SAS® High-Performance Computing Management Console 2.6
User’s Guide
Gain Greater Insight into Your SAS® Software with SAS Books.

Discover all that you need on your journey to knowledge and empowerment.

support.sas.com/bookstore for additional books and resources.
## Contents

*What’s New in SAS High-Performance Computing Management Console* ........................................................................................................ vii

*Accessibility Features of the SAS High-Performance Computing Management Console* ......................................................................................... ix

### Chapter 1 • Overview of the Console

- About the Console ........................................................................................................ 1
- Accessing the Console .................................................................................................... 1
- Specifying Console Preferences ..................................................................................... 2
- Configuring Console Network Settings ........................................................................ 5
- Configuring the Default Language ............................................................................... 7
- Configuring Console Logging ...................................................................................... 9

### Chapter 2 • Managing Console Users and Groups

- Managing Console Users and Groups ........................................................................ 11
- Force Off Console Sessions ......................................................................................... 20

### Chapter 3 • Viewing Console Logs

- View Logs for an Active Session .................................................................................. 21
- Search Console Logs ..................................................................................................... 22
- Understanding Log Details .......................................................................................... 23

### Chapter 4 • Managing Users and Groups

- About Managing Users and Groups ........................................................................... 27
- Managing Users and Groups ....................................................................................... 28
- Managing User Sessions .............................................................................................. 36
- Perform an SSH Lockout .............................................................................................. 38

### Chapter 5 • Managing Database Resources

- Managing Active Queries and Connections ................................................................ 43
- Managing Temporary Tables ...................................................................................... 47
Chapter 6 • Managing Cube Data Files
Understanding the Cube Cleanup Feature
Specifying the Directory to Manage
Searching for Cube Data Files
Deleting Cube Data Files

Chapter 7 • Managing CPU and Memory Resources
Understanding the CGroup Resource Management Feature
About Resource Allocation
CGroups Resource Management Page
Creating a Control Group
Editing and Deleting Control Groups
Example: Resource Management
CGroup Resource Management Administration

Chapter 8 • Gridhosts File Management
What Is the Gridhosts File?
Managing the Gridhosts File

Chapter 9 • Managing Simultaneous Utilities Machine Groups
Understanding the Groups
Creating a Group
Editing and Deleting Sim Groups

Chapter 10 • Simultaneous Shell Utilities
Simultaneous Shell Command
Simultaneous Copy Command

Index
What’s New

What’s New in SAS High-Performance Computing Management Console

Overview

SAS High-Performance Computing Management Console 2.6 removes support for managing memory resources from the **CGroup Resource Management** tab. Information about preserving the CPU share settings before you upgrade is provided in *SAS High-Performance Analytics Infrastructure: Installation and Configuration Guide*.
Accessibility Features of the SAS High-Performance Computing Management Console

Overview

SAS High-Performance Computing Management Console has not been tested for compliance with U.S. Section 508 standards and W3C web content accessibility guidelines. If you have specific questions about the accessibility of SAS products, send them to accessibility@sas.com or call SAS Technical Support.

Documentation Format

Please contact accessibility@sas.com if you need this document in an alternative digital format.
Using Assistive Technology via a Remote Server

If you have questions about running SAS High-Performance Computing Management Console and operating assistive technology via a remote server such as Citrix, contact your assistive technology vendor.

User Interface Layout

The application window contains two sections:

- The top of the window contains a toolbar with links for **Console Management** and **HPC Management** on the left and a **Log Off** link on the right side.
- The center of the window contains the workspace. The workspace contains links for the modules that apply to either console management or HPC management.

For information about using the console management features, see **“Managing Console Users and Groups”** on page 11. For information about using the HPC management features, see **“Managing Users and Groups”** on page 27.
About the Console

The SAS High-Performance Computing Management Console is a web application that is used by system administrators to manage high-performance computing environments that use SAS software. Maintaining high-performance computing (HPC) environments is challenging because of the large number of machines that are used in the distributed computing environment. In order to ensure peak performance and reliability, whatever action is taken on one machine must be performed on all the machines. Tasks that might be simple on a single machine, such as adding a user or changing a system configuration option, become more challenging in a distributed computing environment. Most changes must be propagated to the other machines and this can be labor
intensive and time consuming. The console is used to ease the administration of the environment.

The console includes its own embedded web server, When administrators log on to the console, where authentication occurs is determined by the user name provided. If the user name matches an operating system user account, then the operating system performs authentication. If the user name does not match an operating system user account, then the console performs authentication. In either case, the console does not perform any interaction with the SAS Metadata Server.

Accessing the Console

You can access the console with either of the following methods:

- Follow a web link or enter the URL to access the console directly. For example, you might enter http://hostname.example.com:10020. If the console was installed with SSL enabled, then enter HTTPS as the protocol.

- For SAS Visual Analytics deployments, you can access the console by selecting Tools ▶ SAS HPC Management Console from SAS Visual Analytics Administrator. Log on with a console user account. For more information about console user accounts, see “Managing Console Users and Groups” on page 11.

Specifying Console Preferences

Specifying User Interface Preferences

To specify your preferences:

1. Click Console Management from the toolbar.

2. Click Console Configuration and then click User Interface.
The most important setting is to make sure that the **HPC Environment being managed** menu is set appropriately. This menu choice determines the features that are presented in the console.

The following table identifies the options that are available:

**Table 1.1  SAS High-Performance Computing Management Console User Interface Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Page background</td>
<td>Specify the color to use for each of these options as the RGB hexadecimal code for a color.</td>
</tr>
<tr>
<td>Normal text</td>
<td></td>
</tr>
<tr>
<td>Table background</td>
<td></td>
</tr>
<tr>
<td>Table header</td>
<td></td>
</tr>
<tr>
<td>Link text</td>
<td></td>
</tr>
<tr>
<td>Display titles as text</td>
<td>Specifies whether any title is displayed as text in the console. The default value is <strong>No</strong>.</td>
</tr>
<tr>
<td>Display user ID and hostname for non-framed themes</td>
<td>Specify the location of the client login and host name when non-framed themes are used. Use the menu to select a choice. The default value is <strong>At bottom of browser</strong>.</td>
</tr>
<tr>
<td>Hostname to display in the console</td>
<td>This option enables you to specify the how the host name for the SAS High-Performance Computing Management Console is displayed to clients. Use the menu to select a choice. The default value is <strong>Real hostname</strong>.</td>
</tr>
<tr>
<td>Prefix user ID to page titles</td>
<td>Specify whether the user name or host name of the connected user appears in the page title bar of the web browser.</td>
</tr>
<tr>
<td>Prefix host name to page titles</td>
<td></td>
</tr>
<tr>
<td>Date format</td>
<td>Specify how the date is displayed in the console. Use the menu to select a choice. The default value is <strong>dd/mon/yyyy</strong>.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>File chooser size</td>
<td>Specify the size (in pixels) to use for the dialog box for each of these options. The default value is to use the minimum number of pixels that are needed to display the contents of the dialog box.</td>
</tr>
<tr>
<td>User chooser size</td>
<td></td>
</tr>
<tr>
<td>Multiple users chooser size</td>
<td></td>
</tr>
<tr>
<td>Date selector size</td>
<td></td>
</tr>
<tr>
<td>Module chooser size</td>
<td></td>
</tr>
<tr>
<td>Multiple modules chooser size</td>
<td></td>
</tr>
<tr>
<td>HPC Environment being managed</td>
<td>Specify the environment type.</td>
</tr>
<tr>
<td>Note: For SAS Visual Analytics</td>
<td>deployments, select a menu item that includes SAS LASR Analytic Server.</td>
</tr>
<tr>
<td>Console server host name in /etc/</td>
<td>Specify the host name for the machine that is used for running the SAS High-Performance Computing Management Console. Enter the host name exactly as it appears in the /etc/gridhosts file.</td>
</tr>
<tr>
<td>gridhosts</td>
<td></td>
</tr>
</tbody>
</table>

4 Click **Save**.

**Changing Your Console Password**

Console users can also change their own passwords. This feature is for console users that do not use an operating system user ID to log on to the console.

