:31:41		155 occurrences. If Top Attempt Fails per Minute > 20.0% of Baseline (actual value = 0.2), Current value = 0.0.

Environment Snapshot

Environment Snapshot contains a comprehensive listing of the system information in the SAS Environment Manager database. Although Environment Snapshot was originally designed to provide SAS Technical Support with a method for quickly diagnosing system issues, it also 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 is useful when working with SAS Technical Support, because it provides an easy way to communicate the status and configuration of your system.

To access the Environment Snapshot, select **Analyze ► Environment Snapshot**.

Environment Snapshot

Summary Table

Hardware Summary

Property	Value
CPU Speed	24 @ 2200 MHz (2x12)
Free Memory	76.3 GB
Load Average 5 Minutes	0.08
RAM	96744 MB
Swap Used	0.0 B

CPU Summary

Processor	CPU Usage
Linux CPU 1 (2200MHz AMD Opteron)	0.0%
Linux CPU 2 (2200MHz AMD Opteron)	0.04%
Linux CPU 3 (2200MHz AMD Opteron)	1.21%
Linux CPU 4 (2200MHz AMD Opteron)	0.02%
Linux CPU 5 (2200MHz AMD Opteron)	0.59%
Linux CPU 6 (2200MHz AMD Opteron)	0.53%
Linux CPU 7 (2200MHz AMD Opteron)	0.3%
Linux CPU 8 (2200MHz AMD Opteron)	0.17%
Linux CPU 9 (2200MHz AMD Opteron)	0.12%
Linux CPU 10 (2200MHz AMD Opteron)	0.11%
Linux CPU 11 (2200MHz AMD Opteron)	0.09%
Linux CPU 12 (2200MHz AMD Opteron)	0.10%
Linux CPU 13 (2200MHz AMD Opteron)	1.12%
Linux CPU 14 (2200MHz AMD Opteron)	0.05%
Linux CPU 15 (2200MHz AMD Opteron)	1.0%
Linux CPU 16 (2200MHz AMD Opteron)	0.09%
Linux CPU 17 (2200MHz AMD Opteron)	0.42%

Report Center

The Report Center is collection of SAS Stored Process reports that are produced from data in the SAS Environment Manager Data Mart. These reports are created to 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 SAS Stored Process reports operate only on data stored in the SAS Environment Manager Data Mart by APM or ACM ETL processes. Unless you initialize and enable one of those packages, no reports will be produced. Solution kits, which provide monitoring and reporting for specific applications or SAS solutions, can also add solution-specific reports to the Report Center.

Stored Processes

Products

SAS Environment Manager

Custom

Dynamic Reports

Datamart

ACM Data Mart Platform Resource

ACM Data Mart Platform Types and Resources

ACM Data Mart Server Resources

ACM Data Mart Services Resources

Alerts Enabled By Resource

Alerts Enabled Listing Rpt

All Alert Definitions

Data Mart ACM Listing

Data Mart Artifact Listing

Data Mart Proc Contents Full Listing

Plugin To Discovered Resource Manager

Metadata Inventory

Nightly Reports

System

User Folders

The DATASETS Procedure

Directory	
Libref	ACM
Engine	BASE
Access	READONLY
Physical Name	/opt/SAS/Config/Lev1/Web/SASEnvironmentManager/emi-framework/Datamart/acm
Filename	/opt/SAS/Config/Lev1/Web/SASEnvironmentManager/emi-framework/Datamart/acm
Inode Number	1322309
Access Permission	MODE=0440
Owner Name	sas
File Size (bytes)	4096

#	Name	Member Type	File Size	Last Modified
1	AVAILABILITY	DATA	458752	07/22/2014 01:00:38
2	EVENTS	DATA	393216	07/22/2014 12:09:50
3	FILEMOUNTS	DATA	7340032	07/22/2014 01:00:54
4	GROUPINVENTORY	DATA	262144	07/22/2014 01:00:32
5	HOSTPLATFORMS	DATA	2883584	07/22/2014 01:00:53
6	HTTPCHECKS	DATA	1179648	07/22/2014 01:00:55
7	IDMSERVERS	DATA	3407872	07/22/2014 01:00:54
8	MEASUREINVENTORY	DATA	2088960	07/22/2014 01:00:33
	MEASUREINVENTORY	INDEX	163840	07/22/2014 01:00:33
9	METADATASVRS	DATA	1572864	07/22/2014 01:00:54
10	NETWORKINTERFACE	DATA	5998240	07/22/2014 01:00:54
11	RESOURCEINVENTORY	DATA	524288	07/22/2014 01:00:32
12	TCSERVERMGERS	DATA	23592960	07/22/2014 01:00:56
13	WEBAPP SERVER	DATA	1310720	07/22/2014 01:00:54
14	WIPDATADB	DATA	3932160	07/22/2014 01:00:55

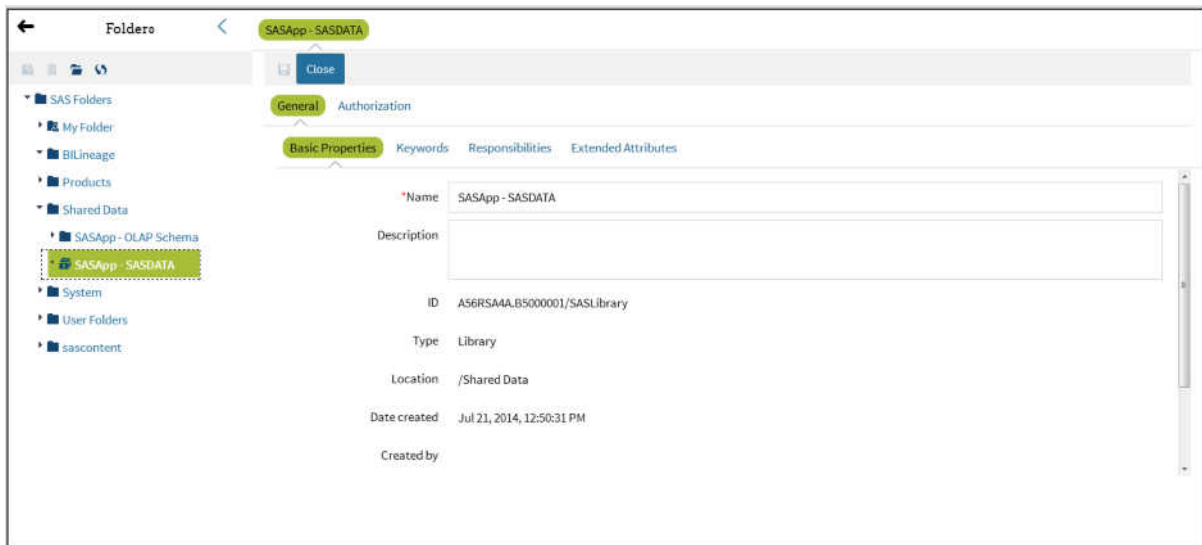
The DATASETS Procedure			
Data Set Name	ACM.AVAILABILITY	Observations	1530
Member Type	DATA	Variables	9
Engine	BASE	Indexes	0
Created	07/22/2014 01:00:39	Observation Length	284
Last Modified	07/22/2014 01:00:39	Deleted Observations	0
Protection		Compressed	CHAR

Performing SAS Tasks: the Administration Page

The Administration page enables you to access and manage SAS metadata folders and folder contents in the SAS Metadata server and to manage SAS metadata user definitions.

After you select a folder or an object contained in a folder, you can perform these tasks:

- view details about the folder or object's metadata
- modify the name, description, keywords, responsible parties, and extended attributes for folders and objects
- manage metadata access (such as access control templates and permissions)
- create, update, and delete folders



The **Users** module enables you to perform the following tasks:

- create, update, and delete users, groups, and roles
- manage account passwords

- administer logins and internal accounts

Configuring SAS Environment Manager: the Manage Page

Overview

Use the pages under Manage to control how the SAS Environment Manager application operates.

Authentication/Authorization

The **Authentication/Authorization** area enables you to manage SAS Environment Manager users and user roles. These users and roles are not the same as the users and roles in SAS metadata that control access to SAS metadata objects, although SAS Environment Manager users are synchronized with users that are defined in metadata and added to specific groups.

In order to distinguish between the SAS Environment Manager access features and those in SAS metadata, this document and the SAS Environment Manager online Help refers to features internal to SAS Environment Manager as native features (such as native users or native roles). However, the SAS Environment Manager interface does not use the native terminology.

Server Settings

The **Server Settings** area enable you to change the settings for the SAS Environment Manager server, the defaults for monitoring, the configuration of escalation schemes, and the SAS Environment Manager plugins.

Server Settings

contains settings for the SAS Environment Manager server, including global alert properties, e-mail configuration, and notification properties

Monitoring Defaults

contains default monitoring and alerting definitions for all types of platforms, platform services, and servers supported by SAS Environment Manager.

Escalation Schemes Configuration

enables you to define notification or logging actions that are taken for alerts.

Plugin Manager

lists all currently loaded plugins and enables you to delete and update existing plugins, and load new ones. Deleting or updating a plugin cannot be reversed. Always save a copy before deleting or updating a plugin. You can find additional plugins for SAS Environment Manager at the Enterprise Management Integration area of SAS Customer Support on the web (support.sas.com/rnd/emi).

Plugins

The **Plugins** area contains functions that are added to the functionality of SAS Environment Manager to perform a specific action. Plugins include the following:

- Network and Host Dependency Manager
- Groovy Console
- HQ Health
- HQ Web Services API
- tc Server Command-line Interface

License Usage Status

The **Licenses Usage Status** area displays the number of licenses in use on the platform as well as the total number of licenses allowed.

Viewing Information at a Glance: Using the Dashboard

<i>Using the Dashboard</i>	28
<i>Customizing Your Dashboard</i>	31
<i>Summary Portlet Examples</i>	32
Adding Summary Portlets	32
Example: Adding a Summary Portlet for SAS	
Servers That Can Be Spawned	33
Example: Adding a Platform Availability Summary Portlet	35
<i>Metric Viewer Portlet Examples</i>	36
Adding Metric Viewer Portlets	36
Example: Adding a SASWork Disk Space Metric Viewer	38
Example: Adding a WebApp Login Response	
Time Metric Viewer	39
Example: Adding a PostgreSQL Data Volume Metric Viewer	40
Example: Adding a tc Runtime Manager Active	
Sessions Metric Viewer	41
<i>Metric Chart Examples</i>	43
Adding a Saved Chart Portlet	43
Creating a Free Memory Chart	44
Creating a Number of Spawned Servers Chart	47
Creating a Metadata Users Chart	48
Adding a Saved Charts Portlet	49

Using the Dashboard

The Dashboard is your first view when you start SAS Environment Manager. It is an at-a-glance view of the things that are most important to you when administering your environment, such as favorite resources, recent alerts, and resources that are currently experiencing problems.

The page contains a collection of portlets that provide information at a glance about the SAS environment. You can select which portlets appear on the Dashboard, so the Dashboard shows you the information that you want to see. Selecting an entry in a portlet takes you to more detailed information about the entry. For example, selecting an entry in the **Recent Alerts** portlet takes you to the Alert Detail page for that alert. The following figure illustrates a sample Dashboard portlet.

Figure 3.1 Sample Portlet



Availability Summary Physical (OS) Components	
Resource Type	Availability
FileServer Mount	✔ 6
Linux	✔ 2
Updated: 2:21 PM	

The Dashboard is divided into two columns, and the portlets that can appear differ between the left and the right column. Some portlets can appear only once on a Dashboard, whereas other portlets can appear more than once. The portlets that can appear more than once are ones that display information about a selected group of resources. Each instance of the portlet displays information about different resources. The portlets that can appear only once display information for the entire environment.

This table lists the portlets that you can choose to appear on a Dashboard, as well as where they can appear and how many instances are allowed.

Table 3.1 Portlets

Name	Description	Location	Instances
Auto-Discovery	Lists new and changed resources and enables you to add them to the inventory. Check this portlet after you install a plugin to accept the newly discovered resources into the inventory.	Right	One
Availability Summary	Indicates the availability of selected resources, grouped by resource type. This portlet refreshes every minute.	Left	Multiple
Control Actions	Lists recently performed actions on managed resources and upcoming scheduled actions. Also indicates which quick control actions are most frequently performed.	Right	One
Favorite Resources	Lists selected resources.	Right	One
Saved Charts	Displays selected charts as a slide show.	Left	One
Recent Alerts	Lists the most recently triggered alerts for selected resources. This portlet refreshes every minute.	Right	Multiple
Recently Added	Lists platforms that have been recently added to inventory.	Left	One
Search Resources	Enables you to search for resources. The search supports case-insensitive, partial-term queries for a specified inventory type.	Left	One


Name	Description	Location	Instances
Summary Counts	Displays a count of managed resources by inventory type. Only those resources that you are allowed to access are displayed.	Left	One
Group Alerts Summary	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.	Right	One
Metric Viewer	Displays selected metrics for selected resources. This portlet refreshes every minute.	Right	Multiple
Problem Resources	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.	Right	One

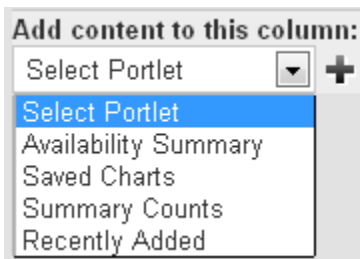
Because the Dashboard page can be customized, each user has access to multiple Dashboards, with each one modified according to different needs. Each user has access to a personal Dashboard, which contains portlets selected by the user. In addition, each user can also access a Dashboard for each of the native roles of which the user is a member. Each of those Dashboards is customized with the portlets that are most useful for that role. To choose a different Dashboard, select the one that you want to use from the **Select a Dashboard** field.

A new Dashboard type is automatically created whenever you create a new native role. For more information about roles, see [“About Native Roles and Users” on page 83](#).


Customizing Your Dashboard

You can customize any Dashboard to which you have access by selecting portlets to appear on your Dashboard and by selecting the information that is displayed in each portlet.

To add a portlet to your Dashboard, use the **Add content to this column** menu to select from the available portlets and then click the Add icon , which is beside the field. The portlets displayed in the list depend on whether you are adding a portlet to the right or left column and which portlets have already been added to the Dashboard.




After the portlet is placed on your Dashboard, you can click and drag the portlet header to move it to a different location. However, you cannot move a portlet from one column to another.

To change the information that a portlet displays, click on the configuration icon  in the portlet's header. Use the Portlet Configuration page to select options that narrow the focus of the information displayed in the portlet. The options available are unique to each portlet. Examples include the following:

- how many of the most recent control actions are displayed (**Control Actions** portlet)
- the number and type of alerts issued for selected resources (**Alerts** portlet)
- specified resources (**Availability Summary** portlet)

You can use groups (compatible groups, mixed groups, and application groups) to make your Dashboard portlets more useful. Groups enable you to organize resources by type or function within your organization. You can then configure portlets to display


information about resources in particular groups, so your Dashboard contains information about the resources that are most vital to you.

To remove a portlet from the Dashboard, click on the delete icon  for the portlet.

Summary Portlet Examples


Adding Summary Portlets

Here are the basic steps for adding a summary portlet to your Dashboard page.

- 1 On the left side of the Dashboard page, select **Availability Summary** in the **Add Content to this column** field and click the Add icon . A blank **Availability Summary** portlet is added to your Dashboard.



The screenshot shows the 'Availability Summary' portlet header with a configuration icon and a close icon. Below the header is a table with two columns: 'Resource Type' and 'Availability'. The table body contains a message: 'No resources to display, please click the  icon above to add resources to portlet.'

- 2 Click the Configuration icon  to display the Dashboard Settings page for the portlet.



The screenshot shows the 'Dashboard Settings: Availability Summary' configuration page. It has a 'Display Settings' section with a 'Description' text field and a 'Display Range' dropdown set to '10' with the text 'Display top 10 resource types.' Below this is a 'Selected Resources' section with a table header 'Resource' and 'Description'. There are 'Add to List' and 'Remove from List' buttons. At the bottom right, it shows 'Total: 0' and 'Items Per Page: 15' with a dropdown. At the very bottom are 'OK', 'Reset', and 'Cancel' buttons.

- 3 Specify a name for the portlet in the **Description** field. This name will appear in the header for the portlet, after the portlet type.

- 4 In the **Selected Resources** area, click **Add to List** to display the Add/Remove Resources page.

Dashboard Settings: Availability Summary Add Remove Resources

Resources

View: Platforms All Types



Filter By Name:

<input type="checkbox"/> Name	Description
<input type="checkbox"/> postslave	Red Hat Enterprise Linux 6
<input type="checkbox"/> Microsoft Windows 2008	Microsoft Windows 2008
<input type="checkbox"/> Red Hat Enterprise Linux 6	Red Hat Enterprise Linux 6
<input type="checkbox"/> Red Hat Enterprise Linux 6	Red Hat Enterprise Linux 6
<input type="checkbox"/> SAS 9.4 Application Server Tier	
<input type="checkbox"/> Red Hat Enterprise Linux 6	Red Hat Enterprise Linux 6

Add Resources


<input type="checkbox"/> Name	Description

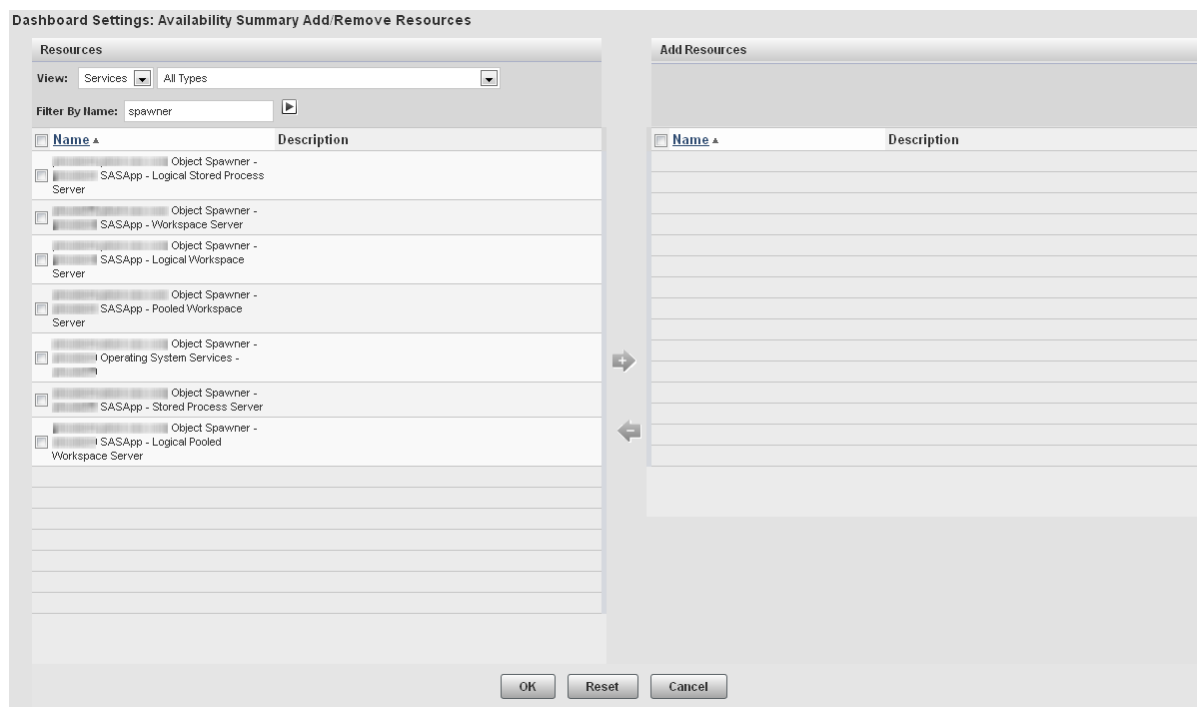
OK Reset Cancel

- 5 To display the resources that you want to use for the summary, specify values in the **View** and **Filter By Name** fields. If you specify a value in the **Filter By Name** field, click  to filter the table contents.
- 6 In the Resources table, select the check boxes for the resources that you want to use in the summary. Click  to move the resources to the **Add Resources** list.
- 7 After you select the resources that you want to use in the Add/Remove Resources window, click **OK** to return to the Availability Summary window. Click **OK** to create the portlet and add it to your Dashboard page.

Example: Adding a Summary Portlet for SAS Servers That Can Be Spawnd

This example explains how to add a portlet to your Dashboard page that monitors the availability of SAS Workspace Servers that are running under a SAS Object Spawner.

- 1 Follow the basic procedure for creating an availability summary portlet in “[Adding Summary Portlets](#)” on page 32. Follow the basic procedure for creating an availability
- 2 On the Add/Remove Resources window, in the **View** field, select **Services**. Logical SAS servers are listed as services in SAS Environment Manager.
- 3 In the **Filter By Name** field, enter **spawner** and click . The **Resources** list displays the services running under the SAS Object Spawner.



- 4 Select the resources **Workspace Server** and **Pooled Workspace Server** and move them to the Add Resources table.

Dashboard Settings: Availability Summary Add/Remove Resources

Resources

View: Services All Types

Filter By Name: spawner

Name	Description
Object Spawner - SASApp - Logical Stored Process Server	
Object Spawner - Operating System Services -	
Object Spawner - SASApp - Stored Process Server	

Add Resources

Name	Description
Object Spawner - SASApp - Workspace Server	
Object Spawner - SASApp - Pooled Workspace Server	
Object Spawner - SASApp - Logical Workspace Server	
Object Spawner - SASApp - Logical Pooled Workspace Server	

OK Reset Cancel

- 5 Finish the procedure for creating the portlet. The portlet displays the availability information for the servers that can be spawned.

Availability Summary	
Resource Type	Availability
SAS Object Spawner 9.4 SAS Logical Pooled Workspace Server	✓ 1
SAS Object Spawner 9.4 SAS Logical Workspace Server	✓ 1
SAS Object Spawner 9.4 SAS Pooled Workspace Server	✓ 1
Updated: 2:24 PM	

Example: Adding a Platform Availability Summary Portlet

To add a portlet to monitor the availability of all of the platforms in the environment, follow these steps:

- 1 Follow the basic procedure for creating an availability summary portlet in [“Adding Summary Portlets”](#) on page 32.

- 2 In the Add/Remove Resources page, select **Platforms** in the **View** field and select the check box beside the **Name** column in the **Resources** table. This selects all of the listed platforms.

Dashboard Settings: Availability Summary Add/Remove Resources

Resources

View: Platforms  All Types 

Filter By Name: 


<input checked="" type="checkbox"/> Name ▲	Description
<input checked="" type="checkbox"/> SAS 9.4 Application Server Tier	
<input checked="" type="checkbox"/> ptnode23.ptest.sas.com	HTTP SAS BI Dashboard
<input checked="" type="checkbox"/> ptnode22.ptest.sas.com	[Auto-Generated] Linux Platform rnb
<input checked="" type="checkbox"/> TrapProxyRNB	

- 3 Complete portlet creation process to add the portlet to your dashboard.

Metric Viewer Portlet Examples


Adding Metric Viewer Portlets

Here are the basic steps for adding a metric viewer portlet to your Dashboard page.

- 1 On the right side of the Dashboard page, select **Metric Viewer** in the **Add Content to this column** field and click the Add icon . A blank **Metric Viewer** portlet is added to your Dashboard.

Metric Viewer  

No resources to display, please click the  icon above to add resources to portlet.

- 2 Click the Configuration icon  to display the Dashboard Settings page for the portlet.

Dashboard Settings: Metric Viewer

Display Settings

Description:

Display Range: Display top resources.

Resource Type:

Metric:

Sort Order:

Selected Resources

<input type="checkbox"/> Resource	Description
<input type="button" value="Add to List"/> <input type="button" value="Remove from List"/>	

Total: 0 Items Per Page:

- 3 On the Dashboard Settings page, specify a name for the portlet in the **Description** field. Select the type of resource that you want to monitor in the **Resource Type** field and the information that you want to display in the **Metric** field. The values available in the **Metric** field change depending on what you select in the **Resource Type** field.
- 4 In the **Selected Resources** area, click **Add to List** to display the Add/Remove Resources page.

Dashboard Settings: Availability Summary Add Remove Resources

Resources

View:

Filter By Name:



<input type="checkbox"/> Name	Description
<input type="checkbox"/> postslave	Red Hat Enterprise Linux 6
<input type="checkbox"/> Microsoft Windows 2008	Microsoft Windows 2008
<input type="checkbox"/> Red Hat Enterprise Linux 6	Red Hat Enterprise Linux 6
<input type="checkbox"/> Red Hat Enterprise Linux 6	Red Hat Enterprise Linux 6
<input type="checkbox"/> SAS 9.4 Application Server Tier	SAS 9.4 Application Server Tier
<input type="checkbox"/> Red Hat Enterprise Linux 6	Red Hat Enterprise Linux 6

➡

←

Add Resources

<input type="checkbox"/> Name	Description

- 5 To display the resources that you want to use for the metric, specify values in the **View** and **Filter By Name** fields. If you specify a value in the **Filter By Name** field, click  to filter the table contents.
- 6 In the **Resources** table, select the check boxes for the resources that you want to use in the metric. Click  to move the resources to the **Add Resources** list.
- 7 After you select the resources that you want to use in the Add/Remove Resources window, click **OK** to return to the Dashboard Settings page. Click **OK** to create the portlet and add it to your Dashboard page.

Example: Adding a SASWork Disk Space Metric Viewer

To add a portlet for viewing the usage of the SASWork directory, follow these steps.

- 1 Follow the basic procedure for creating a metric viewer portlet at [“Adding Metric Viewer Portlets” on page 36](#).
- 2 On the Dashboard Settings page, specify the following information:

Description

specify a name for the portlet

Resource Type

select **SAS Home Directory 9.4 SAS Directory**

Metric

select **Use Percent**

Dashboard Settings: Metric Viewer

Display Settings

Description: SASWork Disk Space

Display Range: Display top 10 resources.

Resource Type: - SAS Home Directory 9.4 SAS Directory

Metric: - Use Percent

Sort Order: Highest Values First

- 3 In the Add Resources window, select all resources in the **Resources** table, click the **Add** icon to move them to the **Add Resources** table, and click **OK**.
- 4 Complete the procedure to add the portlet to your **Dashboard** page.

Example: Adding a WebApp Login Response Time Metric Viewer

To add a portlet for viewing the response time for all web applications, follow these steps.

- 1 Follow the basic procedure for creating a metric viewer portlet at [“Adding Metric Viewer Portlets” on page 36](#).
- 2 On the Dashboard Settings page, specify the following information:

Description

specify a name for the portlet

Resource Type

select **HTTP**

Metric

select **Response Time**

Dashboard Settings: Metric Viewer

Display Settings

Description: WebApp Login Respons

Display Range: Display top 10 resources.

Resource Type: - HTTP

Metric: - Response Time

Sort Order: Highest Values First

- 3 In the Add Resources window, select all resources in the **Resources** table, click the **Add** icon to move them to the **Add Resources** table, and click **OK**.
- 4 Complete the procedure to add the portlet to your **Dashboard** page.

Example: Adding a PostgreSQL Data Volume Metric Viewer

To add a portlet for viewing the volume of data in all PostgreSQL databases, follow these steps.

- 1 Follow the basic procedure for creating a metric viewer portlet at [“Adding Metric Viewer Portlets” on page 36](#).
- 2 On the Dashboard Settings page, specify the following information:

Description

specify a name for the portlet

Resource Type

select **PostgreSQL 9.x DataBase**

Metric

select **Data Space Used**

Dashboard Settings: Metric Viewer

Display Settings

Description: PostgreSQL

Display Range: Display top 10 resources.

Resource Type: - PostgreSQL 9.x DataBase

Metric: - Data Space Used

Sort Order: Highest Values First

- 3 In the Add Resources window, select all resources in the **Resources** table, click the **Add** icon to move them to the **Add Resources** table, and click **OK**.
- 4 Complete the procedure to add the portlet to your **Dashboard** page.

Example: Adding a tc Runtime Manager Active Sessions Metric Viewer

To add a portlet for viewing the number of active sessions for all web applications, follow these steps.

- 1 Follow the basic procedure for creating a metric viewer portlet at [“Adding Metric Viewer Portlets” on page 36](#).
- 2 On the Dashboard Settings page, specify the following information:

Description

specify a name for the portlet

Resource Type

select **SpringSource tc Runtime 7.0 Manager**

Metric

select **Active Sessions**

Dashboard Settings: Metric Viewer

Display Settings

Description: tc Runtime Manager Act

Display Range: Display top 10 resources.

Resource Type: - SpringSource tc Runtime 7.0 Manager

Metric: - Active Sessions

Sort Order: Highest Values First

3 On the Add/Remove Resources page, in the **View** field, select **Servers**. In the **Resources** table, select these servers:

- <server_name> tc Runtime SASServer1_1/SASWebReportStudio localhost Manager
- <server_name> tc Runtime SASServer1_1/SASAdmin localhost Manager
- <server_name> tc Runtime SASServer1_1/SASContentServer localhost Manager
- <server_name> tc Runtime SASServer1_1/SASBIDashboard localhost Manager
- <server_name> tc Runtime SASServer1_1/SASWebDoc localhost Manager
- <server_name> tc Runtime SASServer1_1/SASPortal localhost Manager
- <server_name> tc Runtime SASServer1_1/SASLogon localhost Manager
- <server_name> tc Runtime SASServer1_1/SASStoredProcess localhost Manager


Some of these servers might be on the second page of the list (click the page number at the bottom of the list to navigate between pages). Click the **Add** icon to move the selected servers on one page before moving to another page.

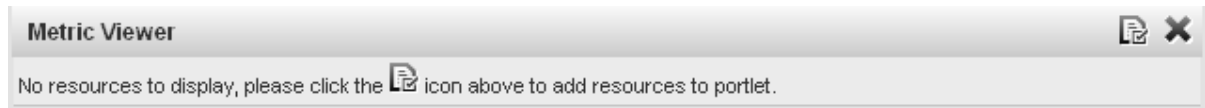
4 Complete the procedure to add the portlet to your **Dashboard** page.


Metric Chart Examples

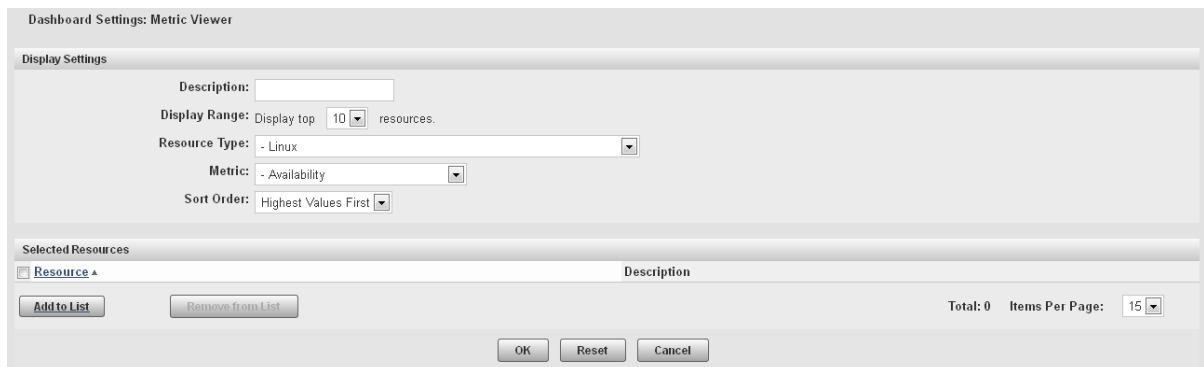
Adding a Saved Chart Portlet

The Saved Chart portlet displays a rotation of all of the resource metric charts that you have saved. The process of creating this type of portlet consists of navigating to the resources that you want to chart, finding the metric charts that you want to display, and saving them to your dashboard. When you create the portlet, all of your saved charts automatically appear. Here are the basic steps for adding a metric viewer portlet to your Dashboard page.

- 1 On the right side of the Dashboard page, select **Metric Viewer** in the **Add Content to this column** field and click the Add icon . A blank **Metric Viewer** portlet is added to your Dashboard.



- 2 Click the Configuration icon  to display the Dashboard Settings page for the portlet.



- 3 On the Dashboard Settings page, specify a name for the portlet in the **Description** field. Select the type of resource that you want to monitor in the **Resource Type** field

and the information that you want to display in the **Metric** field. The values available in the **Metric** field change depending on what you select in the **Resource Type** field.

- 4 In the **Selected Resources** area, click **Add to List** to display the Add/Remove Resources page.