To change your password:

1 Click **Console Management** from the toolbar.

2 Click **Language and Password**.

3 The following table identifies the options that are available:
### Table 1.2 Change Language and Password Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Console UI language</td>
<td>To specify a language, select <strong>Personal choice</strong> and then select a language.</td>
</tr>
<tr>
<td>Management Console login password</td>
<td>To change your password, select <strong>Set to</strong> and then specify your new password in the text field and the <strong>Re-enter password</strong> field. The default is <strong>Leave unchanged</strong>.</td>
</tr>
</tbody>
</table>

4. Click **Make Changes**.

The change is immediate and the console does not need to be restarted for the change to take effect.

---

**Configuring Console Network Settings**

By default, the server process for the SAS High-Performance Computing Management Console listens on port 10020 and on all IP addresses for the machine on which it is installed. However, the port and address settings are configurable.

**Note:** In a SAS Visual Analytics deployment, do not change the port number.

To specify the port and address settings:

1. Click **Console Management** from the toolbar.

2. Click **Console Configuration** and then click **Console Server Network Configuration**.

3. The following table identifies the options that are available:
**Table 1.3  SAS High-Performance Computing Management Console Ports and Addresses Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Listen on specified IP addresses and port numbers</strong></td>
<td>Select the <strong>Only Address</strong> option and specify an IP address to restrict the console to listen for connections on the specified IP address only. The default value is <strong>Any Address</strong>. Specify a port number in the <strong>Port Number</strong> field. The default value is 10020.</td>
</tr>
<tr>
<td><strong>Accept IPv6 connections</strong></td>
<td>Specifies whether the console accepts IPv6 connections. The default value is <strong>No</strong>.</td>
</tr>
<tr>
<td><strong>Listen for broadcasts on UDP port</strong></td>
<td>Specify whether to listen for UDP broadcasts from other console installations. Available options are <strong>Don't Listen</strong> or a specified port. The default value is to listen on port 10020. This option is not used at this time.</td>
</tr>
<tr>
<td><strong>Console server host name</strong></td>
<td>Specify how the console server determines its host name. Available options are <strong>Work out from browser</strong> or specifying a host name. The default value is to determine it from the web browser.</td>
</tr>
<tr>
<td><strong>Reverse-resolve client IP address</strong></td>
<td>Specify whether the IP addresses of the client machines are resolved to host names. The default value is <strong>Yes</strong>.</td>
</tr>
</tbody>
</table>

4 Click **Save**.
Configuring the Default Language

To specify the default language for the console:

1. Click **Console Management** from the toolbar.

2. Click **Console Configuration** and then click **Language**.

3. The following table identifies the options that are available:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Language</strong></td>
<td>Use the menu to select a default language for the console.</td>
</tr>
<tr>
<td><strong>Character set for HTML pages</strong></td>
<td>Specify the character set that the console uses for sending HTML to the web browser. Some sample values are ASCII, ISO-8859-1, and ISO-2022-JA. The default is <strong>UTF-8</strong>.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Use the language that is specified by the client Web browser? | If you set this value to **Yes**, then the console changes the language if one of the following locales is detected from the browser:  
  - en: English  
  - it: Italian  
  - fr: French  
  - de: German  
  - es: Spanish  
  - pl: Polish  
  - ja_JP: Japanese  
  - ko_KR: Korean  
  - zh_TW: Traditional Chinese  
  - zh_CN: Simplified Chinese |

4. Click **Change Language**.

The change is immediate and the console does not need to be restarted for the change to take effect.
Configuring Console Logging

To configure logging settings:

1. Click **Console Management** from the toolbar.

2. Click **Console Configuration** and then click **Logging**.

3. The following table identifies the options that are available:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging Enabled</td>
<td>Select <strong>Disable logging</strong> or <strong>Enable logging</strong>. The default value is <strong>Enable logging</strong>.</td>
</tr>
<tr>
<td>Log resolved hostnames?</td>
<td>Specifies whether to log host names in the logs. The default value is <strong>No</strong>.</td>
</tr>
<tr>
<td>Use combined log format (including referrer and user agent)?</td>
<td>Specifies whether a combined log format is used. The default value is <strong>No</strong>.</td>
</tr>
<tr>
<td>Periodically clear log files?</td>
<td>Specify the interval to use for clearing log files. The default value is not to clear log files.</td>
</tr>
<tr>
<td>Users to log</td>
<td>Specify the user accounts to record in log reports. The default is <strong>Log actions by all users</strong>.</td>
</tr>
<tr>
<td>Modules to log</td>
<td>Specify the modules to log. The default is <strong>Log actions in all modules</strong>.</td>
</tr>
<tr>
<td>Include Console logins and logouts in actions log?</td>
<td>Specify whether logon to and logoff actions from the console are logged. The default value is <strong>No</strong>.</td>
</tr>
<tr>
<td>Log changes made to files by each action?</td>
<td>Specify whether changes that are made to files are logged. The default value is <strong>No</strong>.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Record all modified files before actions, for rollbacks?</td>
<td>Specify whether modified file changes are recorded for possible rollback. The default value is <strong>No</strong>.</td>
</tr>
<tr>
<td>Permissions for log files</td>
<td>Specify the mode permissions for the log files. The default setting is 600 and owned by root.</td>
</tr>
<tr>
<td>Add log to syslog?</td>
<td>Specify whether actions are logged to syslog in addition to log files. The default value is <strong>No</strong>.</td>
</tr>
</tbody>
</table>

4  Click **Save**.
An important concept to understand is that the SAS High-Performance Computing Management Console manages two types of users and groups. The first type is for console users and groups. This provides access control for the user accounts that can use the SAS High-Performance Computing Management Console. The second type of users and groups are the operating system users and groups. The console does assist with managing these users and groups. For information about managing operating system users and groups with the console, see “Managing Users and Groups” on page 27.
The following display shows the interface for managing console users and groups. The links for creating new console users and new console groups are highlighted.

**Display 2.1  Console Users and Groups Management**

Create a Console User

Be aware that a console user is not the same as a user that is created in the **HPC Management** section of the console. Console users are created strictly for using the console. The Users and Groups module in the **HPC Management** section manages the operating system users and groups.

To create a console user:

1. Click **Console Management** from the toolbar.
2. Click **Console Users and Groups**.
3. Click **Create a new console user**.
The following display shows the Create console user screen.

*Display 2.2  Create Console User*

The following table describes the additional fields on the Create console user screen. They become available after clicking **Security and limits options** or **Available console modules**.

*Table 2.1  Create Console User Field Descriptions*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Specify the user account.</td>
</tr>
<tr>
<td>Member of group</td>
<td>Use the menu to select a group.</td>
</tr>
<tr>
<td>Note: The menu becomes available after you add a console group.</td>
<td></td>
</tr>
</tbody>
</table>
Specify the password for the console user. The menu offers the following choices:

**Set to**
sets the password to the value entered into the text field.

**Unix authentication**
passes the authentication request to the operating system.

**No password accepted**
locks the user out of the system.

(Optional) Specify an alternative description for the console user.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password</strong></td>
<td>Specify the password for the console user. The menu offers the following choices:</td>
</tr>
</tbody>
</table>
|                     | **Set to**
|                     | sets the password to the value entered into the text field.                                             |
|                     | **Unix authentication**
|                     | passes the authentication request to the operating system.                                             |
|                     | **No password accepted**
|                     | locks the user out of the system.                                                                     |
| **Real name**       | (Optional) Specify an alternative description for the console user.                                    |

4 Click **Create**.

The following table describes the additional options for creating a user.

**Table 2.2 Create Console User Options**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Language</strong></td>
<td>Leave this option set to <strong>Default</strong>. English is the only supported language for this release.</td>
</tr>
<tr>
<td><strong>Inactivity logout time</strong></td>
<td>Specify an inactivity time-out. The default is no time-out.</td>
</tr>
<tr>
<td><strong>Minimum password length</strong></td>
<td>Specify the minimum number of characters for the user’s password. The default is no minimum length.</td>
</tr>
<tr>
<td><strong>IP access control</strong></td>
<td>Select the option that meets the security requirements for the environment. If <strong>Deny from listed addresses</strong> is selected, then be aware that the console user can log on from any IP address that is not listed. The default value is <strong>Allow from all addresses</strong>.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allowed days of the week</td>
<td>Specify the days of the week on which the console user is permitted to log on. The default value is <strong>Every day</strong>.</td>
</tr>
<tr>
<td>Allowed times of the day</td>
<td>Specify the range of hours during which the console user can log on. The default value is <strong>Any time</strong>.</td>
</tr>
<tr>
<td>Console Configuration</td>
<td>Select this check box to enable the console user to configure console settings such as the user interface, network settings, and console logging.</td>
</tr>
<tr>
<td>Console Users and Groups</td>
<td>Select this check box to enable the console user to configure console users and groups. A best practice is to limit access to this feature. For more information, see “Best Practices for Managing Console Users and Groups” on page 19.</td>
</tr>
<tr>
<td>Console Logs</td>
<td>Select this check box to enable the console user to view and search the console logs. The console logs contain information about the actions performed with the console.</td>
</tr>
<tr>
<td>Language and Password</td>
<td>Select this check box to enable the console user to set the user’s own language preference and password.</td>
</tr>
<tr>
<td>Active Queries and Connections</td>
<td>Select this check box to enable the console user to view and terminate database queries and connections.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This option is available for environments that are configured to manage Greenplum Database deployments only.</td>
</tr>
<tr>
<td>Cube Cleanup</td>
<td>Select this check box to enable the console user to list and remove cube data files from the machines in the cluster.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This option is available for SAS High-Performance Risk environments only.</td>
</tr>
</tbody>
</table>
### Field | Description
---|---
**Gridhosts File Management** | Select this check box to enable the console user to modify the `/etc/gridhosts` file. This file is used to identify the machines in the HPC environment and is very important to the operation of SAS High-Performance Analytics environment and the console itself.

**Sim Groups** | Select this check box to enable the console user to add and manage the groups to use with the simultaneous utilities.

**Users and Groups** | Select this check box to enable the console user to manage the operating system user accounts in the HPC environment.

**CGroup Management** | Select this check box to enable the console user to manage CPU and memory resources.

**SSH Lockout** | Select this check box to enable the console user to use the SSH lockout feature.

**Temporary Table Maintenance** | Select this check box to enable the console user to view and drop temporary database tables.

**Note:** This option is available for environments that are configured to manage Greenplum Database deployments only.

Check boxes that are marked with an 'x' identify features that are enabled through group membership.

### Create a Console Group

To create a console group:

1. Click **Console Management** from the toolbar.

2. Click **Console Users and Groups**.
3 Click **Create a new console group**.

The following display shows the Create Console Group screen.

*Display 2.3*  *Create Console Group*

The following table describes the fields on the Create Console Group screen.

*Table 2.3*  *Create Console Group Field Descriptions*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group name</strong></td>
<td>Specifies the console group name.</td>
</tr>
<tr>
<td><strong>Group description</strong></td>
<td>Specifies a description for the console group.</td>
</tr>
<tr>
<td><strong>Member of users and groups</strong></td>
<td>When a console group that has members is edited, this field lists the members of the group.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Console Configuration</td>
<td>Select this check box to enable the members of the group to configure console settings such as the user interface, network settings, and console logging.</td>
</tr>
<tr>
<td>Console Users and Groups</td>
<td>Select this check box to enable members of the group to configure console users and groups. A best practice is to limit access to this feature. For more information, see “Best Practices for Managing Console Users and Groups” on page 19.</td>
</tr>
<tr>
<td>Console Logs</td>
<td>Select this check box to enable members of the group to view and search the console logs. The console logs contain information about the actions performed with the console.</td>
</tr>
<tr>
<td>Language and Password</td>
<td>Select this check box to enable members of the group to set their own language preferences and passwords.</td>
</tr>
<tr>
<td>Active Queries and Connections</td>
<td>Select this check box to enable members of the group to view and terminate database queries and connections.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This option is available for environments that are configured to manage Greenplum Database deployments only.</td>
</tr>
<tr>
<td>Cube Cleanup</td>
<td>Select this check box to enable members of the group to list and remove cube data files from the machines in the cluster.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This option is available for SAS High-Performance Risk environments only.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Gridhosts File Management</td>
<td>Select this check box to enable members of the group to modify the <code>/etc/gridhosts</code> file. This file is used to identify the machines in the HPC environment and is very important to the operation of SAS High-Performance Analytics software and the console itself.</td>
</tr>
<tr>
<td>Sim Groups</td>
<td>Select this check box to enable members of the group to add and manage the groups to use with the simultaneous utilities.</td>
</tr>
<tr>
<td>Users and Groups</td>
<td>Select this check box to enable members of the group to manage the operating system user accounts in the HPC environment.</td>
</tr>
<tr>
<td>SSH Lockout</td>
<td>Select this check box to enable members of the group to use the SSH lockout feature.</td>
</tr>
<tr>
<td>Temporary Table Maintenance</td>
<td>Select this check box to enable members of the group to view and drop temporary database tables.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This option is available for environments that are configured to manage Greenplum Database deployments only.</td>
</tr>
</tbody>
</table>

4. Click **Create**.

**Best Practices for Managing Console Users and Groups**

Console groups can be used to grant identical access rights to groups of users that share the same administration responsibilities. The **Console Users and Groups** module enables an administrator to manage the access permissions for console users. Limit access to this module because a user can change his access permissions and dilute the security of the SAS High-Performance Computing Management Console.
Force Off Console Sessions

The console enables administrators to force off other console users. To force off a console user:

1. Click **Console Management** from the toolbar.
2. Click **Console Users and Groups**.
3. Click **View Login Sessions** near the bottom of the page.
4. Select the session ID from the table to force off the console user. There is no confirmation prompt.