Dashboard Settings: Availability Summary Add/Remove Resources

Resources

View: Platforms All Types



Filter By Name:

<input type="checkbox"/> Name	Description
<input type="checkbox"/> postslave	Red Hat Enterprise Linux 6
<input type="checkbox"/> Microsoft Windows 2008	Microsoft Windows 2008
<input type="checkbox"/> Red Hat Enterprise Linux 6	Red Hat Enterprise Linux 6
<input type="checkbox"/> Red Hat Enterprise Linux 6	Red Hat Enterprise Linux 6
<input type="checkbox"/> SAS 9.4 Application Server Tier	Red Hat Enterprise Linux 6
<input type="checkbox"/> Red Hat Enterprise Linux 6	Red Hat Enterprise Linux 6

Add Resources

<input type="checkbox"/> Name	Description

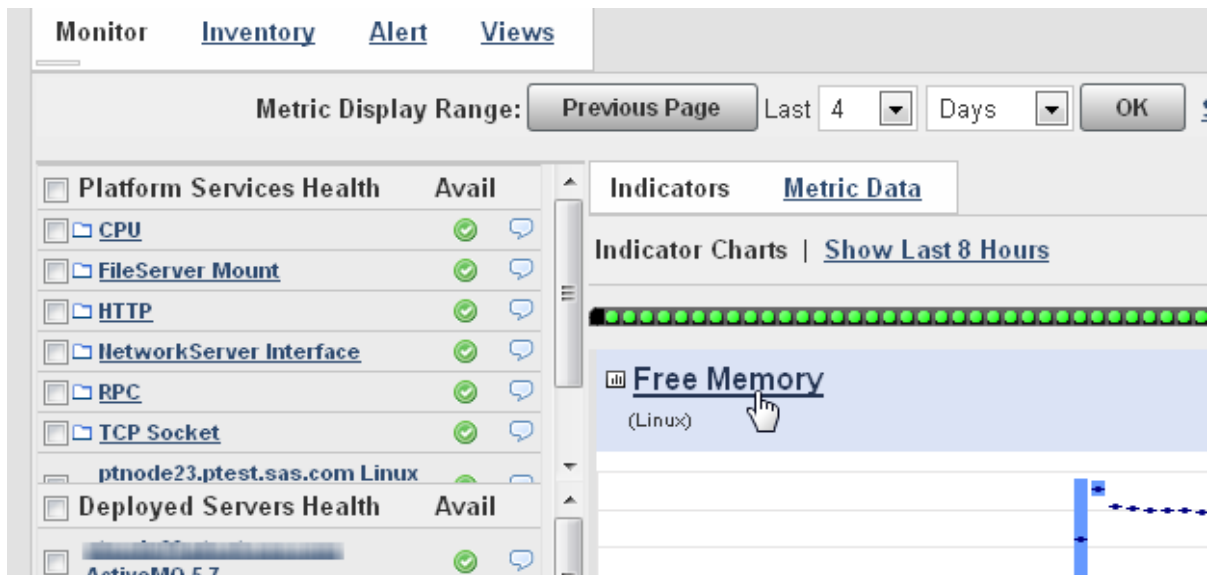
OK Reset Cancel

- 5 To display the resources that you want to use for the metric, specify values in the **View** and **Filter By Name** fields. If you specify a value in the **Filter By Name** field, click  to filter the table contents.
- 6 In the **Resources** table, select the check boxes for the resources that you want to use in the metric. Click  to move the resources to the **Add Resources** list.
- 7 After you select the resources that you want to use in the Add/Remove Resources window, click **OK** to return to the Dashboard Settings page. Click **OK** to create the portlet and add it to your Dashboard page.

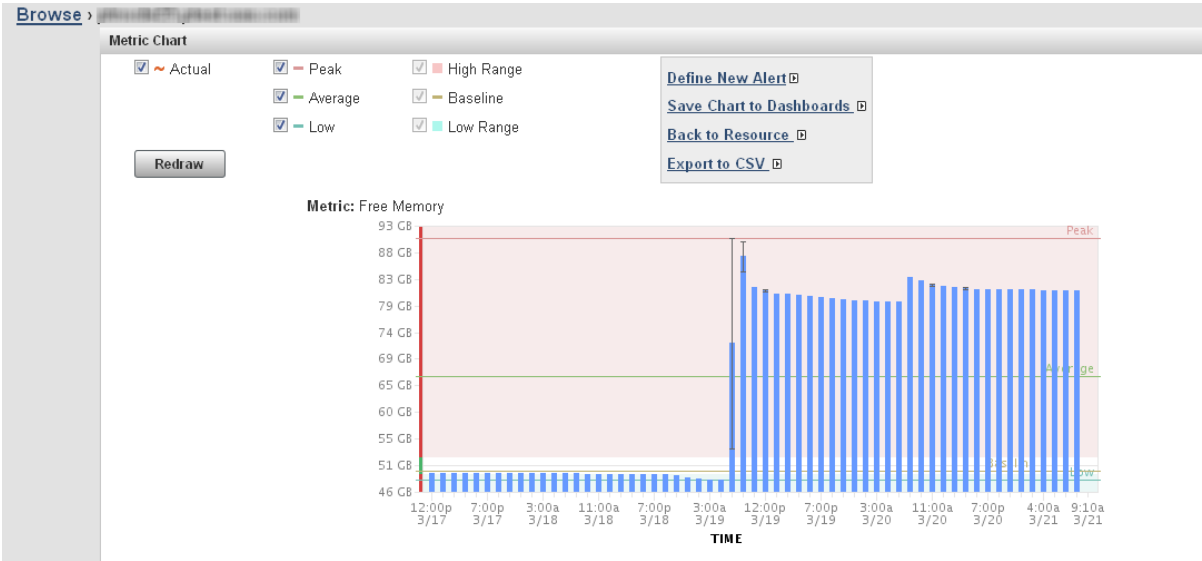
Creating a Free Memory Chart

To create a chart of the free memory on a server and save that chart to your dashboard, follow these steps.

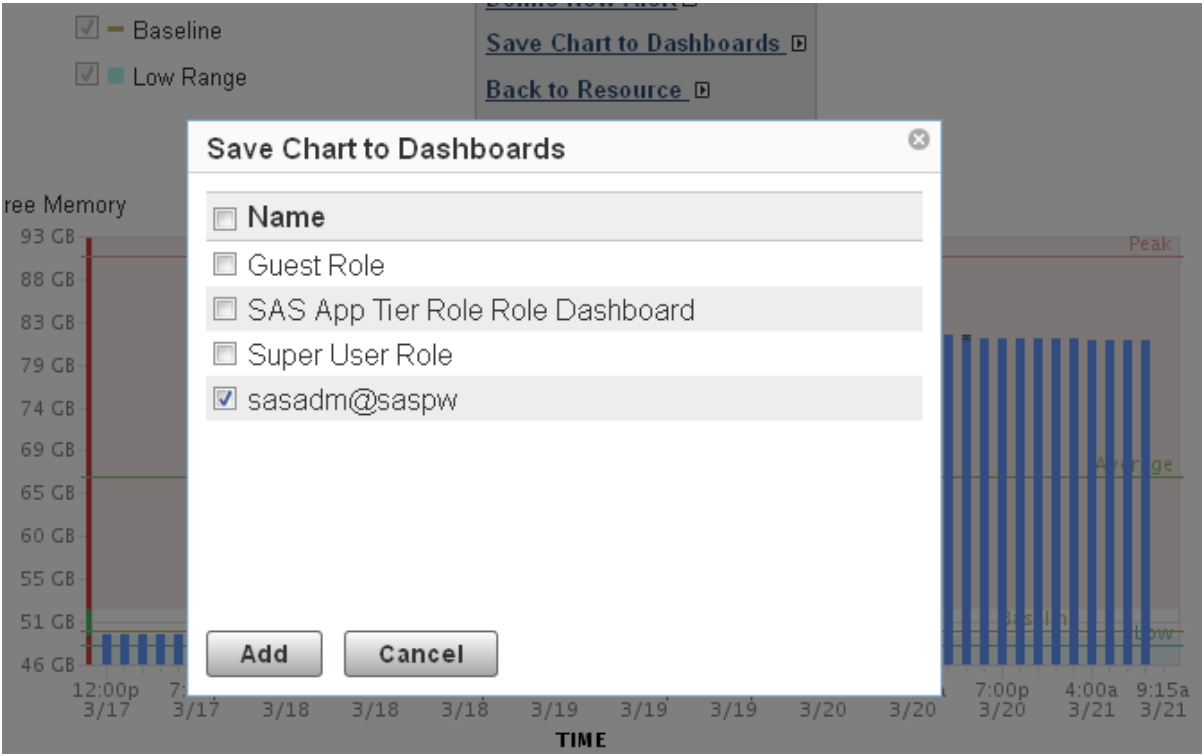
- 1 On the SAS Environment Manager menu bar, select **Resources** ► **Browse**.
- 2 On the Resources page, select **Platforms**.
- 3 In the table of resources, click on the name of your server to display the resource detail page.
- 4 On the resource detail page, one of the displayed metric charts is **Free Memory**. Click on the name of the chart to display the Metric Chart page.



- 5 On the Metric Chart page, select **Save Chart to Dashboards**.




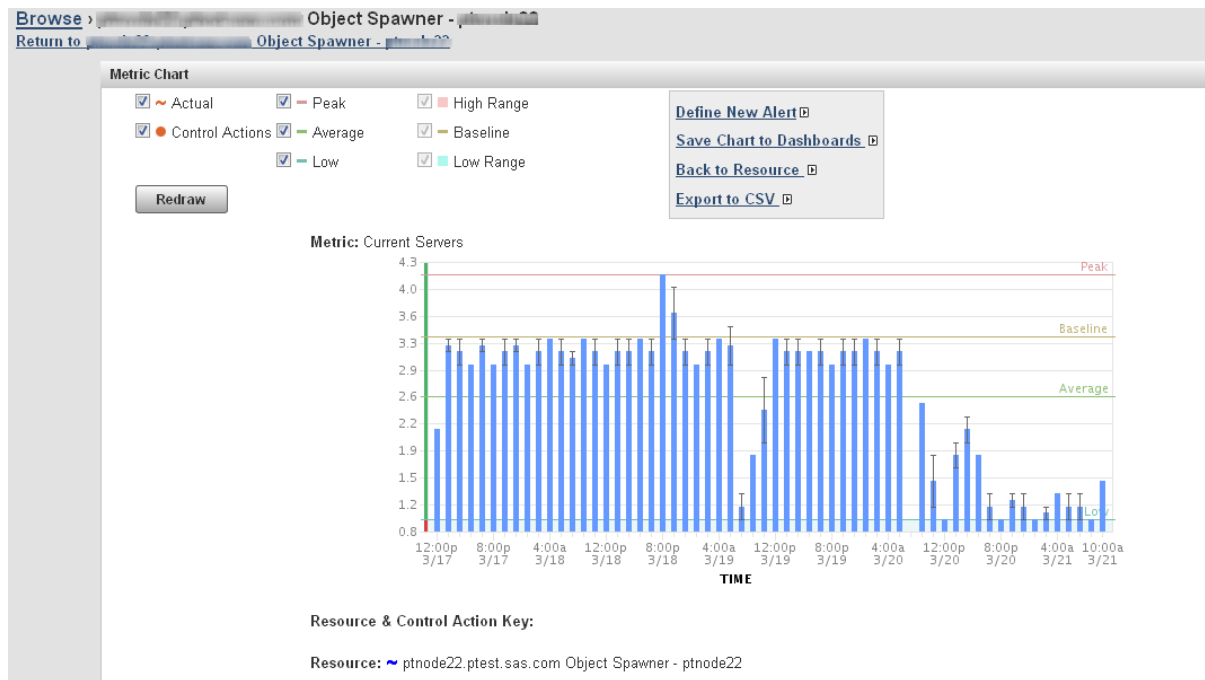
- 6 The Save Chart to Dashboards dialog box appears. Select the dashboards on which the saved chart should appear. Click **Add** to save the chart.



Creating a Number of Spawned Servers Chart

To create a chart of the current number of spawned servers and save that chart to your dashboard, follow these steps.

- 1 On the SAS Environment Manager menu bar, select **Resources** ► **Browse**.
- 2 On the Resources page, in the **All Server Types** field, select **SAS Object Spawner 9.4** and then click on the arrow  at the right of the filter fields.
- 3 In the table of resources, click on the name of the object spawner to display the resource detail page.
- 4 On the resource detail page, one of the displayed metric charts is **Current Servers**. Click on the name of the chart to display the Metric Chart page.




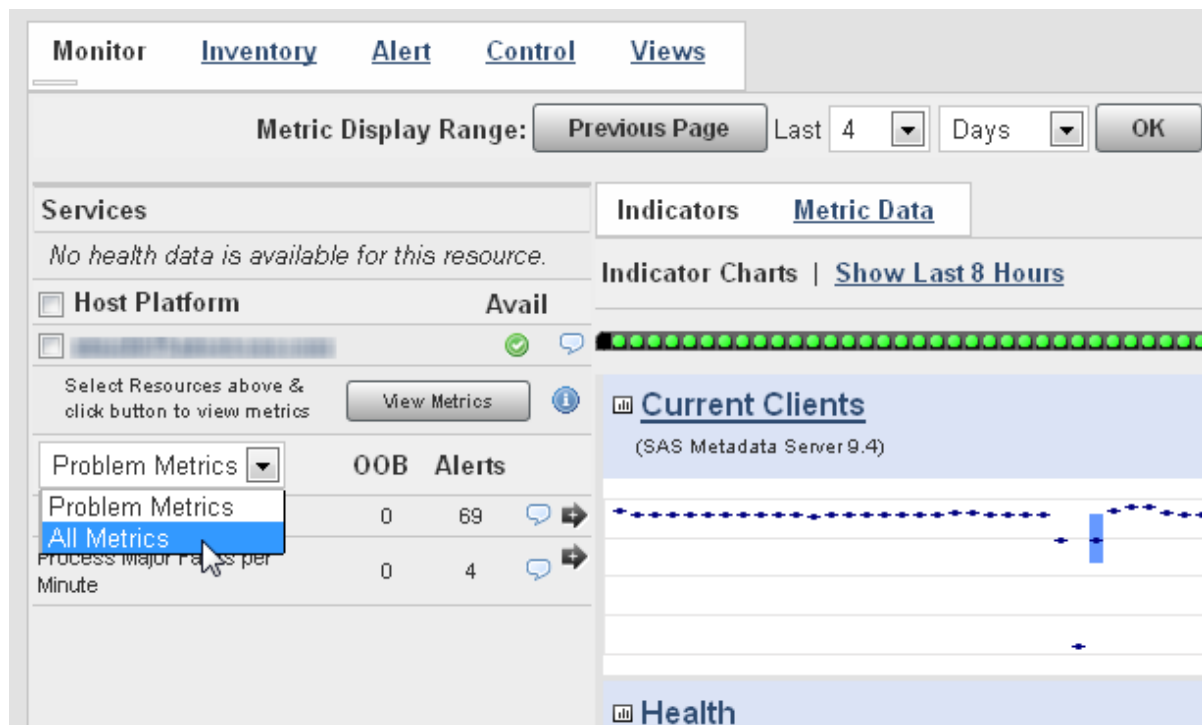
- 5 On the Metric Chart page, select **Save Chart to Dashboards**.

- 6 The Save Chart to Dashboards dialog box appears. Select the dashboards on which the saved chart should appear. Click **Add** to save the chart.

Creating a Metadata Users Chart


To create a chart of the current number of users per minute of the SAS Metadata Server and save that chart to your dashboard, follow these steps.

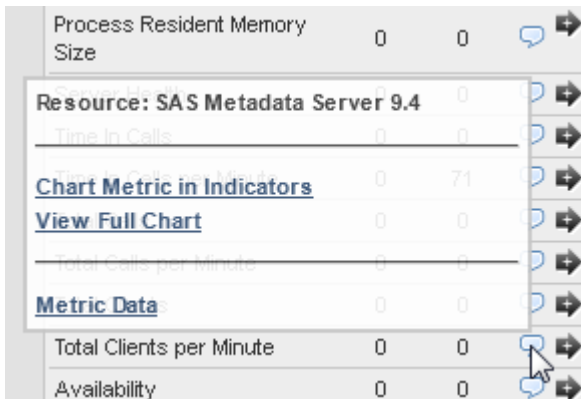
- 1 On the SAS Environment Manager menu bar, select **Resources** ► **Browse**.
- 2 On the Resources page, in the **All Server Types** field, select **SAS Metadata Server 9.4** and then click on the arrow  at the right of the filter fields.
- 3 In the table of resources, click on the name of the metadata server to display the resource detail page.
- 4 On the left side of the resource detail page, select **All Metrics** from the menu.





















The screenshot displays the SAS Environment Manager interface. At the top, there are tabs: **Monitor**, **Inventory**, **Alert**, **Control**, and **Views**. Below these, a 'Metric Display Range' section includes a 'Previous Page' button, a 'Last' dropdown set to '4', a 'Days' dropdown, and an 'OK' button. The main content area is divided into two sections: 'Services' and 'Indicators'. The 'Services' section on the left shows a message 'No health data is available for this resource.' and a table with columns 'Host Platform', 'Status', 'OOB', and 'Alerts'. The 'Indicators' section on the right shows a 'Metric Data' tab and a 'Current Clients' chart for the 'SAS Metadata Server 9.4'. The chart displays a line graph with blue dots representing data points over time. A 'Health' section is visible at the bottom right.

Host Platform	Status	OOB	Alerts
Problem Metrics	0	69	
All Metrics	0	4	

- 5 In the table of metrics, find **Total Clients per Minute** and position your mouse cursor over the information icon . The metric information tooltip appears.




Process Resident Memory Size	0	0		
Resource: SAS Metadata Server 9.4	0			
Time In Cells	0	0		
Chart Metric in Indicators	0	71		
View Full Chart	0	0		
Total Calls per Minute	0	0		
Metric Data	0	0		
Total Clients per Minute	0	0		
Availability	0	0		

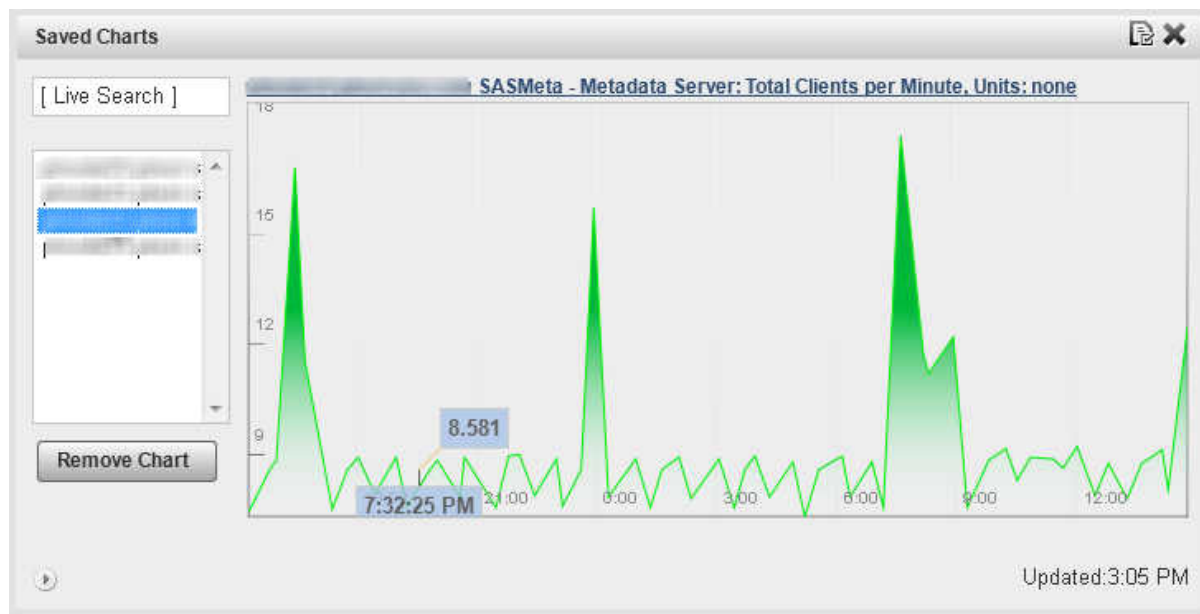
- 6 On the tooltip, select **View Full Chart**. The Metric Chart page appears.
- 7 On the Metric Chart page, select **Save Chart to Dashboards**.
- 8 The Save Chart to Dashboards dialog box appears. Select the dashboards on which the saved chart should appear. Click **Add** to save the chart.

Adding a Saved Charts Portlet

Follow these steps to add a portlet that displays the charts that you have saved.

- 1 Click **Dashboard** on the menu bar.
- 2 On the left side of the Dashboard page, select **Saved Charts** in the **Add Content to this column** field and click the Add icon .

A **Saved Charts** portlet is added to your Dashboard and automatically displays a slideshow of the charts that you previously saved.



- 3 To change how long each chart is displayed or the time period displayed on the chart, click the Configuration icon .

Saved Charts

Configuration

Chart Rotation ☒

Rotation Interval 10 second(s) ▼

Time Range 1 day(s) ▼

Save Cancel

Finding Resources in Your System

<i>Automatically Discovering and Adding SAS Resources</i>	51
<i>Using the Auto-Discovery Portlet</i>	52
<i>Performing an Auto-Discovery Scan</i>	53
<i>Rediscovering Resources</i>	53
<i>Manually Adding a Server</i>	54
<i>Manually Configuring a Service</i>	55

Automatically Discovering and Adding SAS Resources

When the SAS Deployment Wizard installs SAS applications, it creates a file called `auto-approved.properties`. This file is located in the `<agenthome>/conf` directory. This file lists all of the resource types that are automatically monitored after they have been discovered. When you run SAS Environment Manager for the first time, the application auto-discovers and auto-accepts the resources listed in the `auto-approved.properties` file. All of the resources in your initial SAS installation are automatically in your inventory when you start using SAS Environment Manager. Resource types that are not listed in this file must be accepted for monitoring after they have been discovered.

Using the Auto-Discovery Portlet

The Auto-Discovery portlet displays a list of servers and platform services that are auto-discovered but not auto-accepted. All SAS resources should be auto-discovered and auto-accepted, so they will not appear in this portlet. Resources that are listed on the portlet are known but are not yet being monitored. After the resources from the initial SAS installation have been discovered and added to the inventory, the Auto-Discovery portlet lists new resources from custom plug-ins that have been added to the monitored platforms.

To discover and add resources, follow these steps:

- 1 On the Dashboard, check the **Auto-Discovery** portlet to see whether new resources are listed.
- 2 Select the check box beside the resources that you want to monitor and select **Add to Inventory**.
- 3 Go to the Resources page. The resources you just added are listed in the appropriate table, together with any resources that are already being monitored. However, an Unknown icon (🔍) is displayed in the **Availability** column for the new resources, because SAS Environment Manager has not begun to collect monitoring data. SAS Environment Manager collects data at intervals rather than continuously, so you must wait for the next data-collection cycle.
- 4 After approximately five minutes, data should be collected for the new resources and the **Availability** column reflects the status of the resources.

If the status of a new resource is displayed as Unknown even after a period of waiting, then the resource might not be completely configured for data collection. To configure the resource, follow these steps:

- 1 In the Resource page, locate the resource whose status is unknown and click on the entry in the Resources table. The Monitor page for the selected resource is displayed.

- 2 A message is displayed if the resource needs to be configured. If you need to perform additional configuration steps, select **Inventory** to display configuration details for the resource.
- 3 Scroll to the **Configuration Properties** area of the page and verify that the properties are correct. Click **Edit** to make changes to the properties.

Performing an Auto-Discovery Scan

If you know that resources have been added on a platform that you are monitoring, you can run an auto-discovery scan on the platform to locate the resources. Once the resources have been discovered, you can add them to your inventory for monitoring.

To perform an auto-discovery scan of a platform, follow these steps.


- 1 Using the **Resources** tab, go to the Detail page for the platform that you want to scan.
- 2 Select **Tools Menu ► New Auto-Discovery**
- 3 If you want to scan for all servers and system processes on the platform, click **OK**.
- 4 If you want to scan for specific server types, select the check boxes for the server types that you want to scan for. You can also select attributes such as directories to include or exclude from the scan and the depth at which to scan. When you have specified the scanning criteria, click **OK** to start the scan.

Rediscovering Resources

After resources have been auto-discovered, there might be some resources that cannot be added to the inventory for some reason. If this happens, you can clear the contents of the auto-discovery queue and try discovering them again. After the resources are

removed from the queue, and you restart the agent, the agent will rediscover the resources.

To clear the auto-discovery queue follow these steps:

- 1 Select **Manage ► HQ Health** to display the HQ Health page.
- 2 On the HQ Health page, select the **Database** tab.
- 3 In the **Action** field, select **Purge AIQ Data** and click .

You can also manually delete any server resources from the Resources page. The servers are then rediscovered when you run an auto-discovery scan.

Manually Adding a Server

There might be some instances where you need to monitor a server that is not auto-discovered by the SAS Environment Manager agent. To manually add a server, follow these steps:

- 1 Navigate to the Resource Detail page for the platform on which the server runs.
- 2 Select **Tools Menu ► New Server** to display the New Server page.
- 3 On the New Server page, specify the server name.
- 4 Use the **Server Type** menu to select the type of server. If the server type that you want to add is not listed, it is not supported by SAS Environment Manager and cannot be added.
- 5 In the **Install Path** field, specify the full pathname to the server software.
- 6 Click **OK** to complete the server definition.

Note: Because the agent does not update data continuously, it might take several minutes before metric data begins appearing for the new server.

Manually Configuring a Service

There might be some instances where you need to monitor a service that is not auto-discovered by the SAS Environment Manager agent. To manually add a service, follow these steps:

- 1 In the Resources view, select the platform that contains the service that you want to monitor.
- 2 In the Detail view for the selected platform, select **Tools Menu ► New Platform Service**.
- 3 Specify a name for the service and select the service type. Common selections include **HTTP**, **Fileserver File**, and **TCP**.
- 4 Click **OK** to create the service and display the service details. Select the **Configuration Properties** link on the page.
- 5 Use the instructions on the Configuration Properties page to specify the options needed to monitor the service.

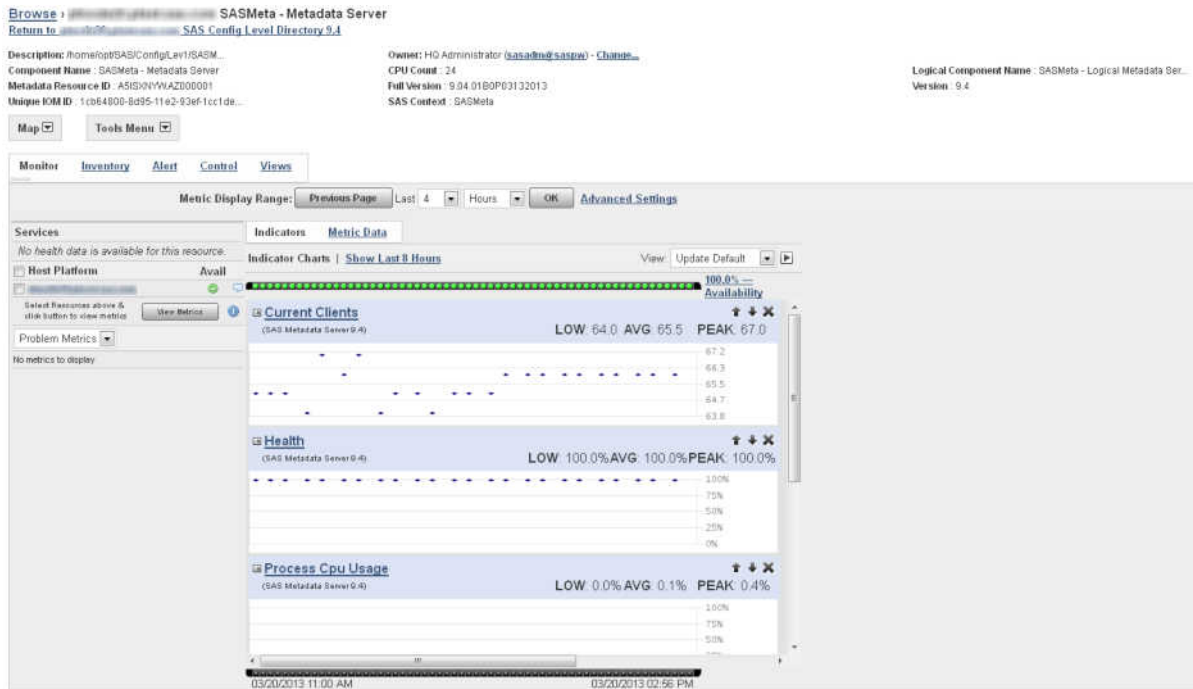
Monitoring and Controlling Resources

- Monitoring Resources* 57
- Managing SAS Resources* 60
 - SAS Server Names 60
 - Using the Map Control 60
- Making Resources Easier to Locate* 62
 - Organizing Resources into Groups 62
 - Create a Group 64
 - Create an Application 64
- Controlling Resources Using Control Actions* 65
 - What is a Control Action? 65
 - Performing Immediate Resource Control Actions 65
 - Scheduling Resource Control Actions 66
 - Performing Server Actions in Response to an Alert 67

Monitoring Resources

A central capability of SAS Environment Manager is the ability to monitor resources. Monitoring enables you to track a resource’s availability and overall health. A variety of metric data is displayed, both in numeric and graphic format, to enable you to examine detailed information about the resource’s operation.

To view the monitoring information for a resource, select a resource from the table on the Resources page.



The fastest way to check the status of the selected resource is to use the availability bar, which is above the indicator charts. The availability bar displays a color-coded dot that represents the availability during a time slice. The length of each time slice depends on the display range that you select (for example, if you display the past eight hours of data, each dot corresponds to approximately eight minutes). The percentage of time that the resource was available is displayed at the end of the availability bar.

The dots are color-coded using the following format:

Green

100% availability

Yellow

Partial availability; between 0% and 100%

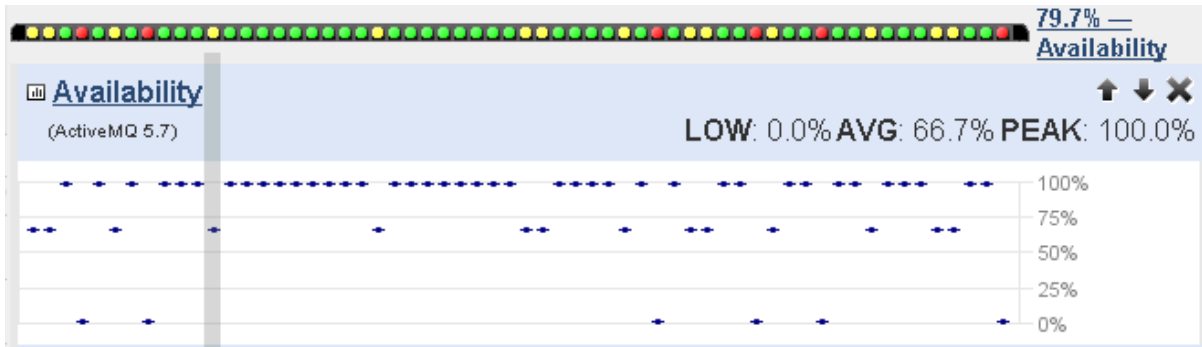
Red

0% availability

An availability bar such as the one in the following figure shows that the resource fluctuated between being available, partially available, and unavailable over the most recent time slices.



To help determine the cause of availability problems, click on the dot for a particular time slice. The selected time slice is highlighted on the indicator charts below the availability bar. This function helps you quickly check the charts for data that might correspond to the availability problem.



To change the metrics that are displayed in the metric charts, use the menu on the left side of the page to select either **All Metrics** or **Problem Metrics**, and then click **View Metrics** to display a list of available metrics. Click the arrow beside a metric to add the chart to those displayed on the page.

Select Resources above & click button to view metrics
View Metrics

All Metrics
OOB Alerts

Process Cpu Usage	0	0	ⓘ ➡
Process Resident Memory Size	0	0	ⓘ ➡
Availability	0	0	ⓘ ➡

The events bar is displayed below the indicator charts. It is similar to the availability bar, with dots representing time slices. The bar displays only a red dot if an event occurs during a time slice. If no event occurs, the bar remains black.



Managing SAS Resources

SAS Server Names

Because SAS Environment Manager is based on VMWare’s Hyperic, some server names in SAS Environment Manager do not match the names that are used in a SAS deployment. Use this table to determine the name of the server that you are interested in.