Display 2.4  SAS High-Performance Computing Management Console Current Login Sessions

Your session ID is shown in bold text.
Viewing Console Logs

View Logs for an Active Session .......................................................... 21
Search Console Logs ............................................................................ 22
Understanding Log Details ................................................................. 23

View Logs for an Active Session

Follow the steps described in “Force Off Console Sessions” on page 20. Instead of selecting the session ID, select View logs for the console user to monitor. The console uses the session ID to perform a search of the console logs. The following display shows an example of the search results:
Select the action to review and then review the details. For information about the details, see “Understanding Log Details” on page 23.

**Search Console Logs**

To search console logs:

1. Click **Console Management** from the toolbar.

2. Click **Console Logs**.

3. Specify the search criteria in the **Search the console log for actions** fields and click **Search**.

   **Note:** The **By non-console user** option does not work in a SAS Visual Analytics deployment.

4. Select the action to review and then review the details. For information about the details, see “Understanding Log Details” on page 23.
Understanding Log Details

The console logs record information such as the action that was performed, the module that was used, the date and time, and the parameters associated with the action. The information in these logs is valuable when reviewing the actions that were performed by a console user. In addition to viewing logs, the console enables an administrator to annotate the log record with comments.

The following display shows a console log example for starting an SSH lockout. The information that the console shows in most of the fields, and especially in the Raw log data section, differs according to which action is performed.

Display 3.2  Console Log Action Details

The Details of logged action section includes the following information:

Table 3.1  Console Log Details of Logged Action

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Specifies the action that was performed.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Console module</td>
<td>Specifies the console module that was used to perform the action.</td>
</tr>
<tr>
<td>Console user</td>
<td>Specifies the user name that performed the action.</td>
</tr>
<tr>
<td>Session ID</td>
<td>Specifies the web session that was used when the action was performed. You can select the link to view the console logs for all actions performed during the web session.</td>
</tr>
<tr>
<td>Generated by script</td>
<td>Specifies the console script that was used to perform the action.</td>
</tr>
<tr>
<td>Client IP or hostname</td>
<td>Specifies the IP address or host name that was used by the console user to perform the action.</td>
</tr>
<tr>
<td>Date and time</td>
<td>Specifies the date and time for when the action was performed. The date and time format can be changed by specifying a different format for displayed dates as described in “Specifying Console Preferences” on page 2.</td>
</tr>
</tbody>
</table>

The **Log entry annotation** section enables an administrator to save a comment about the action. Click **Save** after adding a comment.

The information in the **Raw log data** section differs according to the action that was performed. The information is shown as a two-column table of parameter names and parameter values. Most of the parameters are related to the descriptions provided in the previous table. However, the appearance of some fields is different. The following list describes those fields:

**sid**

This is the value for the web session ID that was in use when the action was performed.
time
This value is a UNIX time representation for when the action was performed. When the data and time are shown in the Details of logged action section, the time is formatted for display from this value.

id
This value is the identifier for the log record.

The Files changed and commands run section shows the operating system commands that were executed to perform the action and the files that were used. This section is populated when the console is configured to log such information. By default, the console is not configured to log commands and files because the list of commands can be large and can contribute to a full system disk.
About Managing Users and Groups

The SAS High-Performance Computing Management Console enables two types of management for users and groups. The first type, for console users and groups, is described in “Managing Console Users and Groups” on page 11. This section describes
the second type of user and group management, operating system users and groups. This management is performed with the High-Performance Computing (HPC) management section of the interface. It is also used to perform an SSH lockout. A lockout is used to limit access to machines in the cluster.

The following figure shows the interface for an administrator who has permission to perform HPC management only. The **Active Queries and Connections** and **Temporary Table Maintenance** modules apply to a SAS LASR Analytic Server with Greenplum environment only.

**Display 4.1  HPC Management Interface**

Managing Users and Groups

Understanding Users and Groups

The users and groups module is used to create, manage, and propagate operating system user accounts and groups throughout the machines in the cluster. It also enables an administrator to generate and distribute SSH keys for each user account. The key generation can be performed as the account is propagated to the machines in the cluster, or it can be performed on existing accounts.
The following display shows the interface for managing operating system users and groups.

**Display 4.2  Managing Users and Groups**

The **HPC Users** tab shows the following information for each user account:

**Table 4.1  User Accounts Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Specifies the user account name.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If the name is displayed in italics, then the account has a null password.</td>
</tr>
<tr>
<td>User ID</td>
<td>Specifies the UID for the user account.</td>
</tr>
<tr>
<td>Group</td>
<td>Specifies the primary group for the user account.</td>
</tr>
<tr>
<td>Real name</td>
<td>Specifies details about the user that make the user account more identifiable.</td>
</tr>
<tr>
<td>Home directory</td>
<td>Specifies the home directory for the user account.</td>
</tr>
</tbody>
</table>
Configuring the Middle-Tier Shared Key

Configuring a middle-tier shared key for SAS Visual Analytics deployments is no longer necessary beginning with the 6.1 release.

Create a User

To create a user:

1. Click **HPC Management** from the toolbar.
2. Click **Users and Groups**.
3. Click **Create a new user** and specify values for the following fields:

   **Table 4.2  Create User Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Specify the user account name, such as madupr or team1usr.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>User ID</td>
<td>Select an option:</td>
</tr>
<tr>
<td></td>
<td><strong>Automatic</strong></td>
</tr>
<tr>
<td></td>
<td>the operating system selects an unused UID.</td>
</tr>
<tr>
<td></td>
<td><strong>Calculated</strong></td>
</tr>
<tr>
<td></td>
<td>(rarely used) the UID is created based on a Berkeley CRC and mkuid. The mkuid command assumes a standard naming convention for user names.</td>
</tr>
<tr>
<td></td>
<td><strong>Specified</strong></td>
</tr>
<tr>
<td></td>
<td>specify the UID to use. By default, this field shows the UID that is assigned if the <strong>Automatic</strong> option is used.</td>
</tr>
<tr>
<td></td>
<td>The default option is <strong>Automatic</strong>.</td>
</tr>
<tr>
<td>Real name</td>
<td>Specify details about the user that make the user account more identifiable.</td>
</tr>
<tr>
<td>Home directory</td>
<td>Select an option:</td>
</tr>
<tr>
<td></td>
<td><strong>Automatic</strong></td>
</tr>
<tr>
<td></td>
<td><code>/home/$username</code> is the home directory value.</td>
</tr>
<tr>
<td></td>
<td><strong>Directory</strong></td>
</tr>
<tr>
<td></td>
<td>specify the fully qualified path to use as the home directory or click the <strong>Browse</strong> button to select a location.</td>
</tr>
<tr>
<td></td>
<td>The default is <strong>Automatic</strong>.</td>
</tr>
<tr>
<td>Shell</td>
<td>Select a shell from the menu. Alternatively, you can enter the path to the shell to use.</td>
</tr>
<tr>
<td>Password</td>
<td>Select an option:</td>
</tr>
<tr>
<td></td>
<td><strong>No password required</strong></td>
</tr>
<tr>
<td></td>
<td>sets the password to null.</td>
</tr>
<tr>
<td></td>
<td><strong>Normal password</strong></td>
</tr>
<tr>
<td></td>
<td>enter the plain-text password in the field.</td>
</tr>
<tr>
<td></td>
<td><strong>Pre-encrypted password</strong></td>
</tr>
<tr>
<td></td>
<td>enter a password in encrypted form.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Password changed</td>
<td>Specifies the last time the password was changed.</td>
</tr>
<tr>
<td>Expiry date</td>
<td>Specify the date on which the password should expire. You can enter the date or use the calendar. The default is no date.</td>
</tr>
<tr>
<td>Minimum days</td>
<td>Specifies the minimum number of days between password changes. The default is zero.</td>
</tr>
<tr>
<td>Maximum days</td>
<td>Specifies the maximum number of days between password changes. The default is 99999.</td>
</tr>
<tr>
<td>Warning days</td>
<td>Specifies the number of days that a password expiration warning is generated before a password expires. The default is zero.</td>
</tr>
<tr>
<td>Inactive days</td>
<td>Specifies the number of days that a user must be inactive before the user account is locked. The default is zero.</td>
</tr>
<tr>
<td>Force change at next login?</td>
<td>Select <strong>Yes</strong> to force the user to change the password after the next logon. The default is <strong>No</strong>.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>This option is not available for deployments that use SUSE Linux Enterprise Server. In this case, edit the user account after it is created to force the change.</td>
</tr>
<tr>
<td>Primary group</td>
<td>You can select <strong>Existing group</strong> and then click <strong>...</strong> to browse for an existing group. Alternatively, you can create a new group and enter the name with the <strong>New group</strong> option.</td>
</tr>
<tr>
<td>Secondary groups</td>
<td>Select groups from the list and use the buttons to specify the secondary groups.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Propagate User</td>
<td>Select Yes to add the user to each machine in the environment. The default is No.</td>
</tr>
<tr>
<td>Generate and Propagate SSH Keys</td>
<td>Select Yes to generate SSH keys and propagate them when the user is created. The default is No.</td>
</tr>
<tr>
<td>Add Shared Midtier Key</td>
<td>This option is obsolete beginning with the SAS Visual Analytics 6.1 release.</td>
</tr>
<tr>
<td>Create home directory?</td>
<td>Select Yes to create the user’s home directory. Select No if the directory already exists. The default is Yes.</td>
</tr>
<tr>
<td>Copy template files to home directory?</td>
<td>Select Yes to copy standard environment files to the user’s home directory at creation time. The default is Yes.</td>
</tr>
</tbody>
</table>

4 Click Create.

If Propagate User was set to Yes, then the progress of adding the user to the machines in the environment is shown.

If a mismatch is detected on a machine, such as a UID already in use, then the change fails and the mismatch is reported.

**About Editing and Deleting Users**

You can edit a user by selecting the user name on the HPC Users tab. The following list identifies the fields that can be changed:

- **Real name**
- **Shell**
- **Password**
- **Expiry date**
- Minimum days
- Maximum days
- Warning days
- Inactive days
- Force change at next login?
- Primary group and Secondary groups
- Generate and Propagate SSH Keys
- Add Shared Midtier Key

The field descriptions for these options are provided in Table 4.2 on page 30.

You can also delete users individually or in groups by selecting the check box for the user on the HPC Users tab and then clicking Delete Selected Users.

**SSH Key Management Features**

As described in the section about creating users, the console can generate and propagate SSH keys. You can also generate SSH keys and propagate them for existing user accounts.

To perform this action, edit the user by selecting the user name on the HPC Users tab, select the radio button for Generate and Propagate SSH Keys, and click Save.

**Create a Group**

To create a group:

1. Click HPC Management from the toolbar.
2. Click Users and Groups.
3. Select the HPC Groups tab and then click Create a new group. Specify values for the following fields:
### Table 4.3 Create Group Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group name</strong></td>
<td>Specify the name for the group, such as finance or team1.</td>
</tr>
</tbody>
</table>
| **Group ID** | Select an option:  
**Automatic**  
the operating system selects an unused GID.  
**Calculated**  
(rarely used) the GID is created based on a Berkeley CRC and mkgid.  
**Specified**  
specify the GID to use. By default, this field shows the GID that is assigned if the **Automatic** option is used.  
The default option is **Automatic**. |
| **Members**  | Select users from the list and use the buttons to specify the members of the group. |

4. Click **Create**.

If a mismatch is detected on a machine, such as a GID already in use, then the change fails and the mismatch is reported.

**About Editing and Deleting Groups**

You can edit a group by selecting the group name on the **HPC Groups** tab. Users can be added as members of the group. This action sets secondary group membership for the user account.

You cannot delete a group if it is used as the primary group for any user accounts.
Managing User Sessions

Features in User Session Management

The HPC management interface of the SAS High-Performance Computing Management Console enables administrators to monitor and manage user logon sessions. The following features are available to administrators:

- review recent SSH log on activity for one user or all users
- display a list of users currently logged on through SSH
- limit SSH logon actions by performing an SSH lockout

Review Recent SSH Logon Activity

To review recent SSH logon activity:

1. Click **HPC Management** from the toolbar.

2. Click **Users and Groups**.

3. Scroll to the bottom of the table of user accounts and then select either **All users** or **Only user**. If you select **Only user**, then enter the user account to review or click the button to select the user account from a list.

4. Click **Display Logins By**.
The recent logon activity is listed in the **Recorded Logins** table.

**Display 4.3  Recent SSH Logon Activity**

![Recorded Logins Table]

<table>
<thead>
<tr>
<th>Login From</th>
<th>Login At</th>
<th>Logout At</th>
<th>On For</th>
</tr>
</thead>
<tbody>
<tr>
<td>pts/0</td>
<td>Tue May 8 04:33</td>
<td>Still logged in</td>
<td></td>
</tr>
<tr>
<td>pts/3</td>
<td>Wed May 2 10:23</td>
<td>10:23</td>
<td>00:00</td>
</tr>
<tr>
<td>pts/3</td>
<td>Wed May 2 10:11</td>
<td>10:11</td>
<td>00:00</td>
</tr>
<tr>
<td>pts/3</td>
<td>Wed May 2 09:53</td>
<td>09:53</td>
<td>00:00</td>
</tr>
<tr>
<td>pts/3</td>
<td>Wed May 2 09:41</td>
<td>09:41</td>
<td>00:00</td>
</tr>
<tr>
<td>pts/3</td>
<td>Wed May 2 09:40</td>
<td>09:40</td>
<td>00:00</td>
</tr>
<tr>
<td>pts/0</td>
<td>Tue Apr 24 11:44</td>
<td>21:57</td>
<td>10:12</td>
</tr>
</tbody>
</table>

The **Login From** field is used to show the IP address or host name that was used for the logon session.

**Show Currently Logged On Users**

To show the users that are currently logged on with SSH:

1. Click **HPC Management** from the toolbar.
2. Click **Users and Groups**.
3. Scroll to the bottom of the table of user accounts and click **Show Logged In Users**.
The currently logged on users are listed **Logged In Users** table. You can select the user name to review the recent SSH logon activity for the user account.

**Display 4.4  Logged In Users**

The **Logged in from** field is used to show the IP address or host name that was used for the logon session.

---

**Perform an SSH Lockout**

**Understanding the SSH Lockout Feature**

The SSH Lockout module enables an administrator to limit SSH logon access to the environment. This feature provides a mechanism for ensuring that processing resources are available for high-priority tasks as well as to assist with managing scheduled maintenance. Be aware that existing SSH logons are not affected by a lockout. A lockout prevents new SSH logons only. Access to software that does not rely on SSH is unaffected.

The feature provides user-level controls for denying SSH logons broadly while permitting SSH logons from specific user accounts. This level of control is available...
based on how you set the lockout controls. The following figure shows the fields that are available on the **Lockout Whitelist** tab.