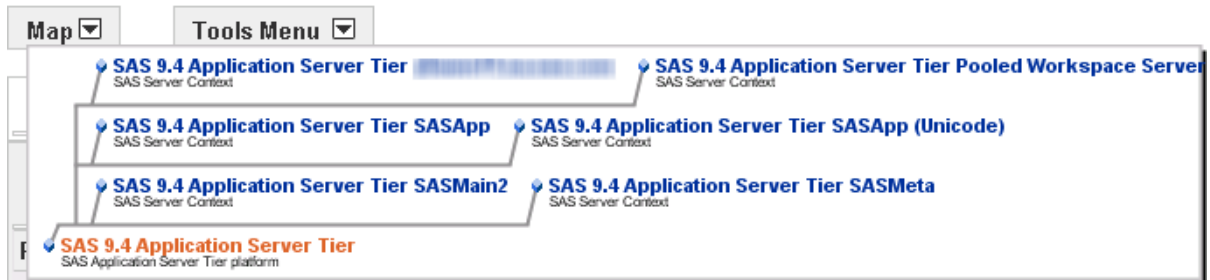
SAS Server Name	Server Name Displayed in SAS Environment Manager
SAS Environment Manager	Apache Tomcat 5.5, 6.0, 7.0
SAS Environment Manager Agent	HQ Agent
SAS Web Server	vFabric Web Server 5.1, 5.2
SAS Web Application Server	SpringSource tc Runtime 7.0
SAS Web Infrastructure Platform Data Server	PostgreSQL 9.x
SAS JMS Broker	Active MQ 4.0, 5.0, 5.1, 5.2, 5.3, 5.4, 5.7

Using the Map Control

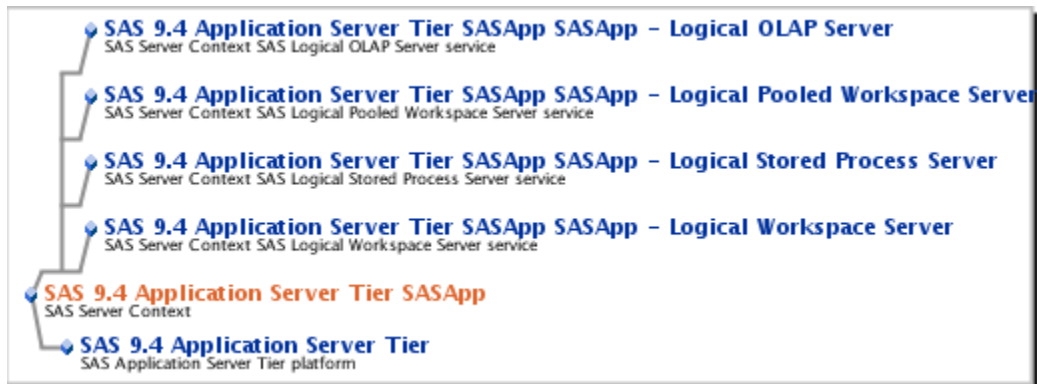
The **Map** control provides a visual representation of resources and the next level of parent and child resources. You can click on any of the resources listed on the map to go to the Monitor page for that resource. The **Map** control is available on the Monitor page for a resource.

The map for a platform displays the servers under the platform, and the map for a server displays the services under the server. You can use the map to better understand how a SAS environment is presented in SAS Environment Manager.

In SAS Environment Manager, the SAS Application Server Tier is a platform. The map for the platform illustrates the SAS servers that are part of the server tier.



Logical SAS servers, such as logical workspace servers or logical stored process servers, are SAS Environment Manager services, so they are displayed as children under the SASApp server.



For a SAS Object Spawner, the services listed in the map are the servers that are spawned by the spawner.



Making Resources Easier to Locate

Organizing Resources into Groups

In SAS Environment Manager, resources are organized into groups to make them easier to locate and manage. There are six different types of groups:

- platform resource groups
- server resource groups
- service resource groups
- compatible groups
- mixed groups
- applications

resource groups

These groups are automatically created. When resources are discovered and then added to the inventory of monitored resources, they are added to the appropriate resource group. The three resource groups that are automatically created in SAS Environment Manager are platforms, servers, and services. It is important to note how SAS resources map to the resource hierarchy. For example, logical SAS servers are added to the services group.

compatible groups

These groups contain selected instances of a single type of resource (for example, SAS Object Spawners). Creating a compatible group enables you to view aggregate metrics for a resource type. Compatible groups also make it easier for you to locate resources that you need to monitor. For example, you can create a group containing several servers of critical importance, which prevents you from having to search for those servers among the large numbers that might be on your site. After you create a compatible group, you can add resources to the group if they match the selected group type.

mixed groups

These groups are user-created groups that can contain multiple types of resources. Mixed groups can contain other groups, platforms, servers, and services, or applications. Availability is the only metric that is available for a mixed group. This type of group is useful for functions such as checking the availability of a SAS Object Spawner and all of the spawned services or for viewing the collective availability of a group of resources.

application

These groups are a set of selected services, usually running in different servers on multiple platforms, that together fulfill a single business purpose. Creating application groups enables you to manage your infrastructure from an application perspective, as opposed to a hardware perspective.

If you initialize SAS Environment Manager Extended Monitoring, a set of default compatible and mixed groups is created. These groups provide commonly-used collections of resources in a SAS environment. They are automatically updated as you add and remove resources. See [“Initializing SAS Environment Manager Extended Monitoring” on page 101](#) for initialization instructions.

Create a Group

To create and populate a group:

- 1 On the Resources page, select **Tools Menu ► New Group**.
- 2 On the New Group page, specify a name for the group.
- 3 Use the **Contains Resources** menu to select the type of group that you want to create.
- 4 Use the **Select Resource Type** menu to select the type of resource that the group will contain.
- 5 Click **OK** to create the group.
- 6 On the Resources page, click on a resource that you want to add to the group.
- 7 On the Details page for the selected resource, select **Tools Menu ► Add To Group**.
- 8 On the Group Manager page, select the group to which you want to add the resource. If the group that you want to add the resource to is not listed, then the selected resource type is not the same as the resource types that are specified for the group.

Create an Application

To create and populate an application:

- 1 On the Resources page, select **Tools Menu ► New Application**.
- 2 On the New Application page, specify a name for the application. Click **OK** to create the application. The Configuration page for the application appears.
- 3 In the **Services** area, click **Add to List** to select resources for the application.

- 4 In the **Services List**, select the services in the **Services** list that you want to add to the application and use the arrow button to move them to the **Add Services** list. Click **OK** when you finish selecting services, and then click **OK** again to create the application.

Controlling Resources Using Control Actions

What is a Control Action?

Control actions enable you to control certain types of servers and services from SAS Environment Manager. You can create control actions to perform operations such as starting, stopping, restarting, pausing, and resuming a server or starting, stopping and sending messages through a service. The specific actions available depend on the server or service type selected. You can define resource actions to run immediately, to run on a schedule, or to run in response to an alert.

You can use control actions to control these types of servers:


- Postgre SQL SAS Web Infrastructure Platform Data Server (PostgreSQL 9.x)
- SAS Object Spawner
- SAS OLAP Server
- SAS Metadata Server
- SAS Web Application Server (SpringSource tc Runtime)

Performing Immediate Resource Control Actions

To use a control action to perform an immediate action on a resource, follow these steps:

- 1 In the Resource Details page for the selected server or service, click **Control**. If this menu item is not present, the resource does not support control actions. The Control Action page is displayed.

The screenshot shows a web interface for controlling resources. At the top, there's a 'Current Status' section with the text 'No current Action'. Below that is the 'Quick Control' section, which states 'Quick Control Actions will occur after the current Control Action'. It features a 'Control Action:' dropdown menu set to 'Start' and a 'Control Arguments (optional):' text input field. A note below the input field says 'Quick Control Actions will be done in parallel to all resources.' At the bottom, there's a 'Control Action Schedule' section with a 'Click "New..." below to schedule a Control Action.' instruction. Below this is a table with columns 'Control Action', 'Date Scheduled', and 'Description'. The table is currently empty. At the bottom right, there's a 'Total: 0' and 'Items Per Page: 15' indicator.

- 2 In the **Quick Control** area, select the type of action that you want to perform in the **Control Action** field.
- 3 Specify any arguments for the action in the **Control Arguments** field.
- 4 Click  to perform the action.

Scheduling Resource Control Actions

To create a scheduled resource control action, follow these steps:

- 1 In the Resource Details page for the selected resource, click **Control**. If this menu item is not present, the resource does not support control actions. The Control Action page is displayed.
- 2 In the **Control Action Schedule** area, click **New**. The Scheduled Control Action page is displayed.
- 3 Select the action that you want to perform in the **Control Action** field.
- 4 In the **Schedule** area, select the radio button next to the date and specify the date and time that the scheduled action should take place.
- 5 Specify how often the action should recur and when the scheduled recurrence should end.

The screenshot shows the 'Control Action Properties' dialog box. At the top, there's a 'Control Action' dropdown menu currently set to 'Restart'. To its right is a 'Description' text area. Below this is the 'Schedule' section. Under 'Start', the 'Immediately' radio button is selected, and a date/time picker shows 'Jun 12, 2014' at '11:00 PM'. A small text note says 'Specify date & time to view recurrence options'. Under 'Recurs', the 'Weekly' dropdown is selected, and 'Every 1' is entered in the frequency field. The 'Week(s) On' section has checkboxes for 'Sunday', 'Monday', 'Tuesday', 'Wednesday', 'Thursday' (checked), 'Friday' (checked), and 'Saturday' (checked). Under 'Recurrence Ends', the 'No End' radio button is selected, and a date picker shows 'Oct 5, 2015'. At the bottom are 'OK', 'Reset', and 'Cancel' buttons.

6 Click **OK** to save the scheduled control action.

To view the list of scheduled control actions for the resource, click **Control** in the Resource Details page for the selected resource. All scheduled control actions are listed in the **Control Action Schedule** area.

Performing Server Actions in Response to an Alert

To define a control action to occur in response to an alert, follow these steps:

- 1 Create or edit an alert definition. See [“Defining an Alert” on page 77](#) for more information. On the Alert Definition page, click **Control Action**, then click **Edit**. The Add Control Action page is displayed
- 2 Use the **Resource Type** field to select the type of server or service for which you want to create the control action.
- 3 After you select the resource type, the **Resource Name** field is populated with all instances of the selected resource type. Select the instance for which you want to create the control action.
- 4 Select the type of action to be performed in the **Control Type** field. The field contains only actions that are supported on the selected resource type.
- 5 Click **OK** to define the control action. The defined action will now take place whenever the associated alert occurs.

Working with Events and Alerts

- Creating Resource Events*** **69**
 - Overview of Events 69
 - Creating Events Based on SAS Server Logs 70
- Importing and Exporting Events*** **72**
 - Overview 72
 - Importing Events 73
 - Exporting Events 74
- Working with Resource Alerts*** **75**
 - Overview of Alerts 75
 - Defining an Alert 77
 - Defining an Escalation Scheme 80

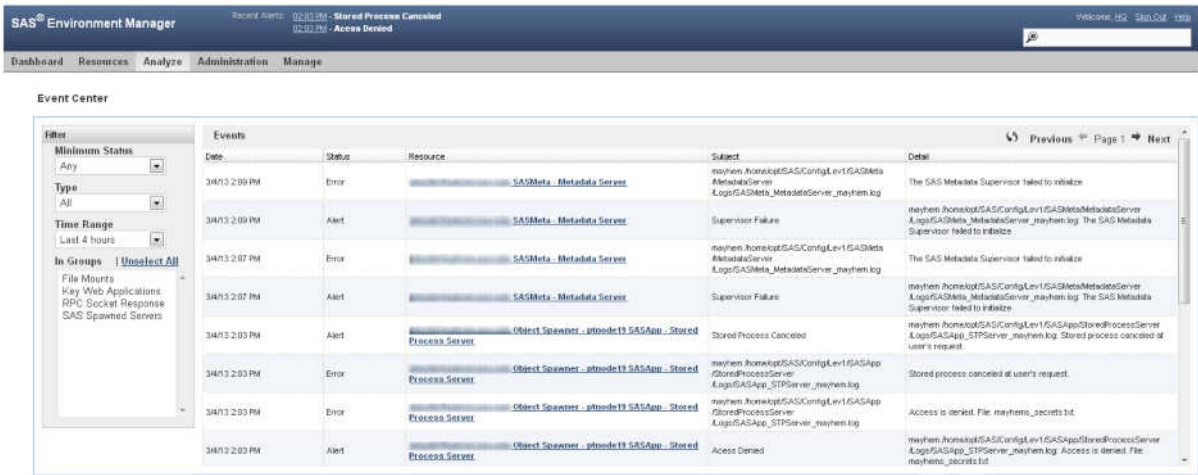
Creating Resource Events

Overview of Events

SAS Environment Manager provides the capability to monitor metrics, scan log files, manage configuration changes, and monitor availability. When there is a change in a resource's threshold value for one of these items, an event is recorded in SAS Environment Manager's event message system. Events are also automatically created for certain types of entries in SAS server logs, and you can specify other criteria that will create events based on SAS server logs. All events throughout the entire deployment

are displayed in the Event Center. To access the Event Center, select **Analyze ► Event Center**.

Figure 6.1 Event Center



The table shows information about recently recorded events, including the status, the resource involved, and information about what caused the event to be triggered. You can subset the table to locate events more quickly. For example, you can show only the events that have at least Error status, or only the ones that affect resources in a specified group.

Clicking on the name of the resource in the event table takes you to the resource's Detail page.

Creating Events Based on SAS Server Logs

SAS Environment Manager monitors the log files for SAS servers and automatically creates events for error messages recorded in those logs. These logs use the standard logging facilities of SAS. For more information, see *SAS Logging: Configuration and Programming Reference*. The events are added to the rest of the events recorded by SAS Environment Manager.

The types of SAS servers whose logs are used to create events are as follows:

- SAS Metadata Server

- OLAP server
- Object spawner
- Stored process server
- CONNECT spawner
- Workspace server
- Pooled workspace server

You can also change the configuration to look for specific types of SAS server log entries in addition to errors. The file `sev_logtracker_plugin.properties` contains entries for each type of SAS server log entry that SAS Environment Manager looks for. You can add to this file to create events for criteria of your choosing. Each SAS server has its own properties file, so logging events can be created for specific server types.

For example, all `sev_logtracker_plugin.properties` files contain these entries by default:

```
# All fatal
level.fatal.1=.*

#
# All errors
level.error.1=.*
#
# User lockout warnings
level.warn.1=.*Access to this account.*is locked out.*
```

The entries in this file use the format

```
level.[level_of_message].[sequential_number]=[regular_expression]
```

.

`level.fatal.1=.*` specifies that an event is created whenever a message appears in the SAS log with a level of Fatal. The message can contain any text. The second entry produces the same result for Error messages.

`level.warn.1=.*Access to this account.*is locked out.*` specifies that an event is created whenever a message with a level of Warn appears that also contains the text `Access to this account.*is locked out.`

To add your own entries to the properties file in order to create events for specific messages, follow these steps:

1 Edit the file `<server_config_directory>/sev_logtracker_plugin.properties` (for example, `/opt/SAS/Lev1/SASApp/OLAPServer/sev_logtracker_plugin.properties`)

2 Add a line for the message that you want to track. The format is

```
level.[level_of_message].[sequential_number]=[regular_expression]
```

For example, this entry looks for an INFO message containing the phrase “AUTOEXEC processing beginning”:

```
level.info.1=.*AUTOEXEC processing beginning.*
```

.

3 If you add multiple entries to look for messages at the same log level, increment the number. For example,

```
level.info.2=.*Message text here.*
```

4 Save the file. SAS Environment Manager automatically uses the revised file.

Importing and Exporting Events

Overview

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.

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 indicating 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 file that you want to track in the **service.log_track.files** field. The file that you specify in this field is the log file that external SAS applications or programs write to. Specify a single log file in this field, and do not use wildcards in the file name. Click **OK** to save the configuration.

If you want a SAS program to create an event, add the EVEVENT macro. This macro creates an event in the proper format and stores it in a specified directory. The syntax for the macro is as follows:

```
%macro evevent(src=source_message_string,msglevel=message_level
,msgtext=message_string);
```

src=

specifies the originator of the event. You can also use this parameter to specify the format of the text in the msgtext= parameter. The value that you specify for the format is specified by the parser. Use a colon (:) to separate the originator and the

format information. For example, you can specify DSA:NVP, where DSA specifies the originator of the event and NVP specifies that the message string uses name-value pairs.

msglevel=

specifies the level of the event. Valid values are **DEBUG**, **INFO**, **WARN**, and **ERROR**.

msgtext=

specifies the text of the event message.

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
- 5 The detail page for the service displays a message indicating that the service has not been configured. Click the **Configuration Properties** link.
- 6 On the Configuration Properties page, select the **exporter.enable** check box to turn on event exporting. Click **OK** to save the configuration.
- 7 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.
- 8 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.

The format of an exported event is as follows:

```
dateTtimeoffset | msglevel | source | message
```

The *date* is specified as *yyyy-MM-dd*.

The *time* is specified as *HH:mm:ss*.

The *msglevel* must be one of these values: ERROR, WARN, INFO, DEBUG.

Here is an example of an exported event:

```
2014-08-06T14:59:20-0400|WARN|EMI Framework|emiInit ran with -f force option
```

Working with Resource Alerts

Overview of Alerts

If you want to identify a type of event for notification or further action, you can create an alert. Alerts are a user-defined type of event that indicates a critical condition in a selected resource. When an alert occurs, it must be acknowledged, and alerts are listed until they are marked as being fixed. You can define escalation schemes to identify the actions that happen if an alert is not fixed within a specified time.

Alerts are logged by the agents and all events throughout the entire deployment are displayed in the Alert Center. To access the Alert Center, select **Analyze ► Event Center**.

Alert Center

Alerts

Definition

Alert Filter

Show:

Not Fixed

In Escalation

All

Alert type:

Resource

Minimum priority:

! Low

In the last:

day

Group:

-- All Groups --

Resource Alerts

Previous

Page 1

Next

<input type="checkbox"/>	Date	Alert Definition	Resource	Platform	Fixed	Ack	Priority
<input type="checkbox"/>	3/25/13 9:55 AM	Host Credentials	Object Spawner - ptnode20		No		Med
<input type="checkbox"/>	3/25/13 3:47 AM	Stored Process Canceled	Object Spawner - ptnode20 SASApp - Stored Process Server		No		Med
<input type="checkbox"/>	3/24/13 7:45 PM	Server Not Running	Object Spawner - ptnode20 SASApp - Pooled Workspace Server		No		Med
<input type="checkbox"/>	3/24/13 4:45 PM	Server Launch	Object Spawner - ptnode20		No		Med

Fixed

Acknowledge

Click the icon to acknowledge an alert

You can filter the alerts, for example, so that only the most recent ones or the ones of a specified type are displayed. Click the icon to acknowledge an alert. Select the check box next to an alert, and then click **Fixed** to fix the alert. You can also click on the entry in the **Alert Definition** column to display the Alert Details page, where you can view details about the alert and mark the alert as fixed (with comments).

Object Spawner - ptnode20 SASApp - Stored Process Server: Stored Process Canceled: Alert Detail

[<< Resource Alert List](#)

Alert Properties	
Name: Stored Process Canceled	Priority: II - Medium
Resource: Object Spawner - ptnode20 SASApp - Stored Process Server	Alert Date: 03/25/2013 03:47 AM
Description: Stored process has been canceled at the user's request	Alert Status: Not Fixed

Condition Set
If Condition: Event/Log Level(ERR) and matching substring "Stored process canceled at user's request"
Actual Value: mayhem /home/opt/SAS/Config/Lev1/SASApp/StoredProcessServer/Logs/SASApp_STPServer_mayhem.log: Stored process canceled at user's request.
Enable Action(s): Each time conditions are met.

Control Type: none

Notification Actions
Notify Roles: (none)
Notify Users: (none)

Fix

Resolution for Fix:

Click the "Fixed" button to mark alert condition as fixed

[<< Resource Alert List](#)

If you initialize SAS Environment Manager Extended Monitoring, a set of alerts is automatically created for you. These alerts identify the most common problems in a SAS environment. Using the alerts in SAS Environment Manager Extended Monitoring enables you to start working with SAS Environment Manager quickly, without having to manually define alerts. See [“Initializing SAS Environment Manager Extended Monitoring” on page 101](#) for initialization instructions.

Defining an Alert

To define an alert, follow these steps:

- 1 Select **Resources** ► **Browse** or use a dashboard portlet to locate the resource for which you want to create an alert.
- 2 There are three icons on the left of the entry for the resource in the table . Click on the alert icon , which is on the right of the group. The Alerts page for the resource appears.

[Browse](#) > [ptnode22.ptest.sas.com](#) Object Spawner - ptnode22

Description: /opt/SAS/Config/Lev1/ObjectSpa...

Component Name : Object Spawner - ptnode22

Full Version : 9.04.01M1P10302013

SAS Context : N/A

Owner: HQ Administrator ([sasadm@saspw](#)) - [Change...](#)

CPU Count : 24

Version : 9.4

Metadata Resource ID: A5KE8INUJAZ000003
Unique IOM ID: 1267f000-aafb-11e3-932b-d48564...

Map

Tools Menu

Monitor

Inventory

Alert

Control

Views

Alerts

Configure

	Description	Date Created	Last Modified	Active
<input type="checkbox"/> Alert Definition ^				
<input checked="" type="checkbox"/> Object Spawner ERROR message in log	Object Spawner ERROR message in log	03/04/2014 07:48 AM	03/29/2014 10:05 PM	Yes
<input checked="" type="checkbox"/> Object Spawner User Lockout	User account lockout on Object Spawner due to excessive login failures	03/04/2014 07:48 AM	03/29/2014 10:05 PM	Yes
<input checked="" type="checkbox"/> Object Spawner Failed Connections	Object Spawner failed to spawn server request	03/03/2014 03:20 PM	03/29/2014 10:05 PM	Yes
<input checked="" type="checkbox"/> Object Spawner Major (page) Faults	Major Faults are page faults requiring disk activity. Possible indication of a memory constraint causing slow performance	03/04/2014 08:19 AM	03/29/2014 10:05 PM	Yes
<input checked="" type="checkbox"/> Object Spawner Server Health % < 100	Object Spawner Health < 100%. Service Ping (equivalent of SASMC Validate) to confirm server is responding	03/03/2014 03:28 PM	03/29/2014 10:05 PM	Yes

New

Delete

Set Active:

Yes

Total: 5

Items Per Page:

15

* Resource Type Alert Definitions (cannot be deleted)

3 Click **New** to display the New Alert page.

Alert Properties

Name:

Description:

Priority:

High - Medium

Active:

Yes

Condition Set

Condition:

Metric

Select

> (Greater than)

(absolute value)

> (Greater than)

% of

value changes

Control Action:

Select

 = (Equal to)

Select

Events/Logs Level:

Any

 Substring to Match (optional, 150 chars max):

Config changed and match file name (optional, 150 chars max):

Add Another Condition

Recovery Alert:

Select alert name

Select

Enable Action(s):

Each time conditions are met

Within a time period of: minutes Occurrence:

Enable Action Filters:

Generate one alert and then disable alert definition until fixed

Disregard control actions that are defined for related alerts.

OK

Reset

Cancel

4 In the **Alert Properties** area, specify the name and priority for the alert and whether it is active.

5 In the **Condition Set** area, specify the conditions that must be met in order for the alert to be triggered. You can specify up to three conditions for each alert. Use these fields to specify the condition that triggers the alert

Metric

specifies that the alert is triggered based on the value of a metric that is monitored for the resource. You can specify that the condition is based on comparison to a fixed value, a percentage of a value, or a change in value. If you

want to create an alert for a metric that is not 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).

Inventory Property

specifies that the alert is triggered based on a change in the value of a resource property (such as version number). This condition is available only for certain types of resources (such as platforms and SAS Metadata Servers).

Control Action

specifies that the alert is triggered when an action meets a specified condition (such as the action of stopping a failed server). This condition is available only for servers that can be controlled through control actions. See [“Controlling Resources Using Control Actions” on page 65](#) for more information.

Events/Logs Level

specifies that the alert is triggered when a selected type of log entry (such as Error) and an optional accompanying text string appears in the log.

If you are defining an alert based on events from SAS server logs, the available values in this field do not match the logging levels available in SAS server logs. The four SAS Environment Manager levels must match the six levels in SAS server logs. Selecting Error in this field matches both the Fatal and Error levels in SAS server logs. Selecting Debug in this field matches both the Trace and Debug levels in SAS server logs.

Config changed

specifies that the alert is triggered when a configuration file changes (you can choose to specify the name of the configuration file).

- 6 In the **Enable Action** field, specify whether the alert is triggered only once, or periodically as long as the alert condition persists.
- 7 Click **OK** to define the alert and display the Alert Configuration page.

[Escalation](#) [Control Action](#) [Notify Roles](#) [Notify Users](#) [Notify Other Recipients](#) [Script](#) [OpenNMS](#)

<input type="checkbox"/> First Name	Last Name	Username ▲	Email	Department
<input type="checkbox"/> HQ	Administrator	sasadm@saspw	sasadm@saspw	

Add to List

Remove from List

Total: 1 Items Per Page: 15 ▼

<< [Return to Alert Definitions](#)

- 8 On the Alert Configuration page, you can specify an escalation scheme and identify the users and roles that should be notified when the alert occurs. To create an escalation scheme, see “[Defining an Escalation Scheme](#)” on page 80.
- 9 Click **Return to Alert Definitions** when you are finished.

Defining an Escalation Scheme

An escalation scheme is a series of actions that take place when an alert is not acknowledged or fixed within a certain period of time. An escalation scheme can be applied to multiple alerts. You can define an escalation scheme to perform any of these actions:

- send an e-mail or SMS message
- make an entry in a system log
- issue an SNMP notification

To define an escalation scheme, select **Manage ► Escalation Schemes Configuration** (in the **Server Settings** area).

Escalation Schemes Configuration

[<< Return to Manage](#)

Escalation Name:

[Default Escalation](#)

An escalation scheme allows you to order alert notifications and actions. It can be applied to one or more alert definitions.

Step 1 - Create New Escalation Scheme:

* Name:

Description:

If the alert is acknowledged:

- ☐ Allow user to pause escalation for
- ☒ Continue escalation without pausing

If the alert state has changed:

- ☒ Notify previously notified users of the change
- ☐ Notify entire escalation chain of the change

If alert is not fixed when escalation ends:

- ☒ Stop escalation execution
- ☐ Repeat escalation actions

For information about the information required when defining an escalation scheme, refer to the Help for the page.

Controlling Access to SAS Environment Manager

<i>Controlling Access to SAS Environment Manager</i>	83
About Native Roles and Users	83
SAS Environment Manager and SAS Metadata Users	84
Updating Passwords for SAS Environment Manager Metadata Identities	86
Creating a Native Role	87
<i>Creating SAS Middle-Tier Administrator IDs</i>	88

Controlling Access to SAS Environment Manager

About Native Roles and Users

SAS Environment Manager controls access and permissions within the application with its own registry of users and its own system of roles and permissions. In order to distinguish between the SAS Environment Manager access features and those in SAS metadata, this document and the SAS Environment Manager online Help refers to features internal to SAS Environment Manager as native features (such as native users or native roles). However, the SAS Environment Manager interface does not use the native terminology.

Although native user definitions are internal to SAS Environment Manager, they are mapped to user definitions created in SAS metadata. Native users are created by first creating the user definition in metadata and then synchronizing the user information with SAS Environment Manager. You cannot create native user definitions in SAS Environment Manager directly.

Native roles enable you to grant capabilities and permissions for actions in SAS Environment Manager to selected users. For example, an administrator role could be granted full permissions for all resource types and the ability to acknowledge and fix alerts, while a guest role could be denied the ability to fix or acknowledge alerts and have only Read permission for resources. Assigning a native role to a native user determines the actions that the user can perform in SAS Environment Manager.

Each native role also has its own unique Dashboard page. Each user has access to their own personal Dashboard page and the Dashboard pages of all native roles of which they are a member.

SAS Environment Manager and SAS Metadata Users

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 and subgroups 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:

Group name in SAS metadata	Role in SAS Environment Manager
SAS_EV_Super_User	Super User role
SAS_EV_Guest	Guest role
SAS_EV_AppServer_Tier	SAS App Tier role

For example, users that are members of the group SAS_EV_Guest in metadata are created as users in SAS Environment Manager and are assigned to the Guest role when the users are synchronized.

When you install SAS Environment Manager, all existing SAS Environment Manager user definitions are automatically added to the SAS_EV_Guest group in metadata. After the existing users have been added to the SAS_EV_Guest group, use SAS Management Console to modify the user definitions or assign users to other SAS_EV groups in metadata.

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 group.

The mapping between user information in metadata and in a SAS Environment Manager user definition is as follows:

Metadata field	SAS Environment Manager field
Display Name	First Name and Last Name
Name	First Name if the Display Name is not specified
Account	Username
Email	Email
Phone	Phone

To create a new SAS Environment Manager user, select **Administration ► Users** in SAS Environment Manager to define the user and assign it to the appropriate SAS_EV user group, and then select **Manage ► Synchronize Users** to create the native user and assign the user to the proper role.

The users in the SAS App Tier role are automatically granted access to the resources in these resource groups:

- SAS App Tier group
- SAS App Tier Server group
- SAS App Tier Services group

An internal account, sasevs (sasevs@saspw), is also created during installation. This account is assigned to the SAS_EV_Guest group. The account is used for communications between the SAS Environment Manager agent and server and enables plugins to access the SAS Metadata Server. The internal account sasadm@saspw is the default account for signing on to SAS Environment Manager.

CAUTION! All accounts in the SAS Environment Manager Super User group have access to the gconsole plugin, which allows groovy code to be submitted. A side effect of this capability is that groovy code can be executed as the server process owner, which is typically the SAS installer account. If your security policy does not permit this account to have this capability, you can move or delete the gconsole plugin. Move or delete the directory `<levelroot>/Web/SASEnvironmentManager/server-5.8.0-EE/hq-engine/hq-server/webapps/ROOT/hqu/gconsole`.

The SAS Logon Manager is used to control the process of logging on to SAS Environment Manager. The application uses the same authentication process and authentication provider as the other SAS web applications.

Updating Passwords for SAS Environment Manager Metadata Identities

To update the password for the sasevs@saspw account, follow these steps:

- 1 Stop all SAS Environment Manager agents on the system.
- 2 On the middle-tier machine, use the SAS Deployment Manager to change the password for the sasevs account.
- 3 Use the SAS Deployment Manager to update the sasevs password on the machines in the other tiers in the system.
- 4 Restart the SAS Environment Manager agents.

Creating a Native Role

To create a native role, follow these steps:

- 1 On the Manage page, select **New Role**.
- 2 On the New Role page, specify a name for the role and select the native permissions and capabilities for each resource type. If you grant the **Read Only** permission for a resource type, you can also select the native capabilities for the resource type. For all other permissions, the capabilities are automatically selected or disabled and cannot be changed.

- 3 Use these guidelines to determine the native permissions to set:

Adding a resource to the inventory and creating alert definitions

Select **Full** or **Read / Write** permissions. Users can also respond to alerts and control resources.

Monitoring resources, responding to alerts, controlling resources

Select the **Read Only** permission and grant the capability to acknowledge and fix alerts and to control resources. Users can respond to alerts and control resources but cannot create or modify alerts or resources.

Monitoring resources

Select the **Read Only** permission, but do not grant capabilities for alerts resource control. Users can view and monitor only resources.

- 4 When you click **OK**, the role and associated Dashboard page are created, and the Role Properties page is displayed. Use this page to select native users and resource groups that should be associated with the role and to create an alert calendar.
- 5 To create an alert calendar, select the days and times during which the roles' users will be notified of alerts. Make sure that at least one role is available during every time period.

The image shows a configuration window titled "Alert Calendar". It contains two main sections. The left section lists the days of the week from Monday to Sunday, each with a checked checkbox and a time range set to "From: 12 AM" and "To: 12 AM". The right section has a similar layout but with "Except" checkboxes and time ranges set to "From: 1 AM" and "To: 2 AM". A "Save" button is located at the bottom left.

Day	From	To	Except	From	To
<input checked="" type="checkbox"/> Monday	12 AM	12 AM	<input type="checkbox"/> Except	1 AM	2 AM
<input checked="" type="checkbox"/> Tuesday	12 AM	12 AM	<input type="checkbox"/> Except	1 AM	2 AM
<input checked="" type="checkbox"/> Wednesday	12 AM	12 AM	<input type="checkbox"/> Except	1 AM	2 AM
<input checked="" type="checkbox"/> Thursday	12 AM	12 AM	<input type="checkbox"/> Except	1 AM	2 AM
<input checked="" type="checkbox"/> Friday	12 AM	12 AM	<input type="checkbox"/> Except	1 AM	2 AM
<input checked="" type="checkbox"/> Saturday	12 AM	12 AM	<input type="checkbox"/> Except	1 AM	2 AM
<input checked="" type="checkbox"/> Sunday	12 AM	12 AM	<input type="checkbox"/> Except	1 AM	2 AM

Creating SAS Middle-Tier Administrator IDs

Administrators for SAS middle-tier servers must be defined in SAS metadata as well as in SAS Environment Manager. To create a middle-tier administrator user ID, follow these steps:

- 1 From the **Administration** tab in SAS Environment Manager, use the User Manager to create a user definition for a middle-tier administrator.
- 2 Assign the user to the SAS_EV_AppServer_Tier user group. This group is created during the installation and configuration process.
- 3 Sign in to SAS Environment Manager using the sasevs@saspw credentials, which is the default administrative identity.
- 4 Click **Manage** ► **Synchronize Users** to synchronize the SAS Environment Manager users with the SAS metadata users..
- 5 Click **List Users** to view the list of all users.
- 6 Locate the entry in the user table for the new user and click the user name entry to display the Properties page.
- 7 In the Roles Assigned To section, verify that the user is assigned to the **SAS App Tier** role.



Part 2

Operations Integration, Audits, and Performance Analysis

Chapter 8

<i>Understanding SAS Environment Manager Service Management Architecture</i>	91
---	-----------

Chapter 9

<i>Initializing and Enabling the Service Management Architecture</i>	101
---	------------

Chapter 10

<i>Using the Report Center</i>	111
---	------------

Chapter 11

<i>Working With Commands</i>	121
---	------------

Understanding SAS Environment Manager Service Management Architecture

- Understanding SAS Environment Manager
Service Management Architecture* 92
- Working with SAS Environment Manager
Extended Monitoring* 94
 - Purpose and Components 94
 - Understanding the SAS Environment Manager
 - Setup Components 94
 - Data Mart Infrastructure 96
- Working with APM ETL* 96
- Working with ACM ETL* 97
- Working with the Solution Kits Infrastructure* 98
- Feeding Data from the Data Mart into SAS Visual Analytics* 98

Understanding 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). The package implements best practices for resource monitoring, automates and extends the application's auditing and user monitoring capabilities, and follows industry standards to enable servers to use Application Response Measurement (ARM). These functions enable SAS Environment Manager to function as a key component in providing service-level management in a strategy that is based on the IT Infrastructure Library (ITIL).

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 Service Management Architecture consists of the following components:

SAS Environment Manager Data Mart

This is the heart of the Service Management Architecture. The SAS Environment Manager Data Mart consists of preconfigured tables that are used to store monitored data. The collected data is processed so that it is stored in a standard format, making it easy to run reports and perform analysis. The infrastructure for the SAS Environment Manager Data Mart is provided in the SAS Environment Manager Extended Monitoring package.

Audit, Performance and Measurement (APM) ETL

When this component is initialized, it collects information from SAS logs, standardizes it, and stores it in the SAS Environment Manager Data Mart. The collected data is used to populate stored process reports that are provided as part of

SAS Environment Manager Service Management Architecture. The data is also available for custom reporting and analysis.

Agent-Collected Metrics (ACM) ETL

When this component is initialized, it uses information that was collected about the computing resources (such as servers and disk storage), standardizes it, and stores it in the SAS Environment Manager Data Mart. The collected data is used to populate stored process reports that are provided as part of SAS Environment Manager Service Management Architecture. The data is also available for custom reporting and analysis.

Report Center

The Report Center provides a convenient access point for the reports that are provided as part of SAS Environment Manager Service Management Architecture. Once one or more of the ETL components have been initialized and enabled, data is available in the SAS Environment Manager Data Mart. This data is then used to produce the predefined reports in the Report Center. The Report Center is not available until the data mart contains data.

solution kit framework

The solution kit framework can extend the capabilities of SAS Environment Manager to support specific solutions or applications. The framework includes support 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

Data from the SAS Environment Manager Data Mart can be easily loaded into SAS Visual Analytics. If the data feed option is enabled in SAS Environment Manager, selected data tables from the SAS Environment Manager Data Mart are copied to a specified drop zone directory. SAS Visual Analytics can then automatically load the tables from the drop zone into the application.

Working with SAS Environment Manager Extended Monitoring

Purpose and Components

SAS Environment Manager Extended Monitoring implements best practices for SAS Environment Manager and also provides the framework needed for SAS Environment Manager Service Management Architecture. Extended monitoring provides these two separate categories of components:

SAS Environment Manager setup

automates the creation of a predefined set of alerts, resource groups, and best-practice metric configurations. This automation quickly optimizes your SAS Environment Manager configuration and implements best practices in how your environment is monitored

SAS Environment Manager Data Mart infrastructure

provides empty data tables, stored processes, and reports that are populated by data that is provided by the APM, ACM, or solution kit ETL processes

Although extended monitoring is installed when SAS Environment Manager 2.4 is installed, its components are not active until you initialize it.

Understanding the SAS Environment Manager Setup Components

Even if you are not using the extended monitoring and reporting capabilities of SAS Environment Manager Service Management Architecture, extended monitoring provides key components for your resource monitoring strategy. The SAS Environment Manager setup components configure SAS Environment Manager Extended Monitoring to provide best practices in resource monitoring and alerting. These configurations and definitions enable you to begin using SAS Environment Manager right away, without having to perform manual configuration and definition processes. Extended monitoring includes these components:

resource configuration

You must configure resources such as platforms and servers that are added to your SAS Environment Manager inventory during installation so that they can begin collecting metric data. Initializing extended monitoring automates the process of configuring these resources, enabling you to start monitoring resources without having to go through a manual configuration process.

tuned alerts

Extended monitoring provides a set of optimized alerts. These alerts notify you of operational issues that might be encountered in a SAS environment (such as storage issues, server status, and hardware issues).

defined resource groups

Resources that form a logical group (such as all platforms, servers, and services in the SAS App Tier) are automatically collected into predefined groups that are defined in extended monitoring. These groups are automatically updated as you add and delete resources, so they always stay current. A resource group for every reporting table in the SAS Environment Manager Data Mart is automatically created and maintained.

event importing and exporting

You can export events that are generated by SAS Environment Manager in order to support third-party monitoring applications. In addition, you can import events from other SAS applications and from third-party applications into SAS Environment Manager for processing.

HTTP checks of web applications

Enabling extended monitoring defines a set of resources that monitor the availability and responsiveness of key SAS web applications such as SAS Stored Process Web Application.

adjustments to monitoring metrics

As part of the process of optimizing resource monitoring, some adjustments are made in the metrics collected for system resources. Collection is started for some metrics, and graphing intervals are changed for others in order to make them easier to follow.

Data Mart Infrastructure

If you are using SAS Environment Manager Service Management Architecture, extended monitoring provides the framework and key components that enable the ETL packages to operate. Extended monitoring provides these infrastructure components:

SAS Environment Manager Data Mart

Extended monitoring creates the tables that comprise the SAS Environment Manager Data Mart. However, extended monitoring does not provide a mechanism for loading data into the tables. Data is loaded into the tables by the ACM, APM, or solution kit ETL processes.

Report Center processes and reports

Much like with the SAS Environment Manager Data Mart, extended monitoring creates the stored processes and the stored process reports that can be created with data from the data mart. However, these processes and reports remain blank until one or more of the ETL processes is enabled, which loads data into the SAS Environment Manager Data Mart.

Working with APM ETL

The APM ETL process extracts performance metric information from various SAS server logs. After the information is extracted, it is loaded into the SAS Environment Manager Data Mart. As with other information in the data mart, you can use this information to produce predefined reports or to conduct custom analysis and reporting.

APM extracts the data from the SAS logs only when the logs roll over at midnight, so the metric data and the reports display forensic or historical data. It provides a look back at how things have been running, rather than a real-time look at how things are currently running. Reports that are produced by APM display the following kinds of information:

- the most heavily used SAS procedures
- the top ten users of the SAS Workspace Server

- the number of times per day each user ID has accessed the SAS Metadata Server
- each instance of an authentication error or of an unauthorized login attempt
- The response time and run time for SAS stored processes

Note: Enabling the APM ETL process causes a separate log to be created for each spawned SAS Workspace Server. You must plan for the large number of log files that this process creates. A best practice is to create a daily archive file of the day's log files, and then to copy the file to archive storage.

Working with ACM ETL

The ACM ETL process extracts and stores metric data that is collected by the SAS Environment Manager agents into the SAS Environment Manager Data Mart. Storing the data in the data mart enables you to access the data for a longer period of time than if it was stored only in the SAS Environment Manager web application. The ACM ETL processes standardize the data in the database and store it in the data mart, where you can then use the information to produce predefined reports or to conduct custom analysis and reporting.

Reports that are produced by ACM display the following kinds of information:

- response time for SAS HTTP web services
- workload, CPU usage, and memory usage for each platform in your environment
- usage and response information for file mounts
- total number of clients per minute on the SAS Metadata Server machine

Working with the Solution Kits Infrastructure

SAS solutions can provide solution kits, which include their own set of log parsers, resource definitions, tuned metrics, and reports. A solution kit, developed and delivered by SAS, enables you to easily add data to the SAS Environment Manager Data Mart for SAS solutions as you add them to your environment. The ETL framework of the kits provides the infrastructure required for the solution kits to work seamlessly with SAS Environment Manager and the SAS Environment Manager Data Mart. Solution kits ensure that the data collected by SAS Environment Manager for a specific SAS solution is available from the SAS Environment Manager Data Mart.

Feeding Data from the Data Mart into SAS Visual Analytics

You can enable a nightly transfer of selected tables from the SAS Environment Manager data mart to the SAS Visual Analytics administrative reporting drop zone. If autoloading is enabled for associated LASR library, the copied tables are loaded to a SAS LASR Analytic Server. For more information see *SAS Visual Analytics: Administration Guide*

Note: Although data tables that are copied to the drop zone can be loaded into SAS Visual Analytics, predefined reports and analytic processing for the data might not be available in SAS Visual Analytics.

To enable the data feed for SAS Visual Analytics, follow these steps:

- 1 On the machine on which SAS Environment Manager is installed, change to the `[Levelroot]/Web/SASEnvironmentManager/emi-framework/bin` (Unix) or `[Levelroot]\Web\SASEnvironmentManager\emi-framework\bin` (Windows) directory.

- 2** From a command line, issue the command `emi_init.sh -vafeed ON` (Unix) or `emi_init.bat -vafeed ON` (Windows).

The tables copied from the SAS Environment Manager Data Mart to the drop zone are suitable for analysis and reporting with SAS Visual Analytics. The specific set of tables and their structure might change over time and in future releases. By default, the following are the tables that are copied:

ACM.FILEMOUNTS

metric data for the file mounts in your environment

ACM.HOSTPLATFORMS

metrics for the platform-level resource monitored by SAS Environment Manager that correspond to operating systems

ACM.HTTPCHECKS

metric data for the HTTP response-checking resources created by SAS Environment Manager Extended Monitoring

ACM.IOMSERVERS

metric data for the SAS IOM servers, such as SAS Stored Process Server and SAS Pooled Workspace Server

ACM.METADATASVRS

metric data for the SAS Metadata Servers

ACM.NETWORKINTERFACE

metric data for the network interfaces

ACM.TCSEVERMGRS

metric data for individual SAS web applications

ACM.WEBAPPSERVER

metric data for SAS Web Application Server instances

ACM.WIPDATADB

metric data for the databases within the Web Infrastructure Platform Data Server

ARTIFACT.ARTIFACTUSAGEDETAILS

usage information for SAS artifacts (such as libraries, directories, and stored processes)

ARTIFACT.ARTIFACTUSAGESESSIONS

usage information at the session level

ARTIFACT.AUDIT_TRANSACTIONS

audit information for metadata transactions

ARTIFACT.AUDIT_GROUP

audit information for metadata changes related to identity groups

ARTIFACT.AUDIT_ADMUSER

audit information for the administrative user activities

ARTIFACT.AUDIT_ACCESSC

audit records for object access events

ARTIFACT.AUDITACCESSCONTROLDETAIL

audit information about changes made to the access control limits and rules for particular metadata objects

KITS.EMI_INFO

metrics on the performance of SAS Environment Manager ETL processes

KITS.LASR_INFO

metrics for the SAS LASR server; this table exists only if the SAS LASR solution kit has been enabled

KITS.SASJOB_INFO

contains metrics extracted from SAS log files that have been placed in a specified landing zone

For information on the contents of these tables, see [Appendix 3, “Data Mart Table Reference,”](#) on page 211.

Initializing and Enabling the Service Management Architecture

- Initializing SAS Environment Manager Extended Monitoring* . 101
 - Overview of Extended Monitoring Initialization 101
 - SAS Environment Manager Extended Monitoring Steps 103
- Enabling and Initializing the APM ETL* 104
 - Overview of the APM ETL Enablement and Initialization Process 104
 - APM ETL Enablement and Initialization Steps 105
 - Setting up OLAP Server Log Parsing 108
- Enabling ACM ETL* 109
- Enabling Kits Infrastructure* 110

Initializing SAS Environment Manager Extended Monitoring

Overview of Extended Monitoring Initialization

When you initialize SAS Environment Manager Extended Monitoring, two main categories of actions are performed:

- initialization of predefined alerts, groups, and configurations to enable you to start using SAS Environment Manager without having to go through a manual setup process
- initialization of the SAS Environment Manager Data Mart

The initialization process performs both sets of actions. If you are not planning to use the SAS Environment Manager Data Mart, initializing its infrastructure does not impact performance of SAS Environment Manager.

The following setup tasks are performed during the initialization of SAS Environment Manager:

configuration of discovered resources

Resources such as platforms and servers that were added to the SAS Environment Manager inventory during installation are configured so that they can begin collecting metric data.

creation of compatible groups and mixed groups

A set of standard resource groups is created and then populated by resources that were discovered in your environment. After the groups are created, the groups are automatically updated as part of ETL processing.

adjustment of monitoring metrics

The metrics provided by SAS Environment Manager are optimized for monitoring of a SAS environment. The optimization process includes turning data collection on or off for certain metrics and changing sampling intervals for others.

creation of HTTP checks of SAS web applications

These HTTP checks are services that check SAS web applications such as the stored process server to make sure they are operational. The check also generates data such as the length of time the query took.

creation of alerts

The process creates a collection of alerts that signal common operational problems in a SAS environment, such as hardware problems, server issues, and storage issues.

The following tasks are performed for the SAS Environment Manager Data Mart:

preparation of the SAS Environment Manager Data Mart

The initialization process creates infrastructure data sets for the SAS Environment Manager Data Mart.

loading of the Report Center and of reports

The initialization process loads the SAS Environment Manager Service Architecture reports into the SAS Metadata Server. However, unless one or more of the ETL packages are enabled and initialized, the data required to produce the reports is not present and the Report Center is not available from SAS Environment Manager.

SAS Environment Manager Extended Monitoring Steps

To initialize Extended Monitoring:

- 1** If you are on an AIX system, you must add the `sasevs@saspw` account to the Super User role.
 - a** Select **Manage ► List Roles**.
 - b** Select **Super User Role**.
 - c** In the **Assigned Users** area, select **Add to List**.
 - d** Select the check box for **sasevs@saspw** in the **Users** table, click the plus (+) arrow, and then click **OK**.
- 2** On the machine on which SAS Environment Manager is installed, change to the `[Levroot]/Web/SASEnvironmentManager/emi-framework/bin` directory.

Note: Directory paths that are provided in this section are UNIX paths, which use a forward slash (/). In Windows environments, replace the forward slash with a backward slash (\).
- 3** Validate the framework by issuing the command `./validate.sh --level 1` (UNIX) or `validate.bat --level 1` (Windows).
- 4** If you are using UNIX, set the `DISPLAY` environment variable to an X11 server.

- 5 From a command line, issue the command `./emi_init.sh -i` (UNIX) or `emi_init.bat -i` (Windows).

Enabling and Initializing the APM ETL

Overview of the APM ETL Enablement and Initialization Process

When you enable and initialize the APM ETL package, the following actions are performed:

Enablement of Application Response Measurement (ARM)

The SAS Application server environment is modified to enable ARM.

Activation of loggers and appenders

SAS logging facility loggers and log appenders are activated to support the ARM-enabled SASApp deployment

Note: One of the SAS resources for which logging is enabled is the SAS Workspace Server. Logging of this server causes a separate log file to be created in the `Lev1/SASApp/WorkspaceServer/PerfLogs` directory for each spawned SAS Workspace Server. You must be aware of the potential for the large number of log files that can be created in this directory. This situation can occur if you have a large number of SAS Enterprise Guide or SAS Data Integration Studio users, because each session for those applications generates a separate log file. You can create a daily archive of the logs in a .zip or .tar file and then copy the daily archive to another storage location. This process enables you to manage the large number of log files while maintaining IT best practices for retaining usage logs.

Note: SAS Workspace Servers are typically configured to run under the client's user identity. In order for logging of SAS Workspace Servers to function correctly, you must ensure that the permissions are specified correctly on the log directories. All users of the SAS Workspace Server and all SAS Environment Manager users that run the APM ETL processes must have Read, Write, and Execute permissions for the /

`SAS/Config/Lev1/SASApp/WorkspaceServer/Logs` and `/SAS/Config/Lev1/SASApp/WorkspaceServer/PerfLogs` directories.

After the APM ETL is enabled and initialized, the ETL process begins extracting data from SAS logs and loading that data into the SAS Environment Manager Data Mart so that the applicable stored processes and stored process reports have data to work with. Data is extracted from the SAS logs only when the logs roll over (usually after midnight). You must wait until after midnight before data appears in Service Management Architecture metrics and reports.

APM ETL Enablement and Initialization Steps

To enable and initialize APM ETL:

- 1 Ensure that SAS Environment Manager Extended Monitoring has been initialized.
- 2 Back up your configuration files and the SAS metadata repository.
- 3 Change to the directory `[levelroot]/Web/SASEnvironmentManager/emi-framework/bin`.
- 4 Verify that the SAS Metadata Server is running, and then run the command `./apm_init.sh` (UNIX) or `apm_init.bat` (Windows). If you have a host alias, you must add the option `--hostAlias hostAliasName`.

The command creates the files `configureAPMlocal_<machine>.sh` (UNIX) or `configureAPMlocal_<machine>.bat` (Windows) for each machine in your environment.

Note: If your SAS environment contains servers that have been manually configured, that are not part of a standard installation by the SAS Deployment Wizard, or that make up a load-balancing deployment, the generated `configureAPM` files represent a best attempt at creating the configuration for the servers.

- 5 Check the logs under the `emi-framework/Logs` directory for errors.
- 6 Change to the directory `[levelroot]/Web/SASEnvironmentManager/emi-framework/apm`.

- 7 Run the command `./configureAPMlocal_<localmachine>.sh` (UNIX) or `configureAPMlocal_<localmachine>.bat` (Windows), where `<localmachine>` corresponds to the machine that you are currently using.
- 8 If your environment has multiple machines, copy each `configureAPMlocal_<machine>.sh` or `configureAPMlocal_<machine>.bat` file to each machine that corresponds to the `<machine>` value. Make sure that each script has Execute permissions on the machine that it was copied to, and then run the script on each machine.
- 9 If your environment has multiple machines, edit the file `[levelroot]/Web/SASEnvironmentManager/emi-framework/Conf/log_definitions.json`. Locate the entries labeled `"levRoot" : "DEFINE_THIS_MOUNT_POINT"`. Above each of these entries is a description of the remote host's name and the definition for the `levRoot` path from the perspective of the remote host. Change the `DEFINE_THIS_MOUNT_POINT` string to the path of the `levRoot` directory from as seen from the APM ETL host.

For example, if you have a two-machine deployment with the EMI framework deployed on machine `alpha.example.com` and additional SAS resources on a second host named `beta.example.com`, the `log-definitions.json` file on `alpha.example.com` has several entries like this:

```
"name": "SAS - Logical Pooled Workspace Server",
"hostname": "beta.example.com",
"hostLevRoot": "/usr/local/SAS/config/Lev1",
"levRoot": "DEFINE_THIS_MOUNT_POINT",
"contextName": "SASApp",
"logLocation": "PooledWorkspaceServer/PerfLogs",
"baseFilename": "arm4_PooledWSServer",
"operation": "Move"
```

The `hostLevRoot` value specifies the path to the SAS configuration from the perspective of the machine specified by the `hostname` value (`beta.example.com`). If the `beta.example.com` machine uses NFS to export the specified directory, it might be specified differently on the `alpha.example.com` machine (such as `/remote/beta/Lev1`). In that case you would change the `levRoot` value to `"levRoot": "/remote/beta/Lev1",`.

- 10** On each machine in your deployment, ensure that no other users are working in the SAS server environment, and then restart the SAS Metadata Server, SAS Object Spawner, SAS OLAP Server, and Connect Server. Because you should not restart the SAS Environment Manager Server, do not issue the `sas.servers restart` command..

On UNIX, issue these commands for each SAS Application Server context:

```
<levelroot>/SASMeta/MetadataServer.sh restart
<levelroot>/ObjectSpawner/ObjectSpawner.sh restart
<levelroot>/ConnectSpawner/ConnectSpawner.sh restart
<levelroot>/SASApp/OLAPServer/OLAPServer.sh restart
```

On Windows, the servers are usually deployed as Windows services. Follow these steps to restart the servers:

- a** Run Windows using an administrative user ID, and then select **Windows Start ► Control Panel ► Administrative Tools ► Services**. The Services window appears.
 - b** Right-click each of the following entries in the window and select **Stop** from the pop-up menu:
 - **SAS [Config-Lev1] SASApp – OLAP Server**
 - **SAS [Config-Lev1] Connect Spawner**
 - **SAS [Config-Lev1] Object Spawner**
 - c** After you have stopped the previous three servers, right-click **SAS [Config-Lev1] SASMeta – Metadata Server** and select **Restart** from the pop-up menu. Restarting the SAS Metadata Server automatically restarts the OLAP Server, the connect spawner, and the object spawner.
- 11** After the configuration commands have completed, sign on to SAS Management Console. Using the Server Manager plug-in, validate the SAS Metadata Server and the other Enterprise BI servers. The servers generate initial entries in the associated `/Logs` or `/PerfLogs` directories. Sign off from SAS Management Console after you validate the servers.

- 12 On the machine on which SAS Environment Manager is installed, change to the `[levelroot]/Web/SASEnvironmentManager/emi-framework/bin` directory.
- 13 From a command line, issue the command `./emi_init.sh --enable APM` (UNIX) or `emi_init.bat --enable APM` (Windows).
- 14 After the initialization process has completed, sign in to SAS Environment Manager. Select **Resources** ► **Browse** ► **Servers** ► **SAS Environment Manager Data Mart 9.4**.
- 15 On the Resource Detail page for the SAS Environment Manager Data Mart 9.4, select the **APM ETL Processing** service.
- 16 On the Resource Detail page for APM ETL Processing, select **Tools Menu** ► **Configure Service**. Specify the information in the required fields and then click **OK**.

Setting up OLAP Server Log Parsing

Although the APM ETL process can parse and analyze logs from an OLAP server, the best practice is to specify a rolling log appender for the OLAP server. This appender enables the ETL process to copy and process the log entries from the previous day. To specify the appender, follow these steps:

- 1 In the directory `[levelroot]/Web/SASEnvironmentManager/emi-framework/ConfigureFiles`, edit the file `logconfig.apm.xml`.
- 2 In the file `logconfig.apm.xml`, replace the three instances of the string `<DEFINE_THIS_VALUE>` with the path name for the OLAP server at your site. To determine the value for this path, you can check the `logconfig.apm.xml` file in the `[levelroot]/SASApp/OLAPServer` directory.
- 3 After modifying and saving the `logconfig.apm.xml` file, copy the file to the `[levelroot]/SASApp/OLAPServer` directory, replacing the file that is already in that directory.

- 4 Restart the OLAP Server. Use the command `[levelroot]/SASApp/OLAPServer/OLAPServer.sh restart (UNIX) or OLAPServer.bat restart (Windows)`.
- 5 Log on to SAS Management Console and validate the OLAP server to make sure that it has successfully restarted.

Enabling ACM ETL

When you enable the ACM ETL, the ETL processes begin extracting metric data from the SAS Environment Manager agent and loading the data into the SAS Environment Manager Data Mart.

To enable ACM ETL:

- 1 On the machine on which SAS Environment Manager is installed, change to the `[levelroot]/Web/SASEnvironmentManager/emi-framework/bin` directory.
- 2 From a command line, issue the command `./emi_init.sh --enable ACM -i (UNIX) or emi_init.bat --enable ACM -i (Windows)`.
- 3 After the enablement command completes, sign in to SAS Environment Manager. Select **Resources ► Browse ► Servers ► SAS Environment Manager Data Mart 9.4**.
- 4 On the Resource Detail page for the SAS Environment Manager Data Mart 9.4, select the **ACM ETL Processing** service.
- 5 On the Resource Detail page for ACM ETL processing, select **Tools Menu ► Configure Service**. Specify the information in the required fields, and then click **OK**.

Enabling Kits Infrastructure

When you enable the kits infrastructure, processes are created to leverage the capabilities of the SAS Environment Manager framework to monitor the operation of a specific SAS solution or application.

To enable the Kits infrastructure:

- 1 On the machine on which SAS Environment Manager is installed, change to the `[levelroot]/Web/SASEnvironmentManager/emi-framework/bin` directory.
- 2 From a command line, issue the command `./emi_init.sh --enable KITS -i` (UNIX) or `emi_init.bat --enable KITS -i` (Windows).
- 3 After the enablement command completes, sign in to SAS Environment Manager. Select **Resources** ► **Browse** ► **Servers** ► **SAS Environment Manager Data Mart 9.4**.
- 4 On the Resource Detail page for the SAS Environment Manager Data Mart 9.4, select the **Kit ETL Processing** service.
- 5 On the Resource Detail page for kit ETL processing, select **Tools Menu** ► **Configure Service**. Specify the information in the required fields, and then click **OK**.

Using the Report Center

<i>What is the Report Center?</i>	111
<i>Use the Report Center</i>	112
<i>Change Report Parameters</i>	115
<i>Finding the Reports You Need</i>	115
Data Mart Reports	115
Metadata Inventory Reports	116
ACM Reports	116
APM Reports	116
Metadata Audit Reports	117
SAS Environment Manager Service Architecture	
Framework ETL Process Reports	117
Event Reports	118
Solution Kit Reports	118
Log File Job Reports	118
Sample Reports	119

What is the Report Center?

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

to be representative samples of the types of reports that can be produced by the available metric data. You can also create your own reports to meet your individual requirements.

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 that was 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.

Note: The reports in the Report Center are provided as a best efforts resource to assist in the troubleshooting and performance tuning of your SAS deployment. However, many other factors might influence your user experience, some of which are beyond the monitoring capabilities of SAS Environment Manager. For additional assistance in performance tuning and hardware configuration references, please contact the SAS Professional Services Division.

To access the Report Center, select **Analyze ► Report Center**. The Report Center is displayed in 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. When the Report Center window appears, it is titled Stored Processes.

Use the Report Center

When you open the Report Center, you see three main folders:

Products

contains most of the predefined reports that are generated by APM or ACM ETL processes

System

Contains ad hoc reports

user folders

Contains any custom reports that you have created and saved in your user folder

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. The Report Center uses the SAS Stored Process web application, so the window title is Stored Processes.

Stored Processes Log Off SAS Administrator

SAS

- Stored Processes
 - Products
 - SAS Environment Manager
 - Custom
 - Dynamic Reports
 - Datamart
 - ACM Data Mart Platform Resource
 - ACM Data Mart Platform Types and
 - ACM Data Mart Server Resources
 - ACM Data Mart Services Resource
 - Alerts Enabled By Resource
 - Alerts Enabled Listing Rpt
 - All Alert Definitions
 - Data Mart ACM Listing
 - Data Mart Artifact Listing
 - Data Mart Proc Contents Full List**
 - Plugin To Discovered Resource Ma
 - Metadata Inventory
 - Nightly Reports
 - System
 - User Folders

The DATASETS Procedure

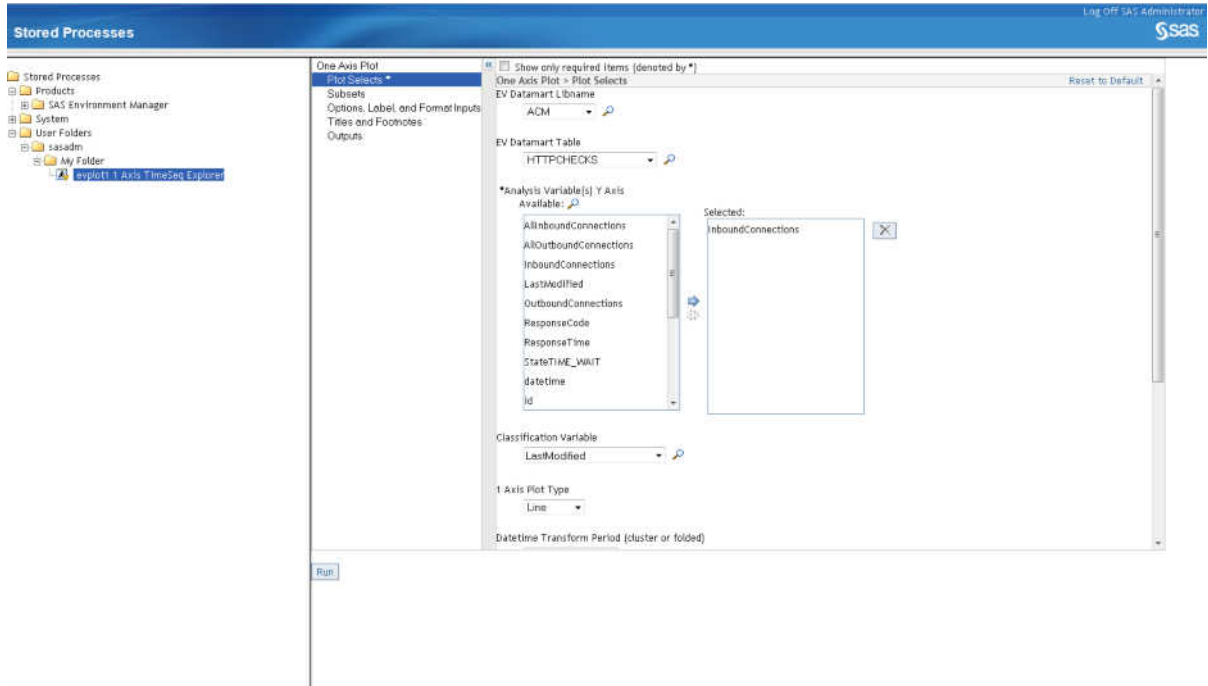
Directory	
Libref	ACM
Engine	BASE
Access	READONLY
Physical Name	/opt/SAS/Config/Lev1/Web/SASEnvironmentManager/emi-framework/Datamart/acm
Filename	/opt/SAS/Config/Lev1/Web/SASEnvironmentManager/emi-framework/Datamart/acm
Inode Number	1322309
Access Permission	rw-rw-r--x
Owner Name	SAS
File Size (bytes)	4096

#	Name	Member Type	File Size	Last Modified
1	AVAILABILITY	DATA	458752	07/22/2014 01:00:38
2	EVENTS	DATA	393216	07/22/2014 12:09:50
3	FILEMOUNTS	DATA	7340032	07/22/2014 01:00:54
4	GROUPINVENTORY	DATA	262144	07/22/2014 01:00:32
5	HOSTPLATFORMS	DATA	2883584	07/22/2014 01:00:53
6	HTTPCHECKS	DATA	1179648	07/22/2014 01:00:55
7	IDMSERVERS	DATA	3407872	07/22/2014 01:00:54
8	MEASUREINVENTORY	DATA	2088960	07/22/2014 01:00:33
	MEASUREINVENTORY	INDEX	163840	07/22/2014 01:00:33
9	METADATASVRS	DATA	1572684	07/22/2014 01:00:54
10	NETWORKINTERFACE	DATA	5898240	07/22/2014 01:00:54
11	RESOURCEINVENTORY	DATA	524288	07/22/2014 01:00:32
12	TCSERVERMORS	DATA	23592960	07/22/2014 01:00:56
13	WEBAPPSERVER	DATA	1310720	07/22/2014 01:00:54
14	WIPDATAB	DATA	3932160	07/22/2014 01:00:55

The DATASETS Procedure

Data Set Name	ACM.AVAILABILITY	Observations	1530
Member Type	DATA	Variables	9
Engine	BASE	Indexes	0
Created	07/22/2014 01:00:39	Observation Length	284
Last Modified	07/22/2014 01:00:39	Deleted Observations	0
Protection		Compressed	CHAR

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, then later run the ETL processes at a different time 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.