**Display 4.5  SSH Lockout**
The following table provides a description for each of the fields on the **Lockout Whitelist** tab and describes how the settings interact with each other. The lockout status is not changed until the **Commit** button is clicked.

**Table 4.4  Lockout Whitelist Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Lockout Status</strong></td>
<td>This field shows the current lockout status and is used to set the lockout status:</td>
</tr>
<tr>
<td></td>
<td><strong>Enabled</strong> only the user accounts listed in the <strong>Admin Users</strong> and <strong>Regular Users</strong> are permitted SSH logon access.</td>
</tr>
<tr>
<td></td>
<td><strong>Disabled</strong> all users, except the users listed in the <strong>Disabled Users</strong> are permitted SSH logon access.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> User accounts in the <strong>Disabled Users</strong> are denied SSH logon access at all times.</td>
</tr>
<tr>
<td><strong>Kerberos Support for SSH Daemon</strong></td>
<td>Select <strong>Yes</strong> if the site uses Kerberos as the passwordless authentication mechanism. The console adds the following to the <strong>/etc/ssh/sshd_config</strong> file.</td>
</tr>
</tbody>
</table>
|                         | GSSAPIAuthentication yes  
GSSAPICleanupCredentials yes  
|                         | The default is **No**.                                                                                                                     |
| **Admin Users**         | Specifies the user accounts that are permitted SSH logon access when the lockout is active.                                                |
| **Regular Users**       | Specifies the user accounts that are permitted SSH logon access when the lockout is active.                                                |
| **Disabled Users**      | Specifies the user accounts that are denied SSH logon access at all times. This list can be used to deny access to single users even when a lockout is not active. |
Perform an SSH Lockout

To perform an SSH lockout:

1. Click **HPC Management** from the toolbar.
2. Click **SSH Lockout**.
3. Select **Enabled** on the **Lockout Status**.
4. Review the **Kerberos Support for SSH Daemon** option, and the **Admin Users**, **Regular Users**, and **Disabled Users** lists.
5. Click **Commit**.

To disable an SSH lockout, set the Lockout Status to **Disabled** and then click **Commit**.
Managing Database Resources

Managing Active Queries and Connections .............................................. 43
Understanding the Active Queries and Connection Feature ................. 43
Configuring the Greenplum Database Connection .......................... 44
Restrict the Database User Account ............................................. 45
Viewing Active Queries and Connections ..................................... 46

Managing Temporary Tables .............................................................. 47
About Temporary Tables ................................................................... 47
Viewing Temporary Tables ............................................................... 47

Managing Active Queries and Connections

Understanding the Active Queries and Connection Feature

For deployments that use Greenplum Data Computing Appliance (DCA) as a co-located data provider, this feature enables an administrator to monitor long running queries and terminate database connections.

In order to monitor queries and terminate connections, a database user account is needed to connect to the database with administrative privileges. In order to list the active queries for all connections and to be able to terminate connections, the database user account should be granted the superuser role.
Configuring the Greenplum Database Connection

When you first access the Active Queries and Connections module, the console cannot connect to the Greenplum database because it is not configured with the connection parameters. The following display shows an example of the console before it is configured.

Display 5.1  Unconfigured Active Queries and Connections

To configure the module:

1. Click HPC Management from the toolbar.
2. Click Active Queries and Connections.
3. Select Module Config. (Shown in the preceding display.)
4. Specify the following parameters:
### Table 5.1  Active Queries and Connections Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Account Name for DB Connections</strong></td>
<td>Enter the name of a database user account that has been granted the superuser role. For information about securing this user account, see “Restrict the Database User Account”.</td>
</tr>
</tbody>
</table>
| **Account Password**          | This field is used for storing a password. This field is also used to avoid changing a stored password:  
                                   **Don’t change**  
                                   Select this option to avoid changing a stored password.  
                                   **Set to**  
                                   Select this option and specify the password for the database user account. The password is stored in `/opt/webmin/etc/actpsgqrys/config`. |
| **Database Name**             | Specifies the database name to use.                                                                                                                                                                     |
| **MDW Hostname**              | Specifies the host name for the Greenplum Database Master Host.                                                                                                                                       |

5  Click **Save**.

**Restrict the Database User Account**

The database user account that is used for the Greenplum Database connection must have superuser privileges in order to monitor queries and terminate connections. You can increase the security for the account by configuring Greenplum Database to accept connections for the account from the machine that hosts the console.
To restrict the database user account:

1. Edit the `$MASTER_DATA_DIRECTORY/pg_hba.conf` file.

2. Add a line to the file that is similar to the following example:

   ```
   # permit the 'sashpcadm' role access to any database from
   # IP address 192.168.1.1 only and use md5 encrypted password
   host   all   sashpcadm   192.168.1.1/32   md5
   ```

3. Save and close the file.

4. Run `gpstop -u` so that Greenplum Database rereads the file and applies the change.

The same database user account can be used for the active queries and connections module and the temporary table maintenance module. For more information about editing the `pg_hba.conf` file, see `Greenplum Database Administrator Guide`.

**Viewing Active Queries and Connections**

Once the database connection information has been configured, the active queries and connections module shows the active query and connection information. Each row provides information about a database server process.

(Display 5.2  Active Queries and Connections)
Select the check box for a server process and click **Kill Selected** to terminate the queries, connection, and server process. In the event that the process is not terminated, see Greenplum Database documentation for information about terminating processes.

---

**Managing Temporary Tables**

**About Temporary Tables**

Temporary tables are a feature of Greenplum Database and several other third-party DBMS vendors. In some circumstances temporary tables are created by processes but are not dropped. The console provides the temporary table maintenance module for listing temporary tables and dropping them to restore system resources.

Before using the temporary table maintenance module, you must configure the Greenplum Database connection. Select **HPC Management ➤ Temporary Table Maintenance ➤ Module Config**. The configuration parameters are identical to those described in “Configuring the Greenplum Database Connection” on page 44.

**Viewing Temporary Tables**

To view temporary tables:

1. Click **HPC Management** from the toolbar.
2. Click **Temporary Table Maintenance**.
3 Select the check box for a table to drop, and click **Delete Tables** to drop the tables.

**Note:** It is possible to drop a table that is in use. Make sure that the table that you have selected to drop is not in use. Perform this action during scheduled maintenance or after using some other method to ensure that the table is not in use.
Managing Cube Data Files

Understanding the Cube Cleanup Feature ........................................ 49
Specifying the Directory to Manage ............................................. 50
Searching for Cube Data Files ...................................................... 51
Deleting Cube Data Files .............................................................. 53

Understanding the Cube Cleanup Feature

**TIP** The cube cleanup feature is available for deployments that use SAS High-Performance Risk only.

When the HPRISK procedure is used in a High-Performance Analytics Environment, the procedure creates data files for cubes on each machine in the cluster. The data files are created in the directory that is specified in the GRIDPATH= option.

The data files can be removed with the TASK=CLEAN option to the HPRISK procedure. However, there are some reasons that it might be necessary to use the console to manage cube data files. Some of these reasons are identified in the following list:

- The cube descriptor was deleted before using the HPRISK procedure with the TASK=CLEAN option.
The cube descriptor file is corrupted or, for some reason, is no longer readable by the HPRISK procedure.

The cube descriptor file references host names for machines in the cluster that are no longer in service. This can be caused by an outage or renaming host names.

As indicated by the preceding list, there can be several reasons that data files are left on the machines in the cluster. The cube cleanup feature is used to list the data files so that you can delete them.