You can change the expiration date and time of reports in the report center. See [“Change Report Parameters” on page 115](#).

Change Report Parameters

You can change global settings (such as font, graph style, and legend options) for the reports in the Report Center. To change the report parameters:

- 1 Log on to SAS Management Console.
- 2 On the **Plug-ins** tab, select **Application Management** ► **Configuration Manager**.
- 3 Right-click **EnvMgr Enablement Kit 2.1** and select **Properties**.
- 4 In the EnvMgr Enablement Kit 2.1 Properties dialog box, click the **Settings** tab.
- 5 Use the pages on the **Settings** tab to change the parameters for the Report Center reports. Some of the settings apply to the SAS Environment Manager Data Mart, rather than only to the reports. Any change that you make in the parameters are applied to all of the reports in the Report Center the next time they are run.
- 6 Click **OK** when you have finished making changes.

Finding the Reports You Need

Data Mart Reports

These reports display information about the content of the SAS Environment Manager Data Mart tables, the resources that support the data mart, and the alerts that are defined in the data mart. Some example reports include:

- All Alert Definitions
- ACM Data Mart Server Resources
- Data Mart Proc Contents Full Listing

The reports are located at **Stored Processes ► Products ► SAS Environment Manager ► Dynamic Reports ► Datamart**.

Metadata Inventory Reports

These reports display information about the metadata that is stored on the SAS Metadata Server. Some example reports include:

- Groups Roles and Users
- Metadata Content
- Server Properties

The reports are located at **Stored Processes ► Products ► SAS Environment Manager ► Dynamic Reports ► Metadata Inventory**.

ACM Reports

These reports display and chart detailed metrics for the computing resources in your environment. They are generated by data from ACM ETL processes. Some example reports include:

- File Mounts Summary Report
- Metadata Server Total Clients per Minute
- Platform Workload 1 Min Average

The reports are located at **Stored Processes ► Products ► SAS Environment Manager ► Nightly Reports ► ACM Reports**.

APM Reports

These reports display and chart detailed metrics and information for SAS jobs and processes. They are generated by data from APM ETL processes. Some example reports include:

- Proc Usage

- Server Usage By User
- Workspace Users By Session (Top 10)

The reports are located at **Stored Processes ► Products ► SAS Environment Manager ► Nightly Reports ► APM Reports**.

Metadata Audit Reports

These reports display events recorded in SAS logs. They are generated by data from APM ETL processes. Some example reports include:

- Access Activity Events
- Metadata Client Activity
- Group Changes

The reports are located at **Stored Processes ► Products ► SAS Environment Manager ► Nightly Reports ► Audit Reports (Log Forensics)**.

SAS Environment Manager Service Architecture Framework ETL Process Reports

These reports display information and metrics about the APM ETL processes. Some example reports include:

- Logfile Analysis Overview Summary
- Logfile Summary by Logfile and Jobname
- Proc Usage Summary

The reports are located at **Stored Processes ► Products ► SAS Environment Manager ► Nightly Reports ► EMI SASJob ETL Reports**.

Event Reports

These reports display information and metrics about the events that are generated and recorded in the data mart. They are generated by data from ACM ETL processes. Some example reports include:

- Event Summary Chart
- Event Summary Counts
- Log Event Details

The reports are located at **Stored Processes ► Products ► SAS Environment Manager ► Nightly Reports ► Event and Availability Reports.**

Solution Kit Reports

These reports display information that was stored in the data mart by the solution kit. Each kit contains its own set of stored processes and custom reports.

The reports are located at **Stored Processes ► Products ► SAS Environment Manager ► Nightly Reports ► Kits ► *solution kit name*.**

Log File Job Reports

These reports display information about the jobs and processes used to analyze the SAS logs. They are generated by data from APM ETL processes. Some example reports include:

- Logfile Analysis Overview
- Logfile Summary by Logfile and Jobname
- Proc Usage Summary

The reports are located at **Stored Processes ► Products ► SAS Environment Manager ► Nightly Reports ► SAS - Job Reports.**

Sample Reports

These reports contain samples of different types of report styles for use when developing custom reports. They are generated by data from APM ETL processes. Some example reports include:

- Pie Chart CPU Usage Profile by Platform
- Daily Resource Usage Summary
- Top 5 Ranked on CPU Usage

The reports are located at **Stored Processes ► Products ► SAS Environment Manager ► Nightly Reports ► Sample Gallery**.

Working With Commands

<i>Performing Functions by Using a Command Line</i>	121
Overview	121
Working with Commonly Used Commands	122
Working with Utility Commands	128

Performing Functions by Using a Command Line

Overview

You can issue commands to call SAS Environment Manager script files, which enable you to perform actions such as running the ETLs, installing kits, or enabling new HTTP checks. The files (.sh files for UNIX and .bat files for Windows) are provided in the directory `[levelroot]/Web/SASEnvironmentManager/emi-framework/bin` (UNIX) or `[Levelroot]\Web\SASEnvironmentManager\emi-framework\bin` (Windows). Some commands are for commonly used functions, and others are for utilities or functions that are used infrequently. The following commands are provided:

■ commonly used commands

- `apm_init`
- `emi_init`
- `master_acm_etl`

- master_apm_etl
- master_kits_etl
- validate
- **utility commands**
 - agentClone
 - create_event
 - create_http_checks
 - ev_kit_installer
 - runSASJob

Specify the `-h` option on any command to display the Help.

Working with Commonly Used Commands

Initializing the APM Processes by Using `apm_init`

Use the `apm_init` command to initialize the APM ETL processes. Manual steps are also required after you run this command. See [“Enabling and Initializing the APM ETL” on page 104](#) for complete information about the initialization process.

The syntax of the command is: `apm_init(.sh|.bat) [-fvdh --hostAlias]`

Options are:

- d (--debug)
 - enables debug output
- f (--force)
 - forces configuration to occur, even if a previous version of APM is found or if APM has already been initialized
- h (--help)
 - displays help for the command

`--hostAlias`

specifies the host alias for the machine

`-v (--verbose)`

enables verbose output

Initializing the EMI Framework Using `emi_init`

Use the `emi_init` command to initialize the EMI framework (provided as part of SAS Environment Manager Extended Monitoring), or to enable the ACM ETL, APM ETL, or solution kits ETL. Issue this command as part of the process of initializing and enabling the components of SAS Environment Manager Service Management Architecture. See [Chapter 9, “Initializing and Enabling the Service Management Architecture,”](#) on page 101 for more information about using this command.

The syntax of the command is: `emi_init(.sh|.bat) [-dfhiksv] [(--enable|--disable) <ACM,APM,KITS,ALL>] [--vafeed <ON|OFF>] [--resetDB --resetFlags]`

Options are:

`-d (--debug)`

enables debug output

`-f (--force)`

re-initializes the framework and overwrites settings

`-h (--help)`

displays help for the command

`-i (--initialize)`

initializes the framework

`-k (--loadKits)`

loads solution kits by issuing the command `evKitInstaller -k ALL`

`-s (--status)`

reports the operational status of the EMI framework

`-v (--verbose)`

enables verbose output

- -enable <[APM,ACM,KITS,ALL]>
specifies the components to enable
- -disable <[APM,ACM,KITS,ALL]>
specifies the components to disable
- vafeed <ON|OFF>
enables or disables the nightly feed of SAS Environment Manager Data Mart tables to a drop zone directory, where they are autoloaded into SAS Visual Analytics
- resetDB
resets the SAS Environment Manager Data Mart and purges all data; you cannot recover the data after issuing this command
- resetFlags
resets the flags that identify the components that have been initialized and enabled

Running the APM ETL Processes by Using `master_apm_etl`

The APM ETL processes are specified to run at 1 AM. Use the `master_apm_etl` command if you want to run the processes manually or at another time. The command runs the processes to extract the information from the SAS logs and load it into the SAS Environment Manager Data Mart. You can use a scheduler to issue the command at a specified time to run the ETL processes at a time other than the default. You can also issue the command yourself to run the processes immediately. However, because the SAS logs roll over at midnight, whenever the ETL processes run after midnight, they always use the same data that was collected during the previous 24 hours.

Although you can run the ETL process at any time, the stored process reports expire at midnight. When you display a report, it uses data from the SAS Environment Manager Data Mart, and then the report is cached. When you display the report again, the cached report is displayed. After midnight, the cached report expires and the report is generated again when you select it. Suppose you display a report that uses data from the APM ETL, and then run the `master_apm_etl` command. If you then display the report again, the report will still use the cached data, rather than the data that the ETL process just loaded.

The syntax of the command is: `master_apm_init(.sh|.bat) [-dhv --evdebug <0-3>]`

Options are:

- d (--debug)
enables debug output
- h (--help)
displays help for the command
- v (--verbose)
enables verbose output
- evdebug <0–3>
specifies the debug level for SAS sessions

Running the ACM ETL Processes Using `master_acm_etl`

The ACM ETL processes are specified to run at 12 midnight. Use the `master_acm_etl` command if you want to run the processes manually or at another time. The command runs the processes to extract the ACM data and load it into the SAS Environment Manager Data Mart. You can use a scheduler to issue the command at a specified time to run the ETL processes at a time other than the default. You can also issue the command yourself to run the processes immediately.

Although you can run the ETL process at any time, the stored process reports expire at midnight. When you display a report, it uses data from the SAS Environment Manager Data Mart, and then the report is cached. When you display the report again, the cached report is displayed. After midnight, the cached report expires and the report is generated again when you select it. Suppose you display a report that uses data from the ACM ETL, and then run the `master_acm_etl` command. If you then display the report again, the report will still use the cached data, rather than the data that the ETL process just loaded.

The syntax of the command is: `master_acm_init(.sh|.bat) [-dhv --evdebug <0–3>]`

Options are:

- d (--debug)
enables debug output

- h (--help)
displays help for the command
- v (--verbose)
enables verbose output
- evdebug <0–3>
specifies the debug level for SAS sessions

Running the Solution Kit ETL Processes by Using `master_kits_etl`

The solution kit ETL processes that load data collected by the installed solution kits run at 2 AM. Use the `master_kits_etl` command if you want to run the processes manually or at another time. The command runs the processes to extract the solution kit data and load it into the SAS Environment Manager Data Mart. You can use a scheduler to issue the command at a specified time to run the ETL processes at a time other than the default. You can also issue the command yourself to run the processes immediately.

Although you can run the ETL process at any time, the stored process reports expire at midnight. When you display a report, it uses data from the SAS Environment Manager Data Mart, and then the report is cached. When you display the report again, the cached report is displayed. After midnight, the cached report expires and the report is generated again when you select it. Suppose you display a report that uses data from a solution kit, and then run the `master_kits_etl` command. If you then display the report again, the report will still use the cached data, rather than the data that the ETL process just loaded.

The syntax of the command is: `master_kits_init(.sh|.bat) [-dhvx --evdebug <0–3>]`

Options are:

- d (--debug)
enables debug output
- h (--help)
displays help for the command
- v (--verbose)
enables verbose output

- x (--noexit)
specifies that the Java virtual machine should not exit after the command is completed
- evdebug <0–3>
specifies the debug level for SAS sessions

Validating the SAS Environment Manager Framework by Using **validate**

Use the `validate` command to validate the structure of the SAS Environment Manager framework and to find any errors or changes. This command runs during the initialization process to verify that the framework is correct before anything new is added. The command has four levels:

- 1
verifies that the command-line interface is functioning properly
- 2
validates connections to the SAS execution environment and the SAS Environment Manager server
- 3
verifies that the framework is initialized and functioning properly and that all enabled ETL components are running successfully
- 4
checks all of the files associated with SAS Environment Manager that should not be changed and notes any changes to any of these files

The syntax of the command is: `validate(.sh|.bat) [-qvdh] [-l <1|2|3|4>] [-p| --userPolicy <IGNORE|WARN|ERROR>]`

Options are:

- q (--quiet)
specifies that the command should run in quiet mode
- v (--verbose)
enables verbose output

- d (--debug)
enables debug output
- h (--help)
displays help for the command
- l --level <1|2|3|4>
specifies the level of validation to perform; default value is 1
- p --userPolicy <IGNORE|WARN|ERROR>
specifies the policy if the current user does not match the install user

Working with Utility Commands

Cloning an Agent by Using agentClone

Use the `agentClone` command to create a machine-neutral archive (.tar) file of the SAS Environment Manager agent. You can then copy the file to a server (such as a SAS grid server) that is not part of the standard SAS environment installed by the SAS Deployment Wizard. The agent provides monitoring support for servers in a SAS grid.

The syntax of the command is: `agentClone(.sh|.bat) [-vdh] [-t <Minimal|Select>] [-w <workingDir>] [tarfile]`

Options are:

- v (--verbose)
enables verbose output
- d (--debug)
enables debug output
- h (--help)
displays help for the command
- t (--type) <Minimal|Select>
specifies whether certain plug-ins are included (Select) or omitted (Minimal) to minimize the size of the clone file and the memory required

-w (--workdir) <workingDir>

specifies the directory to use when constructing the .tar file

tarfile

specifies the name of the .tar file that contains the clone of the SAS Environment Manager agent

Creating an Event by Using `create_event`

Use the `create_event` command to manually create a SAS Environment Manager event. After it is created, the event appears in the SAS Environment Manager Event Center.

The syntax of the command is: `createEvent(.sh|.bat) [-vdh] [-f <file>] [-l <INFO|WARN|ERROR>] [-s <source>]`

Options are:

-v (--verbose)

enables verbose output

-d (--debug)

enables debug output

-h (--help)

displays help for the command

-f (--file) <file>

specifies the event file

-l (--level) <INFO|WARN|ERROR>

specifies the level of the event to create (INFO is the default value)

-s (--source)source

specifies the source of the event

Creating an HTTP Check by Using `create_http_checks`

Use the `create_http_checks` command to create an HTTP check service based on the definitions in the file `httpChecks.json`. This file contains all of the predefined HTTP check definitions, but not all of these definitions are created by default. To create one of the definitions:

- 1 After you have initialized the framework (part of SAS Environment Manager Extended Monitoring initialization), edit the file `[levelroot]/Web/SASEnvironmentManager/emi-framework/Conf/httpChecks.json` (UNIX) or `[Levelroot]\Web\SASEnvironmentManager\emi-framework\Conf\httpChecks.json` (Windows).
- 2 Locate the entry for the HTTP check that you want to create. This is an example entry:

```
{
  "name": "HTTP Check for SASTheme_default",
  "desc": "[Auto-Generate] HTTP Monitoring URL: /SASTheme_default",
  "enable": "false",
  "method": "GET",
  "port": "7980",
  "sotimeout": "30",
  "platform": "ptnode19.ptest.sas.com",
  "path": "/SASTheme_default",
  "follow": "true",
  "pattern": "SASTheme_default"
},
```

- 3 Change the value of the enable parameter from `false` to `true`. `"enable": "false",`
- 4 Save the `httpChecks.json` file.
- 5 Run the `create_http_checks` command.

To verify that the service has been created, sign on to SAS Environment Manager and select **Browse ► Services**. The new HTTP check service is listed,

The syntax of the command is: `create_http_checks(.sh|.bat) [-fxvdh] [-t <taskfile>]`

Options are:

`-t (--taskfile) <taskfile>`

specifies that the HTTP checks should not be generated, but should be based on the specified JSON task file

- f (--force)
re-initializes the HTTP checks and overwrites settings
- x (--noexit)
specifies that the Java virtual machine should not exit after the command is completed
- v (--verbose)
enables verbose output
- d (--debug)
enables debug output
- h (--help)
displays help for the command

Installing a Solution Kit by Using `ev_kit_installer`

Solution kits provide customized metrics and reports to support specific SAS solutions and applications. Use the `ev_kit_installer` command to install new solution kits.

The syntax of the command is: `ev_kit_installer(.sh|.bat) [-fvdh] [-k <kitname|ALL>]`

Options are:

- f (--force)
replaces the existing kit configurations
- v (--verbose)
enables verbose output
- d (--debug)
enables debug output
- h (--help)
displays help for the command
- k (--kitName) <kitname|ALL>
specifies the name of the kit to install, or that all kits should be installed

Accessing SAS Environment Manager with a SAS Job by Using runSASJob

Use the `runSASJob` command to run a SAS program with the SAS autoexec and environment necessary for the program to access the SAS Environment Manager Data Mart and the EMI framework.

CAUTION! Do not run this command unless directed to by SAS Technical Support. Running this command incorrectly could corrupt the SAS Environment Manager Data Mart and cause loss of data.

The syntax of the command is: `runSASJob(.sh|.bat) [-bdhv] [--args <args>] [--autocall <autocall_dir>] [--autoexec <(BATCH|APM|KITS|STP) | <autoexec_file>] [--config <config_file>] [--evdebug <0-3>] [--log <log_results_file>] [--nodms] [--printfile <output_file>] [--work <saswork_dir>] [--workdir <working_dir>]`

Options are:

`-b (--batch)`

specifies that the SAS program runs in batch mode (with the SAS options `-batch -noterminal`)

`-d (--debug)`

enables debug output

`-h (--help)`

displays help for the command

`-v (--verbose)`

enables verbose output

`--args <args>`

specifies any SAS command line arguments to be appended to the SAS invocation command

`--autocall <autocall_dir>`

specifies the autocall directory to use

- `--autoexec <(BATCH|APM|KITS|STP) | <autoexec_file>`
specifies whether to use a defined autoexec file (such as BATCH or APM) or a specified autoexec file
- `--config <config_file>`
specifies a custom configuration file to use
- `--evdebug <0–3>`
specifies the debug level for the SAS session
- `--log <log_results_file>`
specifies the file to contain the log results
- `--nodms`
specifies that SAS should run in line mode with the framework enabled
- `--printfile <output_file>`
specifies the output file for SAS procedures
- `--work <saswork_dir>`
specifies the SAS Work directory
- `--workdir <working_dir>`
specifies the relative working directory (or parent path) used when running a SAS program



Part 3

SAS Metadata Administration

Chapter 12

***Managing User Access* 137**

Chapter 13

***Managing Metadata Access* 157**

Managing User Access

<i>Features in User Administration</i>	138
<i>Introduction to User Administration</i>	139
About User Administration	139
About Users	140
About SAS Administrators	140
About Groups	141
About Roles and Capabilities	141
About Members	142
About Logins	143
About Internal Accounts	145
About Authentication Domains	146
About Passwords	147
Requirement: Unique Names and IDs	148
<i>Access User Management</i>	149
<i>Add a User</i>	150
<i>Add an Administrator</i>	152
<i>Add a Custom Group</i>	152
<i>Add a Custom Role</i>	153
<i>Assign Members to a Group or Role</i>	153
<i>Update the Stored Password in a Login</i>	154
<i>Delete an Identity</i>	154

<i>Store DBMS Credentials</i>	155
Store Shared Credentials	155
Store Individual Credentials	155
<i>Adjust Policies for an Internal Account</i>	156

Features in User Administration

This chapter addresses user administration in the metadata layer, which is provided by the SAS Metadata Server.

The SAS Environment Manager Users module supports some of the user administration tasks that are provided by the User Manager plug-in to SAS Management Console, including the following:

- creation and maintenance of users, groups, and roles
- management of group and role memberships
- management of logins and internal accounts

In addition, this application provides enhanced user administration features. For example, when memberships are displayed, all memberships are shown, including indirect and implicit relationships.

Note: This application provides improved access to information. It does not introduce any changes to the underlying security model.

Many of the general features of SAS Environment Manager are useful in user administration. For example, you can open multiple objects. Each object is displayed in its own tab.

Note: Changes that you make to one object are not reflected in other open objects until those changes are saved.

Introduction to User Administration

About User Administration

SAS Environment Manager provides some of the capabilities that are available in SAS Management Console. SAS Environment Manager is not currently a replacement for SAS Management Console, and no functionality has been removed from SAS Management Console.

In order to make access distinctions and to track user activity, each requesting user must be identified. The main purpose of user administration is to provide information that facilitates the identification of users. In general, SAS stores one external account ID for each user. SAS uses its copy of these IDs to establish a unique identity for each connecting user. All of a user's metadata-layer group memberships, role memberships, and permission assignments are ultimately tied to that user's SAS identity.

Note: For identification purposes, only the account IDs are needed. SAS does not store external passwords for identification purposes.

As an alternative to creating a login for a user or administrator, you can give the new user or administrator an internal account. Enable the **Internal Account** option on the user's **Accounts** page. An account is enabled when the **Internal Account** option settings are displayed. Before you add an internal account, see [“Limitations of Internal Accounts” on page 145](#).

TIP As an alternative to interactively creating and maintaining identity information, you can write a program that performs these tasks as batch processes. See the user import macros documentation in *SAS Intelligence Platform: Security Administration Guide*.

TIP You can use the metadata promotion tools to import and export identity information. See *SAS Intelligence Platform: System Administration Guide*.

About Users

A user is an individual person or service identity.

You should create an individual SAS identity for each person who uses the SAS environment. You can then make access distinctions in the metadata layer and establish a personal folder for each user.

Note: If generic access is sufficient for some of your users, those users can instead share the generic PUBLIC group identity. Not all applications accept PUBLIC-only users.

An individual SAS identity is established by coordination between two sets of identity information:

- in an external system, a user account
- in the metadata, a user definition that includes a copy of the external account ID

To give someone an individual SAS identity, you create a metadata user definition that includes a copy of their external account ID. For example, in the simplest configuration, each user has an account that is known to the metadata server's host.

- If the metadata server is running in Windows, users typically have Active Directory accounts.
- If the metadata server is running in UNIX, users might have UNIX accounts. Sometimes a UNIX host is configured to recognize LDAP, Active Directory, or other types of accounts.

Note: For metadata administrators and some service identities, you can use a SAS internal account instead of an external account.

About SAS Administrators

When creating SAS administrators, consider the following:

- If you want to make someone an unrestricted administrator, assign them to the Metadata Server: Unrestricted role.

- Administrators should not also serve as regular users. If you want someone to be an administrator only some of the time, create two user definitions for that person.
 - One definition is based on an external account and is not a member of SAS Administrators.
 - The other definition is based on an internal account and is a member of SAS Administrators.

A dual user logs on with an internal account in order to use administrative privileges and with an external account the rest of the time.

About Groups

A group is a set of users.

Creating groups enables you to simplify security management in the following ways:

- It is more efficient to assign permissions to groups than to individual users.
- If you need to store passwords in the metadata, you can reduce the amount of required maintenance by using a group to make one shared account available to multiple users.
- It is sometimes more efficient to manage role membership by assigning groups to roles instead of assigning users directly to roles.
- If you need to manage permissions for distinct classes of access, you can create custom groups. For example, you might create a group for each business unit or functional area of responsibility.

TIP A group's membership can include other groups as well as individual users, allowing you to create a nested group structure.

About Roles and Capabilities

A role manages the availability of application features such as menu items.

An application feature that is under role-based management is called a capability. Anyone who is a member of a role has all of that role's capabilities. Roles and capabilities have the following characteristics:

- Roles determine which user interface elements (such as menu items or modules) you see when you use an application. In general, roles do not protect data or metadata.
- Having a certain capability is not an alternative to meeting permission requirements. Permission requirements and capability requirements are cumulative.
- Roles and groups serve distinct purposes. You cannot assign permissions to a role or capabilities to a group.
- Capabilities are additive. Assigning someone to a role never reduces what that person can do.
- If necessary, you can adjust the distribution of capabilities by changing role memberships or by customizing the mapping of roles-to-capabilities.
- If you need to decrease the level of granularity, you can create a new role that aggregates two or more existing roles. For example, you might create a role that includes all capabilities other than those of the most privileged roles.
- If you need to increase the level of granularity, you can create a new role that provides only a subset of the capabilities of a predefined role.
- If you need to create a cross-application role for a particular type of functionality, you can create custom roles. For example, you might create an OLAP role that includes the OLAP capabilities from SAS Enterprise Guide and the SAS Add-In for Microsoft Office.

For information about the predefined administrative roles, see *SAS Intelligence Platform: System Administration Guide*.

About Members

A member is a user or group that is assigned to a group or role.

When adding members to a group or role, consider the following:

- You cannot use the SAS Environment Manager user interface to make a role a member of a group or of another role. You can instead make one role contribute all of its capabilities to another role.
- On a group definition, do not confuse the **Members** tab with the **Member of** tab. Use a group's **Member of** tab only if you want to make that group a member of other groups or roles.
- To reduce complexity, do not make the implicit groups (SASUSERS and PUBLIC) members of other groups. These groups can be members of certain roles.

About Logins

What is a Login?

A login is a SAS copy of information about an external account. Every login must include a user ID. In a login for a Windows account, the ID must be qualified (for example, *userID@company.com*, *domain\userID*, or *machine\userID*).

TIP The requirement to provide a qualified ID for a Windows account applies to the SAS copy of the ID. It is usually not necessary to qualify the user ID that you provide when you log on to a SAS application.

TIP If you do provide a qualified ID when you log on, you must use the same format that was used in your login. For example, Windows environments might accept both *WIN\me* and *Me.MyLastName@mycompany.com*, but SAS can understand only one of these qualified forms (the form in which the SAS copy of the ID is stored).

Logins for Users

Each user should have a login that establishes their SAS identity. You do not need to include a password in this login. The password column displays eight asterisks if a password is stored. For example, this is how Joe's login might look when a user administrator views Joe's **Accounts** settings:

Domain	Stored User ID	Stored Password (Optional)
--------	----------------	----------------------------

DefaultAuth	WIN\Joe
-------------	---------

A user might have additional logins that provide access to other systems. For example, if Joe has his own Oracle account, he might have these two logins:

Domain	Stored User ID	Stored Password (Optional)
DefaultAuth	WIN\Joe	
OracleAuth	ORAJoe	*****

Note: The Oracle login should include a copy of Joe's Oracle password.

If a site uses web authentication, the requirements are different. For example, if Joe uses both web and desktop applications at such a site, Joe might have these three logins:

Domain	Stored User ID	Stored Password (Optional)
DefaultAuth	WIN\Joe	
OracleAuth	ORAJoe	*****
web	WEB\joe	

Note: Like his DefaultAuth login, Joe's web login is used only to launch clients, so there is no need to create a SAS copy of Joe's web realm password.

Logins for Groups

Logins are not required for groups. The main reason to assign a login to a group is to make a shared account available to multiple users. A group login contains a SAS copy of the user ID and password for a shared account. For example, to provide shared access to DB2, a group might have a login that looks like this:

Domain	Stored User ID	Stored Password (Optional)
DB2Auth	sharedDB2id	*****

All members of the group can see and use this login. Because this login is for a third-party database, a copy of the DBMS account password should be stored in this login.

About Internal Accounts

What is an Internal Account?

An internal account is a SAS account that the metadata server authenticates independently, without relying on an external authentication provider such as the operating system. Use internal accounts only for administrators and some service identities. For these purposes, an internal account is an acceptable substitute for an external account with a corresponding login. For example, the SAS Administrator and the SAS Trusted User can be based on internal accounts.

Benefits of Internal Accounts

Internal accounts have these advantages:

- Internal accounts provide an alternative to creating external accounts for SAS internal purposes such as inter-process communication.
- Internal accounts can be maintenance free. You do not have to synchronize internal accounts with another user registry.
- Internal accounts are usable only in the SAS realm, so they reduce exposure to the rest of your security environment.

Limitations of Internal Accounts

Although you can add an internal account to any user definition, internal accounts are not intended for regular users. Someone who has only an internal account cannot perform the following tasks:

- seamlessly launch a standard workspace server that runs under their own individual identity
- participate in Integrated Windows authentication or web authentication
- add, delete, initialize, or unregister a foundation repository

Policies for Internal Accounts

By initial policy, these server-level settings are in effect:

- Accounts do not expire and are not suspended due to inactivity.
- Passwords must be at least six characters in length, do not have to include mixed case or numbers, and do not expire.
- The five most recent passwords for an account cannot be reused for that account.
- There is no mandatory time delay between password changes.
- For an account that has a password expiration period, there is a forced password change on first use and after the password is reset by someone other than the account owner. By initial policy, passwords do not expire, so there are no forced password changes.

These default policies are set in the metadata server's `omaconfig.xml` file. For more information, see *SAS Intelligence Platform: Security Administration Guide*.

About Authentication Domains

What is an Authentication Domain?

An authentication domain is a name that facilitates the matching of logins with the servers for which they are valid.

Note: This matching is not important when you launch a client, but it is important when you access certain secondary servers such as a third-party DBMS or, in some configurations, a standard workspace server.

Each user ID and password is valid within a specific scope. For example, the user ID and password that you use to log on to your computer at work are probably not the same as the user ID and password that you use at home. It is also common for database servers and web servers to have their own authentication mechanisms, which require yet another, different, user ID and password.

An enterprise application that provides access to many different resources might require that a user have several sets of credentials. Each time a user requests access to a resource, the software must determine which credentials to use to provide access. The

software could challenge the user with an interactive prompt for user ID and password, but that quickly becomes an annoyance that interrupts the user experience. The software could randomly try different credentials until it finds a set that works, but authentication attempts can be expensive in terms of performance. In SAS Intelligence Platform, the software attempts to use only the credentials that it expects to be valid for a particular resource or system.

The software's knowledge of which credentials are likely to be valid is based entirely on authentication domain assignments. For this reason, you must correctly assign an authentication domain to each set of resources that uses a particular authentication provider. You must also assign that same authentication domain to any stored credentials that are valid for that provider.

When Do I Need to Add an Authentication Domain?

In the simplest case, all logins and SAS servers are associated with one authentication domain (DefaultAuth). This list describes the most common reasons for using more authentication domains:

- If you use web authentication, you might need a second authentication domain for the logins that contain web-realm user IDs.
- If you have a third-party server (such as a DBMS server) that has its own user registry, you need a separate authentication domain for that server and its logins.
- If both of the following criteria are met, you need a separate authentication domain for the standard workspace server and its logins:
 - The standard workspace server does not share an authentication provider with the metadata server (and cannot be configured to do so).
 - You want to provide seamless individualized access to the standard workspace server.

About Passwords

Managed Passwords

Passwords for a few required accounts (such as the SAS Administrator and the SAS Trusted User) are included in configuration files. If these passwords change, you must

also use SAS Deployment Manager to update the configuration. For instructions, see *SAS Intelligence Platform: Security Administration Guide*.

Passwords in Logins

It is usually not necessary to store an external password in the SAS metadata. The main reason to include a password in a login is to provide seamless access to a server that requires credentials that are different from the credentials that users initially submit. The most common example is a deployment that includes a third-party DBMS server that requires a different set of credentials.

Password management for logins is driven by changes that occur in other systems. For example, if you have a personal login for a third-party DBMS, and you change your DBMS password, you must also update the SAS copy of that password.

If credentials are not otherwise available, some applications prompt users for an appropriate user ID and password.

Passwords in Internal Accounts

Internal accounts exist only in the metadata. Each internal account includes a password. By initial policy, internal passwords do not expire.

Passwords in Configuration Files

Passwords for a few required accounts (such as the SAS Administrator and the SAS Trusted User) are included in configuration files. If you need to change these passwords, use SAS Deployment Manager. For instructions, see *SAS Intelligence Platform: Security Administration Guide*.

Requirement: Unique Names and IDs

Within a metadata server, the following uniqueness requirements apply:

- You cannot create a user definition that has the same name as an existing user definition.
- You cannot create a group or role definition that has the same name as an existing group or role definition.

- You cannot assign the same user ID to different users or groups. All of the logins that include a particular user ID must be owned by the same identity. In this situation, the metadata server resolves each user ID to a single identity.

Note: The exception to this requirement is logins that are associated with outbound authentication domains. These logins are not subject to these constraints.

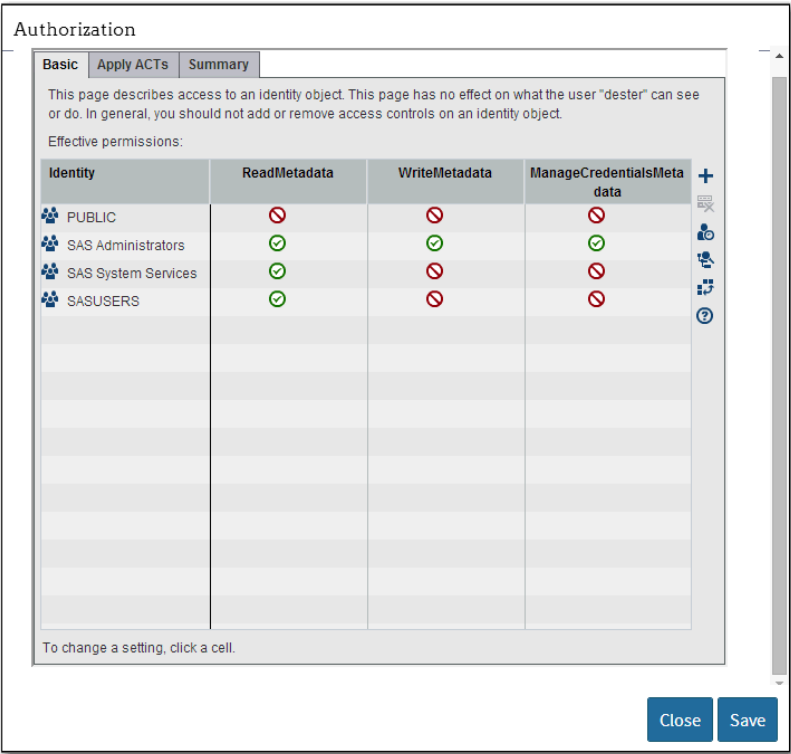
- This requirement is case insensitive. For example, you cannot assign a login with a user ID of `smith` to one user and a login with a user ID of `SMITH` to another user.
- This requirement applies to the qualified form of the user ID. For example, you can assign a login with a user ID of `winDEV\brown` to one user and a login with a user ID of `winPROD\brown` to another user.
- If you give a user two logins that contain the same user ID, the logins must be in different authentication domains. Within an authentication domain, each user ID must be unique. For example, if you give Tara O'Toole two logins that both have a user ID of `tara`, then you cannot associate both of those logins with the OraAuth authentication domain. As with the previous requirement, this requirement is case insensitive and is applied to the fully qualified form of the user ID.

TIP Avoid using spaces or special characters in the name of a user, group, or role that you create. Not all components support spaces and special characters in identity names.



Access User Management

- 1 Click the **Administration** tab.
- 2 Click the **Users** module.
- 3 Right-click on an object in the **Users** pane, and select **Open**. The tab corresponding to the object that you selected is displayed.

- 4 Click the **Authorization** tab, and then click **Open Authorization Information**. A window similar to the following appears:



Add a User

- 1 On the toolbar, click  and select **New User**.
- 2 In the New User window, enter a name and optional display name. Then, click **Save**. The new user object opens in a tab.
- 3 On the **General** tab, click **Accounts**. In the **Logins** table, click  to add a login.
 - In the Domain column, select **DefaultAuth**.

- In the Stored User ID column, enter the user's external account ID. You can use any account (LDAP, Active Directory, host, or other) that is known to the metadata server's host.

Note: For a Windows account, qualify the ID (for example, *WIN\myID* or *myID@mycompany.com*).

If your site uses web authentication, refer to the following table for adapted instructions:

Table 12.1 Adapted Instructions for Sites That Use Web Authentication

Type of User	Adapted Instructions*
Someone who uses only web applications	Select the web realm authentication domain (such as web) instead of DefaultAuth , and enter the user's web realm ID.
Someone who uses both web and desktop applications	Complete the standard instructions and also add a web realm login.

* If the web user IDs and the metadata server user IDs are identical, and the web applications do not use a standard workspace server, you do not need to follow these adapted instructions.

- 4 (Optional) On the **Member of** tab, click  to make a user a direct member of one or more groups and roles.


Note: The user automatically belongs to PUBLIC (everyone who can access the metadata server) and SASUSERS (those members of PUBLIC who have a well-formed user definition).

- 5 (Optional) To provide seamless access to a third-party server such as a DBMS, either give the user a second login or make the user a member of a group that has a shared login for the third-party server.
- 6 Save the new user.


Note: Do not use the settings in the Authorization window to modify authorizations for a user. The settings in this window have no effect on what the user can do. They affect the permissions for the user object itself.


Note: If the user accesses a standard workspace server with Windows host credentials, make sure the user has the "Log on as a batch job" Windows privilege on that host. The user's Windows account should be a member of a Windows group that is named SAS Server Users or something similar.

Add an Administrator

To add an administrator, follow the instructions for adding a user. On the **Member of** tab, click . In the Direct Memberships window, move the SAS Administrators group to the **Direct member of** list box. The new user becomes a member of the SAS Administrators group.

Add a Custom Group

- 1 On the toolbar, click  and select **New Group**.
- 2 In the New Group window, enter a name. A display name and repository are optional. Then, click **Save**. The new group object opens in a tab.

Note: In general, groups are in the foundation repository. If you have custom repositories, you can create groups in those repositories too.
- 3 On the **Members** tab, click  to directly assign members to the new group.
- 4 If you want to make the new group a member of other groups or roles, use the **Member of** tab.


Note: The ability to nest group dependencies is limited. Suppose you make a group a member of another group. As soon as a branch in the tree returns to an item that is previously listed at any point in the branch, SAS Environment Manager stops the nested dependencies in order to avoid an infinite loop. For example, suppose you have three groups named Group1, Group2, and Group3. If Group1 is a member of

Group2 and Group2 is a member of Group3, then you cannot make Group3 a member of both Group1 and Group2.


- 5 If you are using this group to make a shared account available, add a shared login by clicking the **General** tab and then clicking **Accounts**. See [“Logins for Groups” on page 144](#).
- 6 Save the new group.

Note: Do not use the settings in the Authorization window to modify authorizations for a user. The settings in this window have no effect on what the user can do.

Add a Custom Role

- 1 On the toolbar, click  and select **New Role**.
- 2 In the New Role window, enter a name. A display name and repository are optional. Then, click **Save**. The new role object opens in a tab.

Note: In general, roles are in the foundation repository. If you have custom repositories, you can create roles in those repositories too.

- 3 On the **Members** tab, click  to directly assign members to the new role.
- 4 Save the new role.

Note: Do not use the settings in the Authorization window to modify authorizations for a user. The settings in this window have no effect on what the user can do.

Assign Members to a Group or Role

- 1 Open the group or role that you want to update.

- 2 On the **Members** tab, click  to directly assign members.
- 3 Save the group or role.

Update the Stored Password in a Login

- 1 Open the user or group whose external password has changed.
- 2 On the **General** tab, click **Accounts**. In the **Logins** table, click the cell that you need to update.

Note: Logins are visible only if you have user administration capabilities, you are looking at your own user definition, or you are looking at the definition for a group that you belong to.

- 3 In the Store Password (Optional) window, enter and confirm the new password.
- 4 Save the user or group.

Delete an Identity

CAUTION! When you delete a user, group, or role, you lose all of that identity's metadata associations. Creating a new identity with the same name does not restore the associations.

- 1 In the navigation pane, locate the identity that you want to delete.
- 2 Right-click the identity and select **Delete**.
- 3 In the confirmation message box, click **Yes**.

Store DBMS Credentials

Store Shared Credentials

Note: These instructions apply to third-party servers that do not accept the credentials with which users initially log on to SAS clients. These instructions are also appropriate for providing seamless access to other servers that require credentials that are different from the credentials with which users initially log on to SAS clients.

- 1 Open (or create) the group that you will use to manage the shared DBMS account. For example, if you want all users to share the account, use the PUBLIC group.
- 2 On the **General** tab, click **Accounts**. Next to the **Logins** table, click **+** to add a login.
 - In the Domain column, select the authentication domain for the DBMS.

Note: In the DBMS server metadata, the authentication domain is specified on the connection object.
 - In the Stored User ID column, enter the DBMS user ID.
 - In the Stored Password (Optional) column, store the DBMS password.
- 3 On the **Members** tab, make sure that everyone who needs to use the shared account is a member.
- 4 Save the group.

Store Individual Credentials

Follow the instructions in the preceding topic, but add the login to a user definition instead of a group definition.

Note: If a user has more than one available login in a particular authentication domain, the login that is closest to the user is used. If there is tie, you might not be able to predict which will be used. One example of a tie is when a user is a direct member of two groups and both groups have logins in the same authentication domain.

Adjust Policies for an Internal Account

- 1 Open the user whose internal account policies you want to change.
- 2 On the **General** tab, click **Accounts**. Enable the **Internal Account** option.
- 3 Make changes to one or more of the properties on the tab.
- 4 Save your changes.

Note: The properties are displayed only when an administrator accesses the **General** tab and clicks **Accounts** for a user who has an internal account.

Managing Metadata Access

<i>Features in Access Management</i>	158
<i>Concepts in Access Management</i>	160
About Access Management	160
About ACTs	161
Granularity and Mechanics	161
Inheritance and Precedence	163
Use and Enforcement of Each Permission	164
Permission Conditions	166
<i>Icons in Access Management</i>	167
How are Denials, Grants, and Conditional Grants Indicated? ..	167
How are Direct Controls Indicated?	168
What Does a Blank Cell in an ACT Pattern Mean?	169
<i>Permissions Inspector</i>	170
<i>Permission Origins</i>	171
Introduction to Permission Origins	171
Simple Permission Origins	171
Inherited Permission Origins	173
<i>Access Control Inheritance</i>	175
About the Explore Inheritance Diagram	175
Examples of Explore Inheritance Diagrams	175
Tips for Exploring Inheritance	177
<i>Permission Condition</i>	178

Best Practices for Permissions	180
Assign Access Controls to Groups	180
Use Folders to Organize Content	180
Centralize Permissions with Access Control Templates	181
Deny Broadly, Grant Selectively (To the Extent Possible)	181
Manage Metadata Information	182
Apply an ACT	183
Create an ACT	183
Update an ACT	184
Add an Explicit Grant or Denial	186
Add a Row-Level Permission Condition	187
Provide Fine-Grained Access Using Permission Conditions ..	187

Features in Access Management

Access management is in the metadata authorization layer, which is provided by SAS Environment Manager.

This application supports the access control tasks that are provided by the Authorization module to SAS Environment Manager, including the following:

- applying access control templates (ACTs) to metadata objects
- applying explicit controls to objects
- managing repository-level controls
- maintaining ACTs

In addition, this application provides new access management features, including the following:

- The basic authorization display provides a full grid of applicable permissions and access control participants. This enables you to immediately see the entire picture, instead of having to examine the settings for only one identity at a time. You can immediately see the impact of your access control changes across identities. For example, the impact that an explicit denial for PUBLIC has on all restricted identities that do not have offsetting direct controls is immediately apparent.
- For each effective permission, you can view origins information that identifies the source of the effective grant or denial.
- The permissions inspector, enables you to easily and safely look up effective permissions for any user or group.
- In each ACT's definition, a usage tab lists the objects to which that ACT is directly applied. This helps you identify any gaps in your access control implementation, and helps you anticipate the impact of any changes that you make to the ACT.
- The Explore Inheritance diagram enables you to identify all of an object's access control parents. The diagram has an effective permissions overlay that helps you determine, for a specified identity and permission, where within the inheritance path access is gained or lost.
- In each object's authorization properties, a summary tab provides a simple list of any direct controls (explicit controls and directly applied ACTs) that have been set on the object. You can rearrange the list to group settings by identity, permission, or type (explicit versus ACT).

Note: This application provides improved access to information. It does not introduce any changes to the underlying security model.

Concepts in Access Management

About Access Management

You can use SAS Environment Manager to manage access in the metadata authorization layer. The access control tasks that are provided by SAS Environment Manager include:

- application of access control templates (ACTs) to objects
- maintenance of ACTs
- application of explicit controls to objects
- management of repository-level controls

Over the lifecycle of SAS 9.4, functions will be added to extend SAS Environment Manager's capabilities as a centralized administration application for all SAS products. SAS Environment Manager is not currently a replacement for SAS Management Console, and no functionality has been removed from SAS Management Console.

The following topics provide a brief overview of the metadata authorization model. For a comprehensive discussion, see the *SAS Intelligence Platform: Security Administration Guide*.

Access management determines which objects a user can see and interact with. Permissions that you set on the **Authorization** tabs are part of a metadata-based access control system within the SAS Metadata Server.

The SAS metadata authorization layer supplements protections in other layers (such as the operating system, a third-party DBMS, or the SAS Content Server). Protections are cumulative across layers. You cannot perform a task unless you have sufficient access in all layers.

CAUTION! Do not rely exclusively on the metadata authorization layer to protect data. You must manage physical access (operating system and DBMS permissions) in addition to metadata layer access.

About ACTs

Why Use ACTs?

Use ACTs to avoid having to repeatedly add the same explicit controls for the same identities on multiple objects. When you apply an ACT to an object, the pattern settings in an ACT are added to the direct controls of an object.

TIP Settings in the pattern of an ACT affect access to all of the objects to which the ACT is applied. Settings on the **Authorization** tab for an ACT affect who can access that ACT.

Why Create Custom ACTs?

Several predefined ACTs are provided. To further centralize access management, create an ACT for each access pattern that you use repeatedly. Here are some common patterns and tips:

- It is often useful to create ACTs to manage Read access for different business units.
- It is often useful to create an ACT that manages Write access for a functional group that includes users from multiple business units.
- You do not have to capture all of an object's protections in one ACT. You can use combinations of ACTs, explicit controls, and inherited settings to define access to an object.

Granularity and Mechanics

Repository-Level Controls

Repository-level controls function as a gateway. Participating users need ReadMetadata and WriteMetadata permissions for the foundation repository.

Repository-level controls also serve as a parent of last resort, defining access to any objects that do not have more specific settings. Repository-level controls are displayed on the **Pattern** tabs of the repository access control template (Default ACT).

Why Adjust the Repository-Level Controls?

CAUTION! Altering the repository-level controls for service identities can prevent necessary access. We recommend that you do not change these settings.

Here are some key points about working with repository-level controls for a foundation repository:

- If you want some or all users to have default Read access to all data, grant the Read permission at the repository level.
- If you want to experiment with changing repository-level access, we recommend that you create a new ACT and designate that ACT as the repository ACT (instead of modifying the original repository ACT).
- All users need ReadMetadata and WriteMetadata access to the foundation repository. It is appropriate for the SASUSERS group to be granted these permissions in the pattern of the repository ACT.

Which ACT is the Repository ACT?

If your site has multiple metadata repositories, you have multiple repository ACTs. Each repository has its own repository ACT, which is usually named Default ACT.

As an alternative to opening each ACT to determine which repository it belongs to, navigate to the ACT from within the **Folders** view.

- ACTs for the foundation repository are located in the **SAS Folders ► System ► Security ► Access Control Templates** folder.
- ACTs for a custom repository are located in the **SAS Folders ► custom-repository ► System ► Security ► Access Control Templates** folder.

Note: The repository ACT indicator is located at the bottom of the **Usage** tab for *access-control-template*.

Object-Level Controls

Object-level controls manage access to a specific object such as a report, an information map, a stored process, a table, a cube, or a folder. You can define object-level controls individually (as explicit controls) and in patterns (as directly applied access control templates).

Fine-Grained Controls

Fine-grained controls affect access to subsets of data within an object. To establish fine-grained controls, you define permission conditions that constrain access to rows within a table or members within an OLAP dimension.

Feature-Level Controls

Some applications use roles to limit access to functionality. These applications check the roles of each user in order to determine which menu items and features to display for that user. Roles management is part of user administration.

Inheritance and Precedence

Two Relationship Networks

Permissions are conveyed across two distinct relationship networks—a resource network and an identity network. Permissions that are set directly on an object always have priority over permissions that are set on the parent of an object. For example, when access to a report is evaluated, a denial that is set on the report (and explicitly assigned to the PUBLIC group) overrides a grant that is set on the parent folder of the report (even if the grant is explicitly assigned to you).

The Resource Relationships Network

Permissions that you set on one object can affect access to many other objects. For example, a report inherits permissions from the folder in which the report is located. This relationship network consists primarily of the SAS Folders tree. This list highlights some exceptions:

- The root folder is not the ultimate parent. This folder inherits from the repository (through the permission pattern of the repository access control template (ACT)).
- The root folder is not a universal parent. Some system resources (such as application servers, identities, and ACTs) have the repository as their immediate and only parent.
- Inheritance within a table or cube follows the data structure. For example, table columns and cube hierarchies do not have a folder as their immediate parent.

Instead, a column inherits from its parent table and a hierarchy inherits from its parent cube.

- In unusual circumstances, it is possible for an object to have more than one immediate parent. If there is a tie in this network (for example, if there are no settings on an object, the object has two immediate parents, and one parent provides a grant while the other parent provides a denial), the outcome is a grant. If there are no direct controls, a grant from any inheritance path is sufficient to provide access.
- In general, specialized folders (such as search folders, favorites folders, and virtual folders) do not convey permissions to the objects that they contain. An exception is that a favorites folder does convey permissions to any child favorites folders (favorites groups) that it contains.

The Identity Relationships Network

Permissions that you assign to one group can affect access for many other identities. For example, if you grant a group access to an OLAP cube, that grant applies to all users who are members of the group. This relationship network is governed by a precedence order that starts with a primary identity, can incorporate multiple levels of group memberships, and ends with implicit memberships in SASUSERS and then PUBLIC. If there is a tie in this network (for example, if you directly assign a user to two groups and give one group an explicit grant and another group an explicit denial), the outcome is a denial.

Use and Enforcement of Each Permission

Table 13.1 Permission Reference

Permission (Abbreviation)	Actions Affected and Limitations on Enforcement
ReadMetadata (RM)	View an object. For example, to see an information map, you need RM for that information map. To see (or traverse) a folder, you need RM for that folder.

Permission (Abbreviation)	Actions Affected and Limitations on Enforcement
WriteMetadata (WM)	Edit, delete, change permissions for, or rename an object. For example, to edit a report, you need WM for the report. To delete a report, you need WM for the report (and WMM for the parent folder of the report). WM can also affect the ability to create associations. For example, you need WM on an application server in order to associate a library to that server. WM affects the ability to create objects in certain containers. For example, to add an object anywhere in a repository, you need WM at the repository level. For folders, adding and deleting child objects is controlled by WMM, not WM.
WriteMemberMetadata (WMM)	Add an object to a folder or delete an object from a folder. For example, to save a report to a folder, you need WMM for the folder. To remove a report from a folder, you need WMM for the folder (and WM for the report). To enable someone to interact with the contents of a folder, but with not the folder itself, grant WMM and deny WM.*
CheckInMetadata (CM)	Check in and check out objects in a change-managed area. Change management is an optional feature that is supported by only SAS Data Integration Studio.**
Administer (A)	Monitor, stop, pause, resume, refresh, or quiesce a server or spawner. For the metadata server, the ability to perform tasks other than monitoring is managed by the Metadata Server: Operation role (not by this permission).
Read (R)	Read data. For example, you need RM for a cube in order to see the cube, and you need R for the cube in order to run a query against it. Enforced for OLAP data, information maps, data that is accessed through the metadata LIBNAME engine, and dashboard objects.
Create (C)	Add data. For example, on a table, C controls adding rows to the table. Enforced for data that is accessed through the metadata LIBNAME engine.

Permission (Abbreviation)	Actions Affected and Limitations on Enforcement
Write (W)	Update data. For example, on a table, W controls updating the rows in the table. Enforced for data that is accessed through the metadata LIBNAME engine, for publishing channels, and for dashboard objects.
Delete (D)	Delete data. For example, D on a library controls the deletion of tables from the library. Enforced for data that is accessed through the metadata LIBNAME engine and for dashboard objects.
ManageMemberMetadata (MMM)	Change the membership of the Group and Role. Cannot change security or other account attributes
ManageCredentialsMetadata (MCM)	Manage accounts and trusted logins of User and Group. Cannot change security or other account attributes.

- * A folder's WMM settings mirror its WM settings unless the folder has a direct control for WMM. A grant (or deny) of WMM on a folder becomes an inherited grant (or deny) of WM on the objects and subfolders within that folder. WMM is not inherited from one folder to another. WMM is not applicable to specialized folders (such as virtual folders, favorites folders, or search folders).
- ** In any change-managed areas of a foundation repository, change-managed users should have CM (instead of WM and WMM).

Note: For information about the Insert, Update, Select, Create Table, Drop Table, and Alter Table permissions, and an additional use of the Delete permission, see the *SAS Guide to Metadata-Bound Libraries*.

Note: For further information, see *SAS Intelligence Platform: Security Administration Guide*.

Permission Conditions

What is a Permission Condition?

A permission condition limits an explicit grant of the Read permission so that different users access different subsets of data.

About Fine-Grained Access Using Permission Conditions

Starting with the first maintenance release for SAS 9.4, you can use permission conditions to give users access to some but not all of the data within a physical table and parent library. For more information about fine-grained controls for data, see *SAS Intelligence Platform: Security Administration Guide*.




Use the following approach:

- 1 If the physical table and its parent library are not already bound to metadata, bind them.
- 2 Set metadata-layer permissions to control who can access each table.
- 3 Use SAS Environment Manager to specify permission conditions.

Icons in Access Management

How are Denials, Grants, and Conditional Grants Indicated?



Table 13.2 Denials, Grants, and Conditional Grants

Icon	Meaning
	Denial
	Grant
	Conditional grant (a grant that is constrained by a permission condition). This icon is applicable to only fine-grained access controls for data (member-level permissions and row-level permissions).

How are Direct Controls Indicated?




The main displays of effective permissions (**Authorization** ► **Basic** tab) use the following icons to provide immediate information about the source of each setting.






Table 13.3 Direct Access Controls

Icon	Term	Meaning
	Direct control: Explicit	The direct access control is set on the current object and specifically assigned to the selected identity.
	Direct control: ACT	The direct access control comes from an applied access control template (ACT) whose pattern specifically assigns the grant or denial to the selected identity.
(none)	Indirect setting	The setting comes from someone else (a group that has a direct control), somewhere else (a parent object or the repository ACT), or special status (such as unrestricted). For the WriteMemberMetadata permission, indirect means that the setting mirrors the WriteMetadata setting.

TIP The explicit and ACT indicator icons correspond to the white and green colors on the **Authorization** window in SAS Environment Manager. As in SAS Environment Manager, if both an explicit control and an applied ACT setting are present, only the explicit indicator is displayed.

Table 13.4 Icon Combinations in the Main Authorization Displays

Icon	Meaning
	Denial from an explicit control
	Denial from an applied ACT
	Denial from an indirect source (such as a parent group or parent object)

Icon	Meaning
	Grant from an explicit control
	Grant from an applied ACT
	Grant from an indirect source (such as a parent group or parent object)
	Conditional grant from an explicit control
	Conditional grant from an indirect source (a parent group)

TIP For additional details about the source of a setting, use the permission origins feature.

What Does a Blank Cell in an ACT Pattern Mean?

The display of an ACT's pattern is limited as follows:

- An ACT's pattern includes only those identities that have pattern settings. For this reason, the table on an ACT's **Authorization** ► **Basic** tab usually includes only a few groups. Not all users and groups are listed.
- An ACT's pattern consists of only those settings that are explicitly defined in the pattern. For this reason, the table on an ACT's **Authorization** ► **Basic** tab usually has grants or denials in only a few cells. The other cells are blank.

Note: This differs from the display in SAS Environment Manager, where the net effect of the pattern is displayed along with the pattern settings.

For each blank cell and each unlisted identity, the net effect of the pattern is determined by the closest pattern setting. Each identity's group memberships determine which setting is closest. The precedence order is as follows:


- 1 The identity's direct group membership have the highest precedence.

- 2 The identity's nested group memberships are next, with each successive level of nesting having lower precedence than the preceding level. Nested memberships are a consideration only if the identity is a member of a group that is in turn a member of another group.
- 3 The identity's automatic membership in the SASUSERS implicit group is next, unless the identity is a user who is not properly registered in the metadata. This group includes all registered users. For example, most users get their repository-level access through grants to SASUSERS in the default ACT's pattern.
- 4 The identity's automatic membership in the PUBLIC implicit group is last. PUBLIC is a superset of SASUSERS. PUBLIC includes everyone that can connect to the metadata server, regardless of whether they are registered users. Because PUBLIC is the broadest group, denials are usually assigned to it.

If an identity has conflicting pattern settings at the same level of precedence, the net effect of those settings is a denial. If there are no pattern settings that are relevant for an identity, the ACT has no effect on that identity.

Permissions Inspector

The permissions inspector enables you to easily and safely look up effective permissions for any user or group.

To launch the inspector, click  (in the toolbar at the right of the table).

The inspector offers the following features:

- The inspector shows the effective permissions that a selected identity has for the specified object. Permissions information is displayed after you look up and select an identity.
- The contents are also updated when you look up and select a different identity (in the text box within the inspector).
- The inspector uses the same icons and indicators that are used on the **Authorization ► Basic** tab.

- You can view origins information by clicking the grant or deny icon.

Here are some tips for using the inspector:

- The inspector is always read-only. To set permissions, open the target object and use its authorization tabs.
- To select an identity, enter a user or group name in the text box. The search is against display name (or, for an identity that does not have a display name, name). The search uses the "contains" criteria — so that you can provide any part of the name.
- Conditional grants are indicated in the inspector, but you cannot access the associated permission conditions from the inspector. Use the **Authorization** ► **Basic** tab to view or update a permission condition. Permission conditions can be applied to both LASR tables and secured tables.
- One inspector window can be open for each object.
- The inspector does not reflect unsaved changes.

Permission Origins

Introduction to Permission Origins

The permission origins feature identifies the source of each effective permission. Permission origins answers the question: Why is this identity granted (or denied) this permission?





















In the origins answer, only the controlling (winning, highest precedence) access control is shown. If there are multiple tied winning controls, they are all shown. Other, lower precedence controls are not shown in the origins answer.




Simple Permission Origins

The following table provides simple examples of permission origins answers. In each example, we are interested in why UserA has an effective grant on FolderA. In each

example, UserA is a direct member of both GroupA and GroupB. Each row in the table is for a different (independent) permissions scenario. In the table, the first column depicts the contents of the Origins window. The second column interprets the information.

Table 13.5 Origins: Simple Examples

Origins Information	Source of UserA's Effective Grant on FolderA
  UserA [Explicit]	On FolderA, an explicit grant for UserA
  GroupA [Explicit]	On FolderA, an explicit grant for GroupA
  GroupA [Explicit]	On FolderA, explicit grants for GroupA and GroupB Note: Two settings are shown because they are tied and they both win (UserA is a direct member of GroupA and GroupB).
  GroupB [Explicit]	
  GroupA [ACT: GroupARead]	On FolderA, an ACT pattern grant for GroupA (from a directly applied ACT)
  SASUSERS [ACT: GenRead]	On FolderA, an ACT pattern grant for SASUSERS (from a directly applied ACT)
  GroupA [ACT: GroupARead]	On FolderA, ACT pattern grants for GroupA and GroupB (from two different directly applied ACTs). Note: Two settings are shown because they are tied and they both win (UserA is a direct member of GroupA and GroupB).
  GroupB [ACT: GroupBRead]	
  GroupA [ACT: GroupABRead]	On FolderA, ACT pattern grants for GroupA and GroupB (from the same directly applied ACT). Note: Two settings are shown because they are tied and they both win (UserA is a direct member of GroupA and GroupB).
  GroupB [ACT: GroupABRead]	

Origins Information	Source of UserA's Effective Grant on FolderA
  UserA is unrestricted.	UserA's status as an unrestricted user (someone who is unrestricted is always granted all permissions)
 This setting mirrors the WriteMetadata setting.	The WriteMetadata setting on FolderA. To investigate further, examine the origins for that setting.







Inherited Permission Origins























In many cases, the controlling setting is not on the current object. Instead, the controlling setting is defined on a parent object and inherited by the current object.

The following table provides examples in which the controlling setting comes from a parent object. Because the source of the effective permission is a parent object, the answer must identify which parent object has the controlling setting. For this reason, the origins answers in the following examples identify both a particular parent object (the object that has the controlling setting) and the controlling setting itself.

In each example, we are interested in why UserA has an effective grant on FolderA. In each example, UserA is a direct member of both GroupA and GroupB. Each row in the table is for a different (independent) permissions scenario. In the table, the first column depicts the contents of the Origins window. The second column interprets the information.

Table 13.6 *Origins: Inheritance Examples*


Origins Information	Source of UserA's Effective Grant on FolderA
 ParentFolderA   UserA [Explicit]	On ParentFolderA, an explicit grant for UserA
 ParentFolderA   GroupA [Explicit]	On ParentFolderA, an explicit grant for GroupA

Origins Information	Source of UserA's Effective Grant on FolderA
 ParentFolderA   GroupA [Explicit]   GroupB [Explicit]	On ParentFolderA, explicit grants for GroupA and GroupB
 ParentFolderA   GroupA [ACT: GroupARead]	On ParentFolderA, an ACT pattern grant for GroupA (from a directly applied ACT)
 GreatGrandParentFolderA   SASUSERS [ACT: GenRead]	On GreatGrandParentFolderA, an ACT pattern grant for SASUSERS (from a directly applied ACT)
 ParentFolderA   GroupA [ACT: GroupARead]   GroupB [ACT: GroupBRead]	On ParentFolderA, ACT pattern grants for GroupA and GroupB (from two different directly applied ACTs)
 GrandParentFolderA   GroupA [ACT: GroupABRead]   GroupB [ACT: GroupABRead]	On GrandParentFolderA, ACT pattern grants for GroupA and GroupB (from the same directly applied ACT).
 SAS Folders   SASUSERS [Explicit]  Default ACT [CustomRepositoryA]   SASUSERS [Pattern]	<p>On the SAS Folders node, an explicit grant for SASUSERS.</p> <p>Also, in CustomRepositoryA's default ACT, a pattern grant for UserA.</p> <p>Note: In this example, FolderA is within a custom repository, so it inherits from both the SAS Folders node and the custom repository's default ACT pattern. Two settings are shown because they are tied and they both win.</p>

Access Control Inheritance

About the Explore Inheritance Diagram

The Explore Inheritance diagram enables you to identify all of the access control parents for object. You can also use this diagram to easily see, for a particular user and permission, where in an object's inheritance path access is gained or lost. For information about permissions, see *SAS Intelligence Platform: Security Administration Guide*.

To access the Explore Inheritance diagram, open the object of interest, select the **Authorization** ► **Basic** tab, and click  (in the toolbar at the right of the table).

TIP The Explore Inheritance diagram shows access control inheritance relationships (such as "a cube inherits effective permissions from its folder"), not lineage relationships (such as "a cube depends on its parent schema"). For example, an information map might use a cube and therefore depend on that cube, but there is no access control relationship between the information map and the cube. The information map and the cube both inherit access controls from their parent folders.

Examples of Explore Inheritance Diagrams

The following figure shows a simple example of an Explore Inheritance diagram.

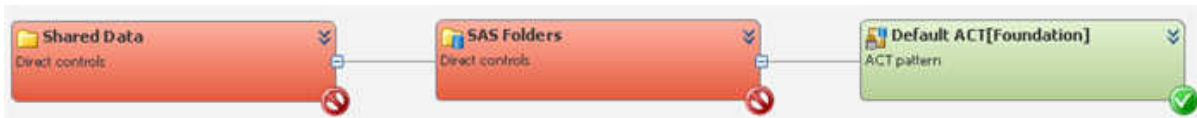


In the preceding example, the diagram was launched from the **Shared Data** folder object, so that object is the left-most object in the display. The immediate parent of **Shared Data** is **SAS Folders**. **SAS Folders** inherits from the repository itself, which is represented by the **Default ACT** because that access control template (ACT) pattern controls access at the repository-level. If you use the controls at the top of the diagram

to show effective permissions for a particular user and permission (for example, the SAS Demo User and the ReadMetadata permission), the display might look like the following figure:



In the preceding example, the selected user has the selected type of access through the entire inheritance path. If you use the controls at the top of the diagram to select a different permission (for example, the WriteMetadata permission), the display might look like the following figure.



In the preceding example, the selected user has the selected type of access at the repository-level, but loses that access at the **SAS Folders** node. One way to investigate why access is lost at that node is to examine the details within that node. For example, you might find that the PUBLIC group has an explicit denial of WriteMetadata, and no other group that the selected user belongs to has a direct grant. In the following figure, the **SAS Folders** node shows its details.



Note: In the unusual circumstance in which an object has more than one immediate parent, the diagram has multiple branches. When an object has more than one inheritance path, a grant from either path is sufficient to provide access.