## Specifying the Directory to Manage

When you first access the **Cube Cleanup** module, the console is not configured to monitor a directory for data files. The following display shows an example of the console before it is configured.

**Display 6.1  Unconfigured Cube Cleanup**

To configure the module:

1. Click **HPC Management** from the toolbar.
2. Click **Cube Cleanup**.
3. Select **Module Config**. (Shown in the preceding display.)
4 Specify the following parameters:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location of Cubes</td>
<td>Specifies the path that is used in the GRIDPATH= option to the HPRISK procedure. If there are sub directories in the specified path, they are monitored as well.</td>
</tr>
<tr>
<td>Max Files per Page</td>
<td>Specifies the number of files to list in the console. If the number of files in the monitored directory exceeds this number, then the console provides a search window instead of listing the files.</td>
</tr>
</tbody>
</table>

5 Click **Save**.

---

**Searching for Cube Data Files**

To search for cube data files:

1 Click **HPC Management** from the toolbar.

2 Click **Cube Cleanup**.

3 If files are listed, click **Search**. If the monitored directory has more files than the Max Files per Page setting, then you are automatically presented with the search options.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Files By</td>
<td>Use the menu to select a value:</td>
</tr>
<tr>
<td><strong>Owner</strong></td>
<td>Select this option to search for files by the user ID that owns the data file.</td>
</tr>
<tr>
<td><strong>Node Hostname</strong></td>
<td>Select this option to search for files by the host name.</td>
</tr>
<tr>
<td><strong>Cube File Name</strong></td>
<td>Select this option to search for files by the name of the data file.</td>
</tr>
<tr>
<td>Which</td>
<td>Use the menu to select either <strong>Contains</strong> or <strong>Equals</strong>.</td>
</tr>
<tr>
<td>This Text</td>
<td>Specifies the user ID, host name, or filename to use for the search. If <strong>Which</strong> is set to <strong>Equals</strong>, then the search criteria must be an exact match. If <strong>Which</strong> is set to <strong>Contains</strong>, then the specified text is used to match substrings.</td>
</tr>
<tr>
<td>Or Files That Are</td>
<td>The search for data files always includes date-based criteria. Use the menu to specify whether the search includes files that are <strong>Older</strong> or <strong>Newer</strong> than the specified date.</td>
</tr>
<tr>
<td>Than This Date</td>
<td>Specifies the date to use for the date-based search criteria.</td>
</tr>
</tbody>
</table>

4 Click **Find**.
Deleting Cube Data Files

Once you have specified the directory to monitor for cube data files, you can delete files that are no longer needed. To delete the cube data files:

1. Click **HPC Management** from the toolbar.

2. Click **Cube Cleanup**.

3. Select the check box beside the cube data file to delete.

   **Display 6.2   Cube Files to Delete**

4. Click **Delete**. Scroll to the bottom of the page if the button is not visible.

You can also use the **Select all** and **Invert selection** links to control which check boxes are selected. You can select the table heading, such as **Last Access Time**, to sort the data files. Click the same heading again to reverse the sort order.
Managing CPU and Memory Resources

Understanding the CGroup Resource Management Feature

You can use the CGroup Resource Management feature to manage CPU consumption for users and groups. Resource management is performed through configuring kernel control groups (cgroups). The Linux kernel used for the SAS High-Performance Analytics Environment supports for cgroups. The Linux kernel supports managing several subsystems to limit, prioritize, and account for resources. The SAS High-Performance Computing Management Console supports managing the CPU subsystem.
because it is a contentious resource in a deployment that uses the SAS High-Performance Analytics Environment.

In order to use the CGroup Resource Management feature, the operating system must include support for it though the Linux kernel version and the CGroups libraries. The Linux kernels used in Red Hat Enterprise Linux 6 and SuSE Linux Enterprise Server 11, and Oracle Linux 6 contain support for CGroups. Older versions from both vendors do not include support for CGroups.

---

**About Resource Allocation**

When you add a control group, you specify a share of the CPU, as a percentage, that the control group can use. When you view the CGroup Resource Management page, the allocated, available, and maximum percentages are listed in the CGroup Resource Allocation table.

Be aware that the allocation of CPU resources is for processes that are managed with control groups. Some CPU resources are consumed by system processes and processes that are started by users that are not part of control groups. In general, the percentages that are specified should be very close to actual CPU utilization when the system reaches full load.
CGroups Resource Management Page

The following display shows the CGroup Resource Management page.

Display 7.1  CGroup Resource Management

The operations that can be performed at the top of the page are described in "CGroup System Services."

The Configured CGroups section is used to manage the control groups, including "Creating a Control Group."
The **CGroup Resource Allocation** table lists the CPU share percentage that is allocated to control groups. For more information about the resources, see "About Resource Allocation."

The “Administrative Functions” operations are available from the bottom of the page.

---

**Creating a Control Group**

To create a control group:

1. Click **HPC Management** from the toolbar.
2. Click **CGroup Management**.
3. In the **Configured CGroups** section, click **add new cgroup**.

4. Specify the following parameters:
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group Name</strong></td>
<td>Specify a name for the control group such as <code>lowpriority</code>.</td>
</tr>
<tr>
<td><strong>Group Description</strong></td>
<td>Specify a description.</td>
</tr>
<tr>
<td><strong>CPU Share Percentage</strong></td>
<td>Specify the share of CPU utilization, as percentage, to allocate to the control group.</td>
</tr>
<tr>
<td><strong>Select Single Task Admin User</strong></td>
<td>Specify the user ID that can add a process to the control group task list. For more information about the task admin user, see the information that follows this procedure.</td>
</tr>
</tbody>
</table>

5. Click **Save**.

The configuration files are updated, copied to the machines in the cluster, and the control group configuration start-up (cgconfig) service is restarted.

The task admin user is more important for Linux environments that manage control groups manually. In a SAS High-Performance Analytics Environment, the choice of a task admin user is less critical. For example, in a SAS deployment, any process that is started by a resource managed user in a control group is subject to the resource allocations. Therefore, the ability for the task admin user to add unmanaged processes to a task file so that the process can become a managed task is not critical in a SAS deployment.

**Editing and Deleting Control Groups**

To edit a control group, select the group name from the **CGroup Name** column. Specify the same parameters that are used for creating a control group.

To delete a control group, select the check box beside the group name and click **Delete**.

When you change the share percentage, memory limit, or delete a group, the **CGroup Resource Allocation** table is updated to show the resources that remain available.
Example: Resource Management

CPU resources are granted freely until the system is under load and there is contention for CPU time. Consider the following table that specifies three sample control groups and CPU share percentages.

Table 7.1  Sample CPU Share Percentage Allocation

<table>
<thead>
<tr>
<th>Control Group Name</th>
<th>CPU Share Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>High priority</td>
<td>60</td>
</tr>
<tr>
<td>Medium priority</td>
<td>30</td>
</tr>
<tr>
<td>Low priority</td>
<td>10</td>
</tr>
</tbody>
</table>

To understand how CPU utilization fluctuates until resource contention emerges, consider the following sequence of events:

1. A user in the low priority control group starts a process. Because there is no demand for CPU resources from any other user, the process receives 100% of the CPU time.
2. A user in the medium priority control group starts a process. The two users share CPU resources.
3. A user in the high priority control group starts a process. The contention for CPU resources causes the allocations to be enforced. The medium priority user receives 30% and the low priority user receives 10% until the process for the user in the high priority group ends or does not require CPU resources.
CGroup Resource Management Administration

CGroup System Services

The CGroup System Services section of the page shows the number of processes and status for the cgconfig service.