Tips for Exploring Inheritance

Here are some tips for using the Explore Inheritance diagram:

- The diagram is read-only. You cannot open new object tabs from within the diagram or make changes from within the diagram.
- Most objects have only one immediate parent, so the display is usually a simple horizontal chain of objects.
- The current object (the object from which you launched the diagram) is the left-most node.
- The orientation, from left to right, moves from child to parent (showing "inherits from" relationships).
- You can use the buttons at the top of the diagram to quickly manipulate the entire display (for example, to expand the entire diagram or show details for all nodes).
- Unsaved changes are not reflected in the diagram.
- Each node contains details as follows:
 - For a right-most node (a node that represents a repository), the permission pattern of the repository's ACT is displayed.
 - For other nodes:
 - If there are direct controls, those controls are displayed.
 - If there are no direct controls, the node does not have details.
- When effective permissions are displayed, a status icon in the lower right corner of each node indicates whether the selected identity is granted or denied the selected permission. You can click on a status icon to view origins information for that effective setting.
- Not all permissions are applicable to all types of objects, so the permission drop-down list does not always list all permissions. Only the permissions that are relevant for the current object (the left-most node) are listed. For example, only ReadMetadata and WriteMetadata are supported for reports, so when you launch

the diagram from a report only those two permissions are offered in the permissions drop-down list.

- If you lack ReadMetadata access to any of the parent objects, the left-most node to which you lack ReadMetadata access is indicated as **Unknown**, and no further nodes are displayed.
- When you examine effective access for the WriteMetadata (WM) or WriteMemberMetadata (WMM) permission, remember that inheritance of these permissions is specialized. WMM on a parent folder becomes WM on the child items within that folder; WM itself is not inherited from folders.

Note: Folders that represent repositories (for example, the **SAS Folders** node) are software components (not true folders), so they do not support WMM. When you examine effective WMM permissions, folders that represent repositories do not show an effective permission.




Permission Condition

Row-level security enables you to control who can access particular rows within a LASR table or a SAS data set bound to a SecuredTable object, and it is defined by data filter expressions. Row-level access distinctions can be based on a simple attribute (such as security clearance level) or on a more complex expression that consists of multiple criteria.

Row-level security affects access to subsets of data within a resource. To establish row-level security, you add constraints called permission conditions to explicit grants of the Read or Select permission. Each permission condition filters a particular LASR table or metadata bound data set for a particular user or group. Each permission condition constrains an explicit grant of the Read or Select permission so that the associated user or group can see only those rows that meet the specified condition.

When row-level security is used, there are three possible authorization decision outcomes for a user request to view data:

Table 13.7 *Denials, Grants, and Conditional Grants for Permission Conditions*

Icon	Term	Meaning
	Denial	The requesting user cannot see any rows.
	Grant	The requesting user can see all rows.
	Conditional grant	The requesting user can see only those rows that meet the specified filtering conditions.

Here are some key points about how permission conditions are incorporated into the metadata-layer access control evaluation process:

- A permission condition is applied only if it is on the setting that is closest to the requesting user. Other permission conditions that are relevant because of further-removed group memberships do not provide additional, cumulative access.
- If there is an identity precedence tie between multiple groups at the highest level of identity precedence, those tied conditions are combined in a Boolean OR expression. If the identity precedence tie includes an unconditional grant, access is not limited by any conditions.

The following table provides examples:

Table 13.8 *Precedence for Permission Conditions*

Principle	Scenario	Outcome and Explanation
If there are multiple permission conditions that apply to a user because of the user's group memberships, then the identity that has the highest precedence controls the outcome.	<p>A condition on TableA limits Read permission for GroupA.</p> <p>Another condition on TableA limits Read permission for the SASUSERS group.</p> <p>The user is a member of both GroupA and SASUSERS.</p>	The user can see only the rows that GroupA is permitted to see. GroupA has a higher level of identity precedence than SASUSERS, so the filters that are assigned to GroupA define the user's access.

If there are multiple permission conditions at the highest level of identity precedence, then any data that is allowed by any of the tied conditions is returned.

A condition on TableA limits Read permission for GroupA.
Another condition on TableA limits Read permission for GroupB.
The user is a first level member of both GroupA and GroupB.

The user can see any row that is permitted for either GroupA or GroupB.

Best Practices for Permissions

Assign Access Controls to Groups

You can simplify access control by assigning permissions to groups rather than to individual users. Here are some examples:

- To allow only unrestricted users to access an object, assign denials to the PUBLIC group.
- To enable only registered users to access an object, assign denials to the PUBLIC group and grants to the SASUSERS group.
- To enable only information developers and unrestricted users to access an object, create a group for the developers. On the object, assign denials to the PUBLIC group and assign grants to the developers group.

Use Folders to Organize Content

You can simplify access control by creating a folder structure that reflects the access distinctions that you want to make. Instead of adding access controls to each individual object, add access controls to parent folders. The objects in a folder inherit the effective permissions for a folder.

TIP To protect the folder structure, do not grant WriteMetadata permission on a folder to someone if granting them WriteMemberMetadata permission is sufficient.

Centralize Permissions with Access Control Templates

You can simplify access control by using access control templates (ACTs). An ACT is a reusable pattern of settings that you can apply to multiple objects. Each ACT consists of the following elements:

- a list of users and groups
- for each identity and permission, an indication of whether the pattern of an ACT provides a grant, a denial, or no pattern setting

Deny Broadly, Grant Selectively (To the Extent Possible)

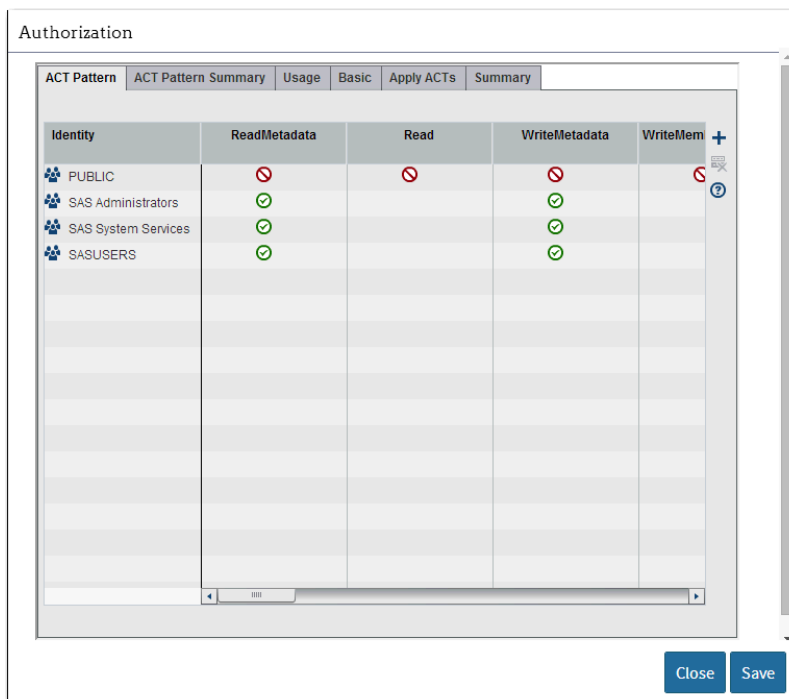
Assign denials to the broadest group (PUBLIC) and then add offsetting grants for users or groups whose access you want to preserve. Deny access at the highest point of control and then grant access back on specific containers or objects. The following constraints apply:

- The highest point of control is the repository-level settings for the foundation repository. The security model requires that participating users have ReadMetadata and WriteMetadata access at this level. Therefore, broadly denying access in the permission pattern of the foundation repository's Default ACT is not a workable approach. Instead, use the next point of control, which is the top of the **SAS Folders** tree.
- In order to navigate within the folder tree, users need a clear path of grants of ReadMetadata to the objects that they use. For the ReadMetadata permission, setting denials on folders at a high level is not a workable approach.

Note: When users access objects by searching (instead of by navigating through the folder tree), a clear path of grants of ReadMetadata is not required.

Manage Metadata Information

- 1 Click the **Administration** tab.
- 2 Click the **Folders** module.
- 3 Right-click on an object in the **Folders** pane, and select **Open**. The tab corresponding to the object that you selected is displayed.
- 4 Click the **Authorization** tab, and then click **Open Authorization Information**. A window similar to the following appears:



Apply an ACT

- 1 Open the object to which you are applying the ACT.
- 2 Select the **Authorization** tab, and then click **Open Authorization Information**.
- 3 On the **Apply ACTs** tab for an object, select the check box for the appropriate ACT.

TIP You should not apply the repository ACT (which is usually named Default ACT) directly to any object. The repository ACT participates through inheritance, serving as an access control parent of last resort.

- 4 On the **Basic** tab for the object, the identities that participate in the pattern of an ACT are listed. Verify that the revised settings are as you expect.
- 5 Save your changes.

Create an ACT

- 1 Access the **Administration** tab.
- 2 From the **Folders** pane, navigate to **SAS Folders** ► **System** ► **Security** ► **Access Control Templates**.
- 3 Right-click **Access Control Templates** and select **New Access Control Template**.
- 4 In the New Access Control Template window, enter a name and description for the ACT. Click **Save**.
- 5 Right-click the new ACT and click **Open**. The new ACT opens in its own tab.

- 6 Click the **Authorization** tab, and then click **Open Authorization Information**. On the **ACT Pattern** tab:
 - a Click **+**. In the Add Identities window, select users and groups that will have explicit settings in the pattern. Click **OK**.
 - b On the **ACT Pattern** tab, click cells and make selections from the lists to define the ACT's pattern.

Note: For information about the icons and blank cells in an ACT's pattern, see [“Icons in Access Management” on page 167](#).
- 7 On the ACT's **Authorization** tabs, protect the new ACT. For example, one approach is to add an explicit denial of WriteMetadata for PUBLIC and an offsetting explicit grant of WriteMetadata for SAS Administrators.

Note: It is important to prevent regular users from modifying or removing an ACT.
- 8 Save the new ACT.
- 9 To use the ACT, apply it to one or more objects.

Note: The applied ACT contributes its pattern of access controls to the object's protections. The object can also have explicit controls and other applied ACTs (as well as inherited settings).
- 10 If necessary, adjust the ACT's pattern. You can change the pattern of an ACT without modifying the objects to which the pattern is applied.

Update an ACT

CAUTION! One ACT can protect thousands of objects. Changes that you make to an ACT's pattern affect every object to which that ACT is applied.

Locate an ACT

- 1 Click the **Administration** tab.
- 2 In the **Folders** pane, navigate to **SAS Folders** ► **System** ► **Security** ► **Access Control Templates**.

Note: To locate ACTs that are in custom repositories, your navigation path will vary slightly. For example: **SAS Folders** ► *custom-repository* ► **System** ► **Security** ► **Access Control Templates**.

- 3 Find the ACT that you want to update.

Modify an ACT

- 4 Right-click the ACT and select **Open**. The ACT opens in its own tab.
- 5 Click the **Authorization** tab, and then click **Open Authorization Information**. To understand the potential impact of your intended changes, examine the ACT's **Usage** tab.

- 6 To modify the ACT's pattern:

- a Adjust settings on the **Basic** tab.

Note: For information about the icons and blank cells in an ACT's pattern, see [“Icons in Access Management” on page 167](#).

- b Save the ACT.

- 3 (Optional) Navigate to an object that uses the ACT and verify that the revised settings are as you expect.

Note: To delete an existing ACT, use SAS Management Console. For more information, see *SAS Management Console: Guide to Users and Permissions*.

Add an Explicit Grant or Denial

- 1 Open the object that you want to protect or make available.
- 2 Click the **Authorization** tab, and then click **Open Authorization Information**. On the **Basic** tab, locate the user or group that you want to assign an explicit control to. If the user or group is not listed, click **+** to open the Add Identities window.

Note: An explicit grant of the ReadMetadata permission is automatically set for each identity that you add.

- 3 Click a cell and make a selection from the list.

Note: If the selected identity is unrestricted, all permissions are granted and you cannot make changes.

Note: When you click outside the cell, the yellow diamond that indicates an explicit control is displayed in the cell that you updated.

- 4 If you changed the access for a group, review the impact on all of the listed identities.

Note: Controls that you add for a group can affect access for all members of that group. For example, an explicit denial that you add for the PUBLIC group blocks access for all restricted users, unless there are also explicit (or direct ACT) grants. You must offset a broad explicit denial with explicit (or direct ACT) grants for any restricted identities whose access you want to preserve.

- 5 Save your changes.



TIP It is easy to add explicit grants and denials on each object that you want to protect or make available. However, adding a large number of individual access controls can make access control management cumbersome.

Add a Row-Level Permission Condition

To limit Read access to rows in a LASR table:

- 1 Click the **Authorization** tab, and then click **Open Authorization Information** for a LASR table. Click the **Basic** tab.
- 2 In the **Read** column, click the cell for the identity that you want to assign the condition to and select **Conditional grant** from the list.

Note: If the identity is not already listed, click **+** at the right edge of the table to add the identity.

Note: If **Conditional grant** is already selected, a condition already exists. Select **Conditional grant** to view or update the condition.
- 3 In the New Permission Condition window, create a condition that specifies which rows the identity can see.
- 4 Click **OK**. The cell contains the conditional grant icon  with an explicit control indicator .
- 5 If you set a permission for a group, review the impact on the other listed identities. Constraints that you add for a group can affect access for all members of that group.
- 6 Save your changes.

Provide Fine-Grained Access Using Permission Conditions

- 1 Click the **Authorization** tab, and then click **Open Authorization Information** for the secured table object that corresponds to the metadata-bound library whose data sets you want to protect.



- 2 Click the **Basic** tab.
- 3 In the **Select** column, click the cell for the identity whose access you want to limit. Select **Conditional grant** to add an explicit grant of the Select permission for the selected identity.

Note: If the identity is not already listed, click **+** at the right edge of the table to add the identity.

Note: If **Conditional grant** is already selected, a condition already exists. Select **Conditional grant** to view or update the condition).
- 4 In the New Permission Condition window, enter the WHERE clause for an SQL query that filters the data as appropriate for the selected identity. Do not include the WHERE key word in your entry.

TIP To make dynamic, per-person access distinctions, you can use identity-driven properties as the values against which target data values are compared. Use the following syntax when you specify one of these properties:
`SUB::property-name` (for example, `SUB::SAS.UserId`). For a list of available identity-driven properties, see *SAS Intelligence Platform: Security Administration Guide*.

CAUTION! The syntax that you enter and save in the New Permission Condition window is not checked for validity. Make sure that the syntax that you entered is correct.

- 5 Click **OK**. The cell contains the conditional grant icon  with an explicit control indicator .
- 6 Save your changes.



Part 4

Appendixes

<i>Appendix 1</i>	
<i>Troubleshooting</i>	191
<i>Appendix 2</i>	
<i>Manual Setup Examples</i>	199
<i>Appendix 3</i>	
<i>Data Mart Table Reference</i>	211

Appendix 1

Troubleshooting

<i>Resolving Problems with SAS Environment Manager</i>	191
<i>Resolving Problems with SAS Environment Manager Agents ..</i>	194
<i>Resolving Problems with SAS Environment Manager Plugins</i>	196

Resolving Problems with SAS Environment Manager

Cannot Add Discovered Resources into Inventory

When you add auto-discovered resources into the inventory, you might see the following error message

```
Unable to import platform :
org.hyperic.hq.common.SystemException:
org.hibernate.ObjectNotFoundException:No row the the given
identifier exists: [org.hyperic.hq.autoinventory.Allp#10001]
```

Purge the AIQ data in the SAS Environment Monitor database. Follow these steps:

- 1** Select **Manage** ► **HQ Health** ► **Database tab**
- 2** Select **Purge AIQ Data** from the **Action** menu.

These messages appear:

- DELETE FROM EAM_AIQ_IP: 0 rows
- DELETE FROM EAM_AIQ_SERVICE: 0 rows
- DELETE FROM EAM_AIQ_SERVER: 0 rows
- DELETE FROM EAM_AIQ_PLATFORM: 0 rows

3 Restart the agents.

Resource in Availability Portlet with No Availability Information

If you add a resource that has been discovered but does not have any availability information to an Availability Summary portlet, the portlet will never display any information for the resource. The server log contains this information:

- 1 On the **Resources** tab, delete the platform that contains the resource.
- 2 Stop the agent.
- 3 Delete the tokendata, keystore, and keyvals files from the directory `<SAS-configuration-directory>/Lev2/Web/SASEnvironmentManager/agent-5.8.0-EE/data`.
- 4 Issue the command `hq-agnet.bat/sh restart` from the command console.

New Folders Are Not Displayed

If you are using Microsoft Internet Explorer, newly created folders might not show up in the folder tree.

To ensure that new folders appear, from the Internet Explorer menu, select **Tools ► F12 Developer Tools**. From the Internet Explorer Developer Tools menu, select **Cache ► Always refresh from server**.

Validate Result Dialog Box Appears When Renaming a Folder

If you cause an error when you rename a folder (because, for example, you used invalid characters in the name or specified a blank name), the folder is not saved and the Validate Result dialog box appears.

To view details about the error, click the text **Basic Properties page failed** in the dialog box.

Disabling Secure Sockets Layer (SSL) 3.0 in SAS Environment Manager Server

When you configure the SAS Environment Manager Server, SSL 3.0 is enabled by default. SSL 3.0 is vulnerable to the POODLE security attack.

To disable SSL 3.0 in the SAS Environment Manager Server, follow these steps:

- 1 Open the server.xml file that is in the directory `server-5.0.0-EE/hq-engine/hq-server/conf` under the SAS Environment Manager directory.

- 2 Locate the <Connector> element that specifies `SSLEnabled="true"`

- 3 Specify the `sslProtocols` parameter in the <Connector> element.

```
<Connector ... sslProtocols="TLSv1,TLSv1.1,TLSv1.2"/>
```

- 4 Save the file and restart the SAS Environment Manager Server.

Note: Depending on your release of SAS Environment Manager, the `sslProtocols` parameter might already be specified. If this is the case, SSL 3.0 is already disabled and you do not need to take any further action.

User Manager Does not Appear in Microsoft Internet Explorer

The User Manager might not appear when you are using SAS Environment Manager with Microsoft Internet Explorer version 9 or version 11.

If you are using Microsoft Internet Explorer version 9, follow these steps:

- 1 From the Internet Explorer menu bar, select **Tools ► F12 developer tools**. The developer tools area appears at the bottom of the window.
- 2 In the menu bar of the developer tools area, locate the **Developer Tools** entry.
- 3 If the entry appears as **Developer Tools: Quirks**, click on the entry and select **Internet Explorer 9 standards** from the context menu.
- 4 From the developer tools menu bar, select **File ► Exit**.

If you are using Microsoft Internet Explorer version 11, follow these steps:

- 1 Select the **Tools** icon in the upper-right corner of the Internet Explorer window to display the **Tools** menu.
- 2 Select **Compatibility View settings** from the **Tools** menu.
- 3 In the Compatibility View Settings window, clear the checkbox **Display intranet sites in Compatibility View**.
- 4 Close the Compatibility View Settings window.

Resolving Problems with SAS Environment Manager Agents

Agent Fails to Start

When you try to configure the SAS Environment Manager Agent, it does not start and you receive the error message `No token file found, waiting for Agent to initialize`

- 1 Stop the SAS Environment Manager agent.
- 2 Verify that the agent wrapper processes and the agent Java processes have stopped.
- 3 On the W6X platform, verify that the directory `%SystemRoot%/TEMP` exists. Remove the file `%SystemRoot%/TEMP/agent.encrypt.lock`.

On all other UNIX platforms, search for the `java.io.tmpdir` environment variable in the agent wrapper process and the agent Java process. By default, the value of the variable will be set to the `/tmp` or `/var/tmp` directory. If the variable exists, remove the file `agent.encrypt.lock` under the specified directory.

Agent Receives the Error “OutOfMemory GC Overhead Limit Exceeded”

The `agent.log` file contains the message `java.lang.OutOfMemoryError: GC overhead limit exceeded`

Include these JVM options in the startup script for each agent:

```
-XX:NewRatio=8
-XX:+CMSClassUnloadingEnabled
-XX:+UseTLAB
-XX:+UseCompressedOops
```

Modify the file `SAS-configuration_directory/LevX/Web/SASEnvironmentManager/agent-5.8.0-EE/bundles/agent-5.8.0/bin/hq-agent.sh` or `hq-agent.bat` and add these JVM options to the `CLIENT_CMD` variable:

```
CLIENT_CMD="${HQ_JAVA} \
-D${AGENT_INSTALL_HOME_PROP}=${AGENT_INSTALL_HOME} \
-D${AGENT_BUNDLE_HOME_PROP}=${AGENT_BUNDLE_HOME} \
-XX:NewRatio=8 \
-XX:+CMSClassUnloadingEnabled \
-XX:+UseTLAB \
-XX:+UseCompressedOops \
-cp ${CLIENT_CLASSPATH} ${CLIENT_CLASS}"
```

EncryptionOperationNotPossibleException Error Message

After the agent successfully starts, some agent properties might get encrypted. If the agent cannot read the `agent.scu` file (which contains the encryption keys), it cannot decrypt the properties. The agent will not start and the `agent.log` or the `wrapper.log` file contains the error

```
org.jasypt.exceptions.EncryptionOperationNotPossibleException.
```

- 1** Stop the SAS Environment Manager agent.
- 2** In the directory `SAS-configuration/Lev2/Web/SASEnvironmentManager/agent-5.8.0-EE`, delete the `/data` directory.
- 3** In the directory `SAS-configuration/Lev2/Web/SASEnvironmentManager/agent-5.8.0-EE/conf`, delete the `agent.scu` file.

- 4 Modify the encrypted property to a plain text value. In the file `SAS-configuration/Lev2/Web/SASEnvironmentManager/agent-5.8.0-EE/agent.properties`, set the property `agent.setup.camPword` to a plain text value (if it is encrypted, it will appear as `ENC(XXXXXXXXXX)`).
- 5 In the file `SAS-configuration/Lev2/Web/SASEnvironmentManager/agent-5.8.0-EE/auto-approve.properties`, change all values to `True`.
- 6 Restart the agent.

Cannot Stop EAgent Service Using Windows Services

On Windows, if you use Windows Services to stop the Hyperic Agent service, you will receive the error message `Windows could not stop the SAS[SAS94-Lev1] SAS Environment Manager Agent on Local Computer. Clicking OK in the error message dialog box seems to stop the service, but the System Event Log contains the error` `The SAS [SAS94-Lev1] SAS Environment Manager Agent service terminated with service-specific error Incorrect function..`

Use the command line, rather than Windows Services, to stop the agent. The command to stop the agent is `<sas_configuration_directory>/Lev2/Web/SASEnvironmentManager/agent-5.8.0-EE/bin/hq-agent.bat stop`.

Resolving Problems with SAS Environment Manager Plugins

PostgreSQL Resources Not Configured Properly

After a PostgreSQL server is added into inventory, the Dashboard page indicates that the resource is not configured properly

On the Configuration Properties page for the server, specify this information:

`postgresql.user`

specify the Web Infrastructure Platform Data Server database user name. The default value is `dbmsowner`

postgresql.pass

specify the password for the user name

postgresql.program

specify the path to the postgres.bat or postgres.sh file (on UNIX); or postgres.exe or postgres.bat (on Windows). On UNIX, the path is `/opt/sas/Lev1/SASWebInfrastructurePlatformDataServer/webinfdsvrc.sh`. On W6X, the path is `<SAS_Configuration_Directory>\Lev1\SASWebInfrastructurePlatformDataServer\webinfdsvrc.bat`.

Tomcat Resources Not Configured Properly

On the AIX platform, the Apache Tomcat 6.0 server Resource page displays the error This resource is turned off or has not been configured properly. The problem is: Invalid configuration: Error contacting resource: Can't connect to MBeanServer url .

- 1 Open the file `SAS_configuration_directory/Lev1/Web/SASEnvironmentManager/server-5.8.0-EE/hq-engine/hq-server/conf/hq-catalina.properties` and find the `jmx.url` port number. The default value is 1099.
- 2 On the Configuration Properties page for the server, specify the following property:

`jmx.url`

`service:jmx.rmi:///jndi/rmi://localhost:port_number`

Cannot Discover tcServer Instances

On the H6I platform, no tcServer instances can be discovered.

HPUX has a limit of 1020 characters on command line queries. The parameters that the tcServer plugin uses to identify the tcServer process are not seen by the agent because they fall after the 1020 character limit has been reached. Edit the startup script so that the parameters that the plugin needs are seen before the 1020 character limit.

Edit the `catalina.sh` script. Change this section of the script:

```
eval \"$_RUNJAVA\" \"${LOGGING_CONFIG}\" $JAVA_OPTS $CATALINA_OPTS \
-Djava.endorsed.dirs=\"${JAVA_ENDORSED_DIRS}\" -classpath \"${CLASSPATH}\" \
-Dcatalina.base=\"${CATALINA_BASE}\" \
```

```
-Dcatalina.home="\$CATALINA_HOME\" \
-Djava.io.tmpdir="\$CATALINA_TMPDIR\" \
org.apache.catalina.startup.Bootstrap "$@" start \
>> "\$CATALINA_OUT" 2>&1 "&"
```

Change the script to this:

```
eval "\$ _RUNJAVA\" \"$LOGGING_CONFIG\" \
-Dcatalina.base="\$CATALINA_BASE\" \
-Dcatalina.home="\$CATALINA_HOME\" \
$JAVA_OPTS \
$CATALINA_OPTS \
-Djava.endorsed.dirs="\$JAVA_ENDORSED_DIRS\" -classpath "\$CLASSPATH\" \
-Djava.io.tmpdir="\$CATALINA_TMPDIR\" \
org.apache.catalina.startup.Bootstrap "$@" start \
>> "\$CATALINA_OUT" 2>&1 "&"
```

SAS Environment Manager Agent Will Not Start

Cannot start the SAS Environment Manager Agent by using the start script \$SAS - configuration _directory/LevX/Web/SASEnvironmentManager/agent-5.8.0-EE/bin/hq-agent.sh start.

The console displays this message:

```
Starting HQ Agent.....Removed stale pid file:
/local/install/cfgsas1/config/Lev1/Web/SASEnvironmentManager/agent-5.8.0-EE/wrapper
WARNING: HQ Agent may have failed to start.
```

Use the unset command to remove the COLUMNS environment variable.

Appendix 2

Manual Setup Examples

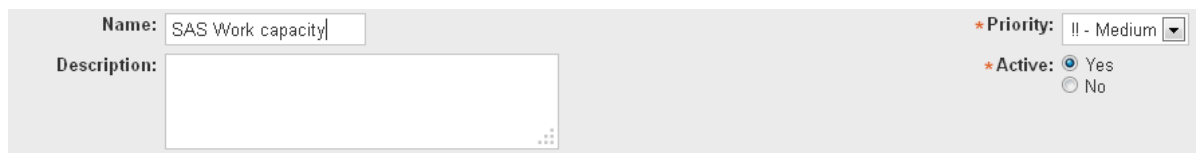
<i>Alert Definition Examples</i>	200
Example: Defining an Alert for SAS Work Directory Space	200
Example: Defining an Alert for a SAS Server Log File	201
<i>Manually Configuring HTTP Components and Applications</i>	202
Creating a Platform Service	202
Configuring a Platform Service for SAS Stored	
Process Web Application	204
Configuring a Platform Service for SAS Content Server	205
Configuring a Platform Service for SAS Web Report Studio	206
Configuring a Platform Service for SAS BI Dashboard	207
Configuring a Platform Service for SAS Help	
Viewer for Middle-Tier Applications	208
Configuring a Platform Service for SAS	
Information Delivery Portal	208
Configuring a Platform Service for SAS Web	
Administration Console	209

Alert Definition Examples

Example: Defining an Alert for SAS Work Directory Space

This example provides information for setting up an alert to be triggered whenever the SAS Work directory reaches 90% of its capacity. The alert should be issued once every two hours until the condition is cleared. When the alert is triggered, users with the Operations role should be notified.

- 1 Locate the service **SAS Home Directory 9.4 SAS work directory**. The service is under the **SAS Home Directory 9.4** server.
- 2 Navigate to the Resource Detail page for the service. On the Detail page, select **Alert ► Configure** to display the Alert Configuration page. Click **New** to display the New Alert Configuration page.
- 3 Name the alert, select the priority, and specify that the alert should be active.



The screenshot shows the 'New Alert Configuration' page. It has a light gray background. On the left, there are two labels: 'Name:' and 'Description:'. The 'Name:' label is followed by a text input field containing 'SAS Work capacity'. The 'Description:' label is followed by a larger text area that is currently empty. On the right side, there are two settings. The first is 'Priority:' with a dropdown menu showing '!! - Medium'. The second is 'Active:' with two radio buttons: 'Yes' (which is selected) and 'No'.

- 4 In the **If Condition** area, select the **Metric** radio button, then select **Use Percent** in the **Metric** field.
- 5 To specify 90% capacity, enter .9 in the **absolute value** field. To specify that the alert is triggered whenever the used capacity exceeds 90%, specify and select **> (Greater than)** from the comparison menu.

★ **If Condition:** ☒ Metric: Use Percent ▼

☒ is ▶ > (Greater than) ▼ .9 (absolute value)

☐ is ▶ > (Greater than) ▼ % of Select... ▼

☐ value changes

- 6** In the **Enable Action(s)** field, specify **1** for the number of times the alert is issued, **2** for the timer period, and select **hours** for the time period units. These values specify that the alert is issued one time every two hours while the alert conditions are met.

★ **Enable Action(s):** ☐ Each time conditions are met

☒ Once every times conditions are met within a time period of hours ▼

- 7** Click **OK** to define the alert and display the Configuration page for the new alert.
- 8** Select **Notify Roles**, and then select **Add to List**.
- 9** Select the check box beside **Operations** in the **Roles** list and use the arrow control to move the role to the **Add Role Notification** list.
- 10** Click **OK** to close the Role Selection page and then **Return to Alert Definitions** to complete the process of defining the alert.

Example: Defining an Alert for a SAS Server Log File

This example provides information for setting up an alert to be triggered whenever a warning message for the I/O Subsystem appears in the log of the SAS Metadata Server. The alert should be issued every time an error appears in the log.

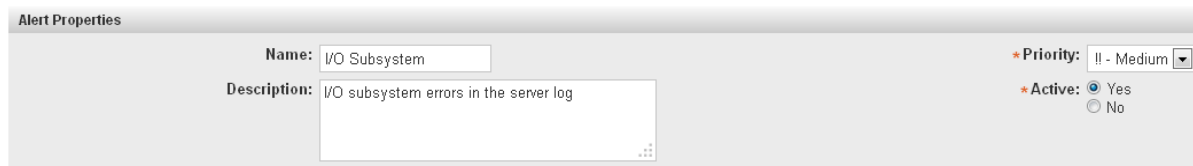
- 1** Follow the procedure in [“Creating Events Based on SAS Server Logs”](#) on page 70 to create an event from the SAS Metadata Server log file. Add the entry

```
level.warn.2=.*I/O Subsystem.*
```

to the sev_logtracker_plugin.properties file for the SAS Metadata Server.

- 2** Locate the server **SASMeta – SAS Metadata Server** in the Resource page.

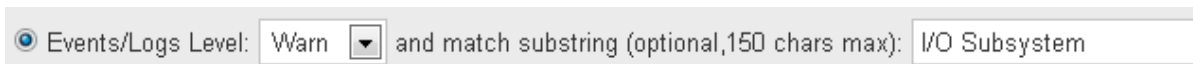
- 3 Navigate to the Resource Detail page for the server. On the Detail page, select **Alert** ► **Configure** to display the Alert Configuration page. Click **New** to display the New Alert Configuration page
- 4 Name the alert, select the priority, and specify that the alert should be active.



The image shows the 'Alert Properties' dialog box. It has a 'Name' field with the value 'I/O Subsystem'. The 'Description' field contains the text 'I/O subsystem errors in the server log'. On the right side, there are two settings: 'Priority' is set to '!! - Medium' (indicated by a red star icon), and 'Active' is set to 'Yes' (indicated by a selected radio button).

- 5 In the **If Condition** area, select the **Event/Logs Level** radio button, then select **Warn** in the **Event/Logs Level** field.

In the **match substring** field, enter **I/O Subsystem**. These values specify that an alert is issued whenever an event is found for a Warn message from the log containing the string “I/O Subsystem.”



The image shows the configuration for the 'Events/Logs Level' section. It includes a radio button for 'Events/Logs Level', a dropdown menu set to 'Warn', and a text field for 'and match substring (optional, 150 chars max):' containing the value 'I/O Subsystem'.

- 6 In the **Enable Action(s)** area, select the **Each time conditions are met** radio button. This specifies that the alert is triggered each time an I/O Subsystem warning appears in the log.
- 7 Click **OK** to define the alert.

Manually Configuring HTTP Components and Applications

Creating a Platform Service

You must create several platform services in order to monitor access to SAS web applications. This is the basic procedure for creating and configuring a platform service.

If you enable SAS Environment Manager Extended Editing, these services are created automatically.

- 1 Select **Resources** ► **Browse**
- 2 Select **Platforms**.
- 3 Select the entry in the **Platform** table for your server.
- 4 On the Details page for the selected platform, select **Tools Menu** ► **New Platform Service**. The New Service window appears.
- 5 Specify a name for the service and select **HTTP** in the **Service Type** field. Click **OK**.

The screenshot shows the 'New Service' dialog box with the following details:

- General Properties:**
 - Name:** Stored Process Web Ap
 - Description:** (Empty text area)
- Type & Host Properties:**
 - Service Type:** HTTP (selected in the dropdown menu)
 - The dropdown menu lists the following options: DHCP, DNS, EMIPing, FileServer Directory, FileServer Directory Tree, FileServer File, FileServer Mount, FileServer Physical Disk, FTP, **HTTP** (highlighted), HyperV Logical Processor, HyperV Memory, HyperV Network Interface, HyperV Physical Disk, IMAP, InetAddress Ping, LDAP, MultiProcess, NetworkServer Interface, and NTP.
- Buttons:** OK, Reset, Cancel

- 6 The **Details** page for the new service page appears. A message is displayed that the resource has not been configured. Click the **Configuration Properties** link to configure the service.
- 7 On the Configuration Properties page, specify the information required for the service. Values for each service are provided in the following sections.

Configuration Properties
Shared

Use SSL ☐

port 7980
Port

path /SASStoredProcess
Path

pass
Password

method GET
Request Method

follow ☒
Follow Redirects

proxy
Proxy Connection

secretrequestparams
Secret Request Arguments: arg0=va0,arg1=va1,...

hostname localhost
Hostname

timeout 10
Socket Timeout (in seconds)

user sasdemo
Username

realm
Realm

hostheader
Host Header

pattern SASStoredProcess
Response Match (substring or regex)

requestparams
Request Arguments: arg0=va0,arg1=va1,...

Monitoring

service.log_track.enable ☒
Enable Log Tracking

service.log_track.level Info
Track event log level

service.log_track.include Stored
Log Pattern Match

service.log_track.exclude
Log Pattern Exclude

OK Reset Cancel

8 Click **OK** to complete the configuration process.

Configuring a Platform Service for SAS Stored Process Web Application

Follow the steps in “[Creating a Platform Service](#)” on page 202 to create the service. Specify the following information on the Configuration Properties page.

port

specify 7980

path

specify /SASStoredProcess

user

specify a username (such as sasdemo)

pass

specify the password for the specified user

method

select **GET**

follow

select this check box

pattern

specify `SASStoredProcess`

service.log.track.enable

select this check box

service.log.track.level

select **Info**

service.log.track.include

specify `Stored`

Configuring a Platform Service for SAS Content Server

Follow the steps in [“Creating a Platform Service” on page 202](#) to create the service. Specify the following information on the Configuration Properties page.

port

specify `7980`

path

specify `/SASContentServer`

user

specify `sasadm@saspw`

pass

specify the password for the user

method

select **GET**

follow

select this check box

pattern

specify `SASContentServer`

service.log.track.enable

select this check box

service.log.track.level

select **Info**

service.log.track.include

specify **Content**

Configuring a Platform Service for SAS Web Report Studio

Follow the steps in “[Creating a Platform Service](#)” on page 202 to create the service. Specify the following information on the Configuration Properties page.

port

specify 7980

path

specify **/SASWebReportStudio**

user

specify a username (such as sasdemo)

pass

specify the password for the user

method

select **GET**

follow

select this check box

pattern

specify **SASWebReportStudio**

service.log.track.enable

select this check box

service.log.track.level

select **Info**

service.log.track.include

specify **Report**

Configuring a Platform Service for SAS BI Dashboard

Follow the steps in [“Creating a Platform Service” on page 202](#) to create the service. Specify the following information on the Configuration Properties page.

port

specify **7980**

path

specify **/SASBIDashboard**

user

specify a username (such as **sasdemo**)

pass

specify the password for the user

method

select **GET**

follow

select this check box

pattern

specify **SASBIDashboard**

service.log.track.enable

select this check box

service.log.track.level

select **Info**

service.log.track.include

specify **Dashboard**

Configuring a Platform Service for SAS Help Viewer for Middle-Tier Applications

Follow the steps in “[Creating a Platform Service](#)” on [page 202](#) to create the service. Specify the following information on the Configuration Properties page.

port

specify **7980**

path

specify **/SASWebDoc**

method

select **GET**

follow

select this check box

pattern

specify **SASWebDoc**

service.log.track.enable

select this check box

service.log.track.level

select **Info**

service.log.track.include

specify **Documentation**

Configuring a Platform Service for SAS Information Delivery Portal

Follow the steps in “[Creating a Platform Service](#)” on [page 202](#) to create the service. Specify the following information on the Configuration Properties page.

port

specify 7980

path

specify `/SASPortal`

user

specify a username (such as sasdemo)

pass

specify the password for the user

method

select **GET**

follow

select this check box

pattern

specify `SASPortal`

service.log.track.enable

select this check box

service.log.track.level

select **Info**

service.log.track.include

specify `Portal`

Configuring a Platform Service for SAS Web Administration Console

Follow the steps in [“Creating a Platform Service” on page 202](#) to create the service. Specify the following information on the Configuration Properties page.

port

specify 7980

path

specify `/SASAdmin`

user

specify `sasadm@saspw`

pass

specify the password for the user

method

select **GET**

follow

select this check box

pattern

specify `SASAdmin`

service.log.track.enable

select this check box

service.log.track.level

select **Info**

service.log.track.include

specify `Administration`

Appendix 3

Data Mart Table Reference

About SAS Environment Manager Data Mart Tables	212
ACM Tables	213
ACM.AVAILABILITY Table	213
ACM.FILEMOUNTS Table	213
ACM.GROUPINVENTORY Table	213
ACM.EVENTS Table	214
ACM.HOSTPLATFORMS Table	214
ACM.HTTPCHECKS Table	215
ACM.IOMSERVERS Table	215
ACM.MEASUREINVENTORY Table	216
ACM.METADATASVRS Table	216
ACM.NETWORKINTERFACE Table	217
ACM.RESOURCEINVENTORY Table	218
ACM.TCSSERVERMGRS Table	218
ACM.WEBAPPSERVER Table	218
ACM.WIPDATADB Table	219
APM Tables	219
ARTIFACT.RELATIONSHIPS Table	219
ARTIFACT.ARTIFACTS Table	220
ARTIFACT.ARTIFACTSPHYSICALLOCATION Table	220
ARTIFACT.ARTIFACTUSAGEDETAILS Table	220
ARTIFACT.ARTIFACTUSAGESESSIONS Table	221
ARTIFACT.AUDIT_ACCESSC Table	222

ARTIFACT.AUDIT_ADMUSER Table	222
ARTIFACT.AUDIT_GROUP Table	222
ARTIFACT.AUDIT_TRANSACTIONS Table	223
ARTIFACT.AUDITACCESSCONTROLDETAIL Table	224
ARTIFACT.AUDITIM Table	224
ARTIFACT.DTINFOALL Table	225
ARTIFACT.LIBRARIES Table	225
ARTIFACT.SERVERTYPEBYUSER Table	225
ARTIFACT.SERVERUSAGEBYUSER Table	226
Solution Kits Table	226
KITS.EMI_INFO Table	226

About SAS Environment Manager Data Mart Tables

The following topics contain an overview of the use and contents of the tables in the SAS Environment Manager Data Mart. Although the topics list the columns in the tables that contain metric or inventory information, the tables also contain other columns that are not listed. Those columns provide information such as the date and time that a metric was recorded, the ID and name of the involved resource, and the time zone offset and shift for when the metric was recorded.

The columns listed for each table represent the metric and inventory data that is collected by default. If you use SAS Environment Manager to start collecting data for a metric that is not currently activated, a column for the new metric appears in the appropriate table. If you stop collecting data for a metric, the corresponding column remains in the data table because the SAS Environment Manager Data Mart retains 45 days of historical data. The column for the deactivated metric remains in the table even after 45 days have passed, although the column is blank.

ACM Tables

These tables are located in the directory `[levelroot]/Web/SASEnvironmentManager/emi-framework/Datamart/acm`.

ACM.AVAILABILITY Table

The ACM.AVAILABILITY table contains data about resource availability.

By default, this table contains the following metric data columns:

avail	endtime
starttime	minutes

ACM.FILEMOUNTS Table

The ACM.FILEMOUNTS table contains usage data for the file mounts in your SAS environment. If the feed to SAS Visual Analytics is enabled, this table is copied to the drop zone.

By default, this table contains the following metric data columns:

diskWrites1m	DiskQueue
diskReads1m	DiskSeviceTime
UsePercent	DiskReadBytes1m
TotFsFree	DiskWriteBytes1m
Capacity	

ACM.GROUPINVENTORY Table

The ACM.GROUPINVENTORY table contains data about the resource groups that are defined in SAS Environment Manager. If the feed to SAS Visual Analytics is enabled, this table is copied to the drop zone.

By default, this table contains the following inventory columns:

id	desc
name	

ACM.EVENTS Table

The ACM.EVENTS table contains data about the events that are logged by SAS Environment Manager.

By default, this table contains the following metric data columns:

msg	resource_id
fixdate	status
datetime	what
duration	who
eventType	

ACM.HOSTPLATFORMS Table

The ACM.HOSTPLATFORMS table contains metrics for the platforms. If the feed to SAS Visual Analytics is enabled, this table is copied to the drop zone.

By default, this table contains the following metric data columns:

MemFree	PercentUsedSwap
SwapUsed	ZombieProcesses
CpuUsage	PercentFreeSwap
LoadAverage1	RunningProcesses
CpuSoftLrq	TcpInErrs1m
CpuStolen	SwapPagesOut1m
SwapFree	TcpPassiveOpens1m
TotalProcesses	TcpRetransSegs1m
CpuLrq	Commit1m

CpuSys	Write1m
CpuNice	TcpEstabResets1m
TcpOutboundConnections	Read1m
CpuIdle	TcpOutRsts1m
LoadAverage2	TcpAttemptFails1m
MemUsed	TcpActiveOpens1m
ActualMemUsed	SwapPagesIn1m
PercentFreeMemory	Access1m
PercentUsedMemory	FileSystemReadsWrites1m
CpuUser	SwapTotal
LoadAverage0	ActualMemFree
CpuWait	NumCPUs
TcpInboundConnections	MemTotal

ACM.HTTPCHECKS Table

The ACM.HTTPCHECKS table contains metric data for HTTP checks of web services. If the feed to SAS Visual Analytics is enabled, this table is copied to the drop zone.

By default, this table contains the following metric data columns:

AllInboundConnections	ResponseTime
InboundConnections	OutboundConnections
AllOutboundConnections	ResponseCode
StateTIME_WAIT	LastModified

ACM.IOMSERVERS Table

The ACM.IOMSERVERS table contains metric data for SAS IOM server resources. If the feed to SAS Visual Analytics is enabled, this table is copied to the drop zone.

By default, this table contains the following metric data columns:

ServerState	NumProcesses
UnauthorizedAccesses	TotalClients1m
LastAccessState	CurrentClients
CurrentRunningServers_Local	Usage
ActivePeers	ResidentMemSize
CurrentPendingClients	MemSize
TotalWaitingTime	TotalTime1m
CurrentWaitingClients	UserTime1m
CurrentConnectedClients	SystemTime1m
TotalTimedOutClients	TimeInCalls1m
CurrentWaitingClients_Local	TotalCalls1m
CurrentRunningServers	

ACM.MEASUREINVENTORY Table

The ACM.MEASUREINVENTORY table contains data about the measurements that are being performed.

By default, this table contains the following inventory columns:

measurement_id	UNITS
resource_id	type
enabled	MONITORABLE_TYPE_ID
NAME	category
PLUGIN	resource_desc
ALIAS	deleted

ACM.METADATASVRS Table

The ACM.METADATASVRS table contains metric data for the SAS Metadata Servers in the environment. If the feed to SAS Visual Analytics is enabled, this table is copied to the drop zone.

By default, this table contains the following metric data columns:

serverState	ProcessShare
ProcessEnd_Last_Time	SystemTime
HighestThreadCount	health
ProcessStartTime	UserTime
CurrentClients	ProcessThreads
ProcessUserID	Usage
ProcessGroupID	ProcessMajorFaults
CounterJournalSpaceAvailable	TotalCalls1m
HighestMemoryUsage	CounterJournalDataWrite1m
CurrentThreadCount	ProcessPageFaults1m
CurrentMemoryUsage	CounterJournalTransProcessed1m
TotalClients1m	ProcessMinorFaults1m
ProcessResidentMemorySize	TimeInCalls1m
TotalTime	CounerJournalTransQueued1m
ProcessVirtualMemorySize	

ACM.NETWORKINTERFACE Table

The ACM.NETWORKINTERFACE table contains metric data for the network performance in your environment. If the feed to SAS Visual Analytics is enabled, this table is copied to the drop zone.

By default, this table contains the following metric data columns:

BitsIn1s	RxDropped1m
PacketsOut1m	BytesOut1m
BitsOut1m	TxCollisions1m
PacketsOut1m	TxDropped1m
RxErrors1m	BytesIn1m
TxErrors1m	

ACM.RESOURCEINVENTORY Table

The ACM.RESOURCEINVENTORY table contains information about the resources in the SAS Environment Manager inventory. If the feed to SAS Visual Analytics is enabled, this table is copied to the drop zone.

By default, this table contains the following inventory columns:

name	invLevel
type	

ACM.TCSSERVERMGRS Table

The ACM.TCSSERVERMGRS table contains metric data for tcServers in the system. If the feed to SAS Visual Analytics is enabled, this table is copied to the drop zone.

By default, this table contains the following metric data columns:

rejectedSessions1m	activeSessions
sessionCreateRate	sessionExpireRate
sessionAverageAliveTime	processingTime

ACM.WEBAPPSERVER Table

The ACM.WEBAPPSERVER table contains metric data for SAS web applications. If the feed to SAS Visual Analytics is enabled, this table is copied to the drop zone.

By default, this table contains the following metric data columns:

HeapMemoryMax	HeapMemoryUsed
HeapMemoryFree	DeadlocksDetected
PercentUpTimeinGarbageCollection	OpenFileDescriptionCount
Uptime	ThreadCount1m
HeapMemoryCommitted	

ACM.WIPDATADB Table

The ACM.WIPDATADB table contains metric data for the SAS Web Infrastructure Platform. If the feed to SAS Visual Analytics is enabled, this table is copied to the drop zone.

By default, this table contains the following metric data columns:

DataSpaceUsed	seq_scan1m
idx_tup_read1m	idx_blks_read1m
tup_fetched1s	xact_rollback1s
numbackends	xact_commit1s
blks_hit_p	blks_read1s
granted_locks	tup_altered1s

APM Tables

These tables are located in the directory `[levelroot]/Web/SASEnvironmentManager/emi-framework/apm/Data/artifacts`.

ARTIFACT.RELATIONSHIPS Table

The ARTIFACT.RELATIONSHIPS table contains information about the relationships between artifacts that are defined in other tables.

By default, this table contains the following metric data columns:

artifact1	relationshipSubType
artifact2	distance
relationshipType	_loadtm

ARTIFACT.ARTIFACTS Table

The ARTIFACT.ARTIFACTS table contains information about the artifacts (such as libraries, directories, and stored processes) in your environment.

By default, this table contains the following metric data columns:

ID	type
Name	_loadtm
Desc	path
Created	physicalPath
Updated	

ARTIFACT.ARTIFACTSPHYSICALLOCATION Table

The ARTIFACT.ARTIFACTSPHYSICALLOCATION table contains information about the physical location of artifacts.

By default, this table contains the following metric data columns:

ID	type
Name	_loadtm
Desc	path
Created	physicalPath
Updated	directoryName

ARTIFACT.ARTIFACTUSAGEDETAILS Table

The ARTIFACT.ARTIFACTUSAGEDETAILS table contains usage information about artifacts. If the feed to SAS Visual Analytics is enabled, this table is copied to the drop zone.

By default, this table contains the following metric data columns:

HostName	elapsedUserCPUTime
TotalIOCount	hour
TotalMemoryUsage	level
_loadtm	measurementSubType
artifact	measurementType
artifactType	minute
client_context	parentUsage
currentUsage	sourceId
datetime	startSystemCPUTime
datetimeMinute	startUserCPUTime
dayOfMonth	stopSystemCPUTime
dayOfWeek	stopUserCPUTime
elapsedSystemCPUTime	subType
elapsedTime	type
elapsedTotalCPUTime	usageId

ARTIFACT.ARTIFACTUSAGESESSIONS Table

The ARTIFACT.ARTIFACTUSAGESESSIONS table contains usage information about artifacts in a session. If the feed to SAS Visual Analytics is enabled, this table is copied to the drop zone.

By default, this table contains the following metric data columns:

HostName	hour
_loadtm	level
artifact	measurementType
artifactType	minute
client_context	parentUsage
currentUsage	sourceId
datetime	stopdt
datetimeMinute	subType

dayOfMonth	type
dayOfWeek	usageld
elapsedTime	

ARTIFACT.AUDIT_ACCESSC Table

The ARTIFACT.AUDIT_ACCESSC table contains audit records for object access events. If the feed to SAS Visual Analytics is enabled, this table is copied to the drop zone.

By default, this table contains the following metric data columns:

A_ACT_Message	A_ObjType
A_ActiveUserid	A_RecordEvent
A_IdentityName	A_RecordT
A_Level	A_Thread
A_ObjID	Log_Line

ARTIFACT.AUDIT_ADMUSER Table

The ARTIFACT.AUDIT_ADMUSER table contains audit information for the administrative user activities. If the feed to SAS Visual Analytics is enabled, this table is copied to the drop zone.

By default, this table contains the following metric data columns:

A_ActiveUserid	A_Thread
A_Level	Log_Line
A_RecordT	

ARTIFACT.AUDIT_GROUP Table

The ARTIFACT.AUDIT_GROUP table contains audit information for identity groups. If the feed to SAS Visual Analytics is enabled, this table is copied to the drop zone.

By default, this table contains the following metric data columns:

A_ActiveUserid	A_ObjID
A_IdentityName	A_ObjType
A_IdentityTargetName	A_RecordEvent
A_IdentityTargetObjID	A_RecordT
A_IdentityTargetType	A_Thread
A_IdentityType	Log_Line
A_Level	

ARTIFACT.AUDIT_TRANSACTION Table

The ARTIFACT.AUDIT_TRANSACTION table contains audit information for transactions. If the feed to SAS Visual Analytics is enabled, this table is copied to the drop zone.

By default, this table contains the following metric data columns:

A_ACT_Message	A_MetaUserid
A_ActiveUserid	A_ObjID
A_AuthDomain	A_ObjType
A_ClientID	A_PermissionName
A_ClientIPAddr	A_PermissionType
A_ClientPort	A_RecordEvent
A_IdentityName	A_RecordT
A_IdentityTargetName	A_Repository
A_IdentityTargetObjID	A_Thread
A_IdentityTargetType	Client_Context
A_IdentityType	Log_File
A_Level	Log_Line

ARTIFACT.AUDITACCESSCONTROLDETAIL
Table

The ARTIFACT.AUDITACCESSCONTROLDETAIL table contains detailed audit information about access requests. If the feed to SAS Visual Analytics is enabled, this table is copied to the drop zone.

By default, this table contains the following metric data columns:

A_ActiveUserid	Insert
A_ClientID	Read
A_ObjID	ReadMetadata
Administer	References
Alter_Table	Select
CheckInMetadata	Update
Create	User_Group
Create_Table	Write
Delete	WriteMemberMetadata
Drop_Table	WriteMetadata
Execute	

ARTIFACT.AUDITIM Table

The ARTIFACT.AUDITIM table contains audit information by time.

By default, this table contains the following metric data columns:

A_ActiveUserid	A_ObjID
ActionID	Path
Action	Map
ActionType	resourceType
SessionID	webApp

ARTIFACT.DTINFOALL Table

The ARTIFACT.DTINFOALL table contains information about log file access.

By default, this table contains the following metric data columns:

ArchiveLoc	file
_loactm	maxDT

ARTIFACT.LIBRARIES Table

The ARTIFACT.LIBRARIES table contains information about the SAS libraries in the environment.

By default, this table contains the following metric data columns:

libname	orapath
ServerContext	host
AuthDomain	install_loc
port	LASR_Name
tag	desc
hpath	libref
opt	engine
sqldatasrc	

ARTIFACT.SERVERTYPEBYUSER Table

The ARTIFACT.SERVERTYPEBYUSER table contains information about server access.

By default, this table contains the following metric data columns:

ServerType	description
ServerUser	sourceId
dayOfMonth	user

dayOfWeek

ARTIFACT.SERVERUSAGEBYUSER Table

The ARTIFACT.SERVERUSAGEBYUSER table contains usage information about SAS servers by user.

By default, this table contains the following metric data columns:

ServerType	description
ServerUser	sourceId
dayOfMonth	user
dayOfWeek	

Solution Kits Table

This table is located in the directory `[levelroot]/Web/SASEnvironmentManager/emi-framework/Datamart/kits`.

KITS.EMI_INFO Table

The KITS.EMI_INFO table contains metrics for SAS Environment Manager ETL processes. If the feed to SAS Visual Analytics is enabled, this table is copied to the drop zone.

By default, this table contains the following metric data columns:

logfile	blkinput
stepname	blkoutput
step	obsin
hostname	obsout
portdate	varsout
platform	memused

scp	osmem
realtime	sumsize
usertime	sortsize
systime	memsize
pageflt	jobname
pagercl	stepcnt
pageswp	pid
osvconsw	parm
osiconsw	

Recommended Reading

Here is the recommended reading list for this title:

- The online Help for SAS Environment Manager 2.4.
- *SAS Intelligence Platform: Middle-Tier Administration Guide.*
- *SAS Intelligence Platform: System Administration Guide.*
- *SAS Logging: Configuration and Programming Reference*

For a complete list of SAS publications, go to sas.com/store/books. If you have questions about which titles you need, please contact a SAS Representative:

SAS Books

SAS Campus Drive

Cary, NC 27513-2414

Phone: 1-800-727-0025

Fax: 1-919-677-4444

Email: sasbook@sas.com

Web address: sas.com/store/books

Index

A

access control templates 181
 access permissions 86
 See also [roles](#)
 creating middle-tier
 administrator IDs 88
 access to data
 fine-grained, using permission
 conditions 167
 Active MQ 60
 ACTs
 See [access control templates](#)
 administrative tasks 23
 administrator IDs, SAS middle
 tier 88
 administrators
 Administer permission 165
 intermittent 140
 agents 5
 Alert Center 18, 75
 alerts
 default definitions for 25
 defining 77
 examples of defining 200
 monitoring with Alert Center
 18, 75
 responding with control
 actions 67

Analyze pages 17
 Apache Tomcat 60
 applications 63
 authentication 24, 86
 authentication domains 146
 authorization 24, 86
 Auto-Discovery portlet 29
 using 52
 automatic discovery of
 resources 51
 rediscovering resources 53
 running an auto-discovery
 scan 53
 availability of resources 58
 Availability Summary portlet 29

C

capabilities 142
 Cisco IOS 9
 clearing the auto-discovery
 queue 53
 clusters
 monitoring with Resources
 pages 15
 compatible groups 63
 components of SAS
 Environment Manager 5

- configuration 24
 - escalation schemes 25, 80
 - manually configuring a service 55
 - of resources for data
 - collection 52
 - plugins 25
- control actions 65
 - in response to an alert 67
 - scheduling 66
- Control Actions portlet 29
- customizing a Dashboard 31

D

- Dashboard 14, 28
 - customizing 31
 - for native roles 84
- database, SAS Environment Manager 6
- default ACT
 - See [repository ACT](#)
- discovering resources
 - automatically
 - See [automatic discovery of resources](#)

E

- escalation schemes, configuring 25, 80
- events

- monitoring with Event Center 19, 69

F

- Favorite Resources portlet 29
- fine-grained access to data
 - using permission conditions 167

G

- GemFire Distributed System 9
- Groovy Console 25
- Group Alerts Summary portlet 30
- groups 141
 - creating 64
 - DBMS access 155
 - monitoring with Resources
 - pages 15
 - types 62

H

- HQ Agent 60
- HQ Health 25
- HQ Web Services API 25
- Hyperic 4, 60

I

identity precedence [164](#)
 interface, SAS Environment
 Manager [14](#)
 Administration page [23](#)
 Alert Center [18](#)
 Analyze pages [17](#)
 Dashboard [14](#), [28](#)
 Event Center [19](#)
 Manage page [24](#)
 Operations Center [20](#)
 Resources pages [15](#)
 internal accounts [145](#)

L

license usage [25](#)
 logins [143](#)
 qualifying Windows user IDs
 in [143](#)
 uniqueness requirement [148](#)

M

Manage page [24](#)
 management server [5](#)
 Map control [60](#)
 members [142](#)
 metadata
 viewing in Administration page
 [23](#)
 Metric Viewer portlet [30](#)

middle-tier administrator IDs [88](#)
 mixed groups [63](#)
 monitoring
 availability of resources [58](#)
 default definitions for [25](#)
 licences [25](#)
 platforms, servers, and
 services [15](#)
 resource events and alerts
 [17](#), [69](#)
 using portlets on Dashboard
 [28](#)
 using Resources pages [57](#)
 using the Map control for
 servers and services [60](#)

N

native roles
 See [roles](#)
 Network and Host Dependency
 Manager [25](#)
 Network Device [9](#)
 Network Host [9](#)
 network platforms [9](#)

O

operating system platforms [8](#)
 Operations Center [20](#)

P

passwords 147

permissions 164
 See also [access permissions](#)
 inheritance 163

platforms 8
 monitoring with Resources
 pages 15
 supported 9

plugins 6
 configuring 25

portlets
 adding to Dashboard 31
 on Dashboard 28

PostgreSQL 60
 controlling with control actions
 65

Problem Resources portlet 30

R

Recent Alerts portlet 29

Recently Added portlet 29

repository ACT 161

resource groups 63

resource inventory model 8
 platforms 8
 servers 9
 services 10

resources
 automatically discovering 51
 availability 58

 configuring for data collection
 52

 controlling with control actions
 65

 manually adding to inventory
 54

 monitoring alerts 17, 75

 monitoring events 19, 69

 monitoring with Dashboard
 portlets 28

 monitoring with Operations
 Center 20

 monitoring with Resources
 pages 15, 57

 organizing into groups 62

 platforms 8

 rediscovering 53

 running an auto-discovery
 scan 53

 servers 9

 services 10

Resources pages 15, 52, 57

roles 141
 creating native roles 87
 Dashboard pages 84
 managing with Manage page
 24
 native 84

S

SAS Application Server 9

SAS Application Server Tier
 platform 9

- SAS Environment Manager
 - access permissions 86
 - components 5
 - configuring 24
 - interface 14
 - overview 3
- SAS Environment Manager
 - Agent server 60
- SAS Environment Manager
 - database 6
- SAS Environment Manager
 - server 60
- SAS JMS Broker 60
- SAS Logon Manager 86
- SAS Metadata Server 9, 23
 - controlling with control actions 65
- SAS Object Spawner
 - controlling with control actions 65
- SAS OLAP Server 9
 - controlling with control actions 65
- SAS Stored Process Server 9
- SAS Web Application Server 60
 - controlling with control actions 65
- SAS Web Infrastructure
 - Platform Data Server 60
 - controlling with control actions 65
- SAS Web Server 60
- SAS Workspace Server 9
- Saved Charts portlet 29
- scanning for resources 53
- scheduling control actions 66
- Search Resources portlet 29
- servers 9
 - Active MQ 60
 - Apache Tomcat 60
 - controlling with control actions 65
 - determining server names 60
 - HQ Agent 60
 - management server 5
 - managing settings with
 - Manage page 24
 - manually adding to inventory 54
 - monitoring with Map control 60
 - monitoring with Resources
 - pages 15
 - PostgreSQL 60, 65
 - SAS Application Server 9
 - SAS Environment Manager 60
 - SAS Environment Manager
 - Agent 60
 - SAS JMS Broker 60
 - SAS Metadata Server 9, 23, 65
 - SAS OLAP Server 9, 65
 - SAS Stored Process Server 9
 - SAS Web Application Server 60, 65
 - SAS Web Infrastructure
 - Platform Data Server 60, 65
 - SAS Web Server 60

- SAS Workspace Server 9
- SpringSource tc Runtime 60, 65
- vFabric Web Server 60
- services 10
 - controlling with control actions 65
 - manually adding to inventory 55
 - monitoring with Map control 60
 - monitoring with Resources pages 15
- SpringSource tc Runtime 60
 - controlling with control actions 65
- Summary Counts portlet 30
- supported platforms 9

T

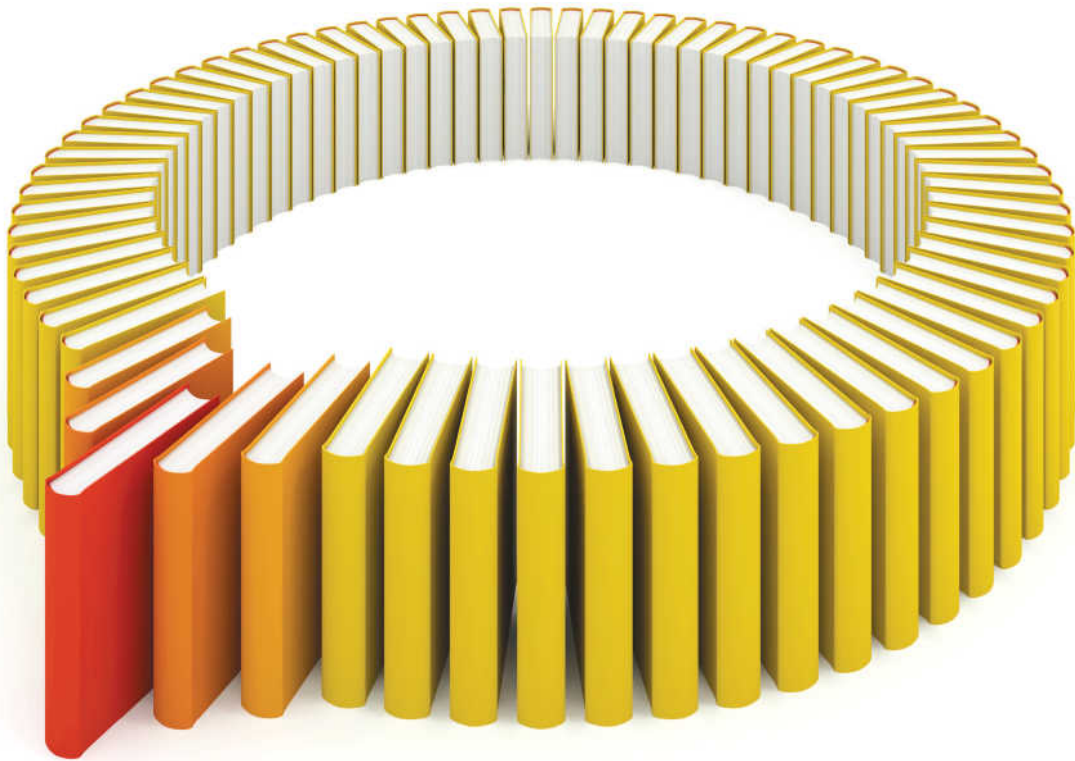
- tc Server Command-line Interface 25

U

- user administration 139
- user IDs
 - qualifying in logins 143
 - uniqueness requirement 148
- users 140
 - access permissions 86
 - creating middle-tier administrator IDs 88
 - DBMS access 155
 - dual 140
 - intermittent administrators 140
 - managing with Manage page 24

V

- vFabric Web Server 60
- virtual platforms 9
- VMWare Hyperic 4, 60
- VMware vSphere Host 9
- VMware vSphere VM 9



Gain Greater Insight into Your SAS® Software with SAS Books.

Discover all that you need on your journey to knowledge and empowerment.