You can click view all services to view a table of host names, services, and service statuses.

Administrative Functions

The most commonly used administrative functions are listed as buttons at the bottom of the page. The buttons are as follows:

**Compare Config Files**

Click this button to ensure that the configuration files for the control groups are the same on each machine in the cluster.

**Copy Config Files**

Click this button to copy the configuration files from the machine that is running the console to the other machines in the cluster.

**Restart All Services**

Click this button to restart the cgconfig service on each machine in the cluster.
Gridhosts File Management

What Is the Gridhosts File? ................................................................. 63

Managing the Gridhosts File ......................................................... 64
  Creating the File ................................................................. 64
  Editing Host Names in the Gridhosts File ......................... 65

What Is the Gridhosts File?

Identifying all the machines in the environment is critical to ensuring that the console can perform operations in parallel or serially on the machines in the cluster. The /etc/gridhosts file is used to identify the machines. It is a list of the machines, with one host name on each line. The /etc/gridhosts file is not the same as the /etc/hosts file.

The /etc/gridhosts file is created immediately after installing SAS High-Performance Computing Management Console. If the /etc/gridhosts file has not been created already, then follow the steps described in “Creating the File” on page 64. The console is also used to manage the host names that are listed in the file. The following sections provide more detail.
Managing the Gridhosts File

Creating the File

The contents of the file (host names) are typically created in a text editor or with shell scripting to avoid repetitive typing. If the file is not present on the machine that is hosting the console, then the following page is seen after accessing the Gridhosts File Management module of the console.

Display 8.1  Generate Gridhosts File

Note: The **Use /etc/hosts** button cannot be used in a SAS Visual Analytics deployment to create the **/etc/gridhosts** file.

If you can access the file, then you can upload it to the machine that is hosting the console. The file must contain one host name on each line. The host name must be the host name of the network interface to use for communication between the machines in the grid.

To upload a file:

1. Click **Upload a file**.
2 Click **Browse** and then navigate to the file that contains the host name of the machines in the cluster.

Click **Upload**.

3 Review the host names that are listed in the table. If the list of host names is accurate, click **Select all** at the top of the table. Click **Submit**.

After the **Submit** button is clicked, the `/etc/gridhosts` file is created on the machine that is hosting the console.

**Editing Host Names in the Gridhosts File**

You can use the console to add and delete host names from the `/etc/gridhosts` file. The following display shows the link for adding host names and the button for deleting them.

*Display 8.2  Gridhosts File*

To add a host name:

1 Click **Add Host**.

2 Enter the host name in the **Hostname** field and click **Add**.
Note: If the machine that you specify is running and passwordless SSH is configured for the root user, then the SSH Connectivity field indicates Yes.

To delete a host name:

1. Select the check box beside the host name to remove.

2. Click Delete.

This action prevents the console from performing configuration operations on the machine. If the SAS High-Performance Computing Environment software or SAS High-Performance Deployment of Hadoop is configured, then those products need to be reconfigured to remove references to the machine too.
Managing Simultaneous Utilities Machine Groups

Understanding the Groups

You can use simultaneous utilities machine groups to manage a subset of the machines in the cluster. You might want to use one of the simultaneous utilities (\texttt{simsh} and \texttt{simcp}) to perform an action on some of the machines in the cluster instead of all of them.

\textit{Display 9.1 Sim Groups Management}
Creating a Group

To create a group:

1. Click **HPC Management** from the toolbar.
2. Click **Sim Groups**.
3. Click **Add New Sim Group**. Specify values for the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify a name for the group such as <code>datanodes</code>.</td>
</tr>
<tr>
<td>Membership</td>
<td>Select host names from the list and use the buttons to specify the members of the group.</td>
</tr>
</tbody>
</table>

4. Click **Add Group**.

   The `/etc/simgroups` file is updated with the new group.

Editing and Deleting Sim Groups

To edit a group, select the group name from the **Sim Group Name** column. Specify the host names to use in the group.
To delete a group, select the check box beside the group name and click **Delete**.
Simultaneous Shell Utilities

**Simultaneous Shell Command** ................................. 71
What is the Simultaneous Shell Command? ....................... 71
Example: Counting Files ........................................... 72
Example: Retrieving the Command Return Code ............... 72
Example: Checking Disk Usage on DataNodes ................. 73

**Simultaneous Copy Command** ................................. 73
What is the Simultaneous Copy Command? ......................... 73
Example: Copying Files ........................................... 74
Example: Retrieving the Copy Return Code .................... 74
Example: Copying Files to Some Machines Only ............... 74

---

**Simultaneous Shell Command**

**What is the Simultaneous Shell Command?**

The simultaneous shell command, `simsh`, is installed with the console. The default location is `/opt/webmin/utilbin/simsh`. The `simsh` command relies on passwordless SSH and the `/etc/gridhosts` file. When you use the `simsh` command, passwordless SSH is used to log on to each machine identified in the `/etc/gridhosts` file and run the command line that follows the `simsh` command.

The `-r` option is used to retrieve return codes. The `-g $groupname` option is used to specify the group to use for the command.
Example: Counting Files

The following example counts the number of files in `/tmp` on each machine in the cluster:

```
/opt/webmin/utilbin/simsh "ls /tmp | wc -l"
```

```
grid001.example.com: 6
grid002.example.com: 7
grid003.example.com: 12
...
grid016.example.com: 6
```

Example: Retrieving the Command Return Code

By default, the `simsh` command returns the host name, a colon, and the output of the command that ran on the machine. Some commands do not provide output, such as the `mkdir` command. In order to determine whether the `mkdir` command succeeds, you must check the return code. The following example uses the `-r` option to report the return code for the `mkdir` command:

```
/opt/webmin/utilbin/simsh -r "mkdir -p /tmp/sas/somedir"
```

```
grid001.example.com:0
grid002.example.com:0
grid003.example.com:0
...
grid016.example.com:0
```

Zero indicates success. Any other value indicates an error.

You can also use the `-r` option with commands that do return output. The following example uses the `grep` command to determine whether `grp1` is listed in `/etc/group` on every machine in the cluster:

```
/opt/webmin/utilbin/simsh -r "grep '^grp1:' /etc/group"
```
In the preceding example, the return code for machine grid003.example.com is 1. The `grep` command did not execute successfully on the machine.

**Example: Checking Disk Usage on DataNodes**

The following example uses a group that is named `datanodes` to check the disk usage for the directory that is used for HDFS blocks:

```bash
/opt/webmin/utilbin/simsh -g datanodes du /hadoop-0.23/hadoop-data -sm
```

When you specify a group name with the `-g` option, `simsh` uses the `/etc/simgroups` file to identify the machines to use.

**See Also**

“Creating a Group” on page 68

---

**Simultaneous Copy Command**

**What is the Simultaneous Copy Command?**

The simultaneous copy command, `simcp`, is installed with the console. The default location is `/opt/webmin/utilbin/simcp`. The `simcp` command relies on passwordless SSH and the `/etc/gridhosts` file. When you use the `simcp` command, passwordless SSH is used to copy a file or a directory securely to each machine identified in the `/etc/gridhosts` file.
The `-r` option is used to retrieve return codes. The `-g $groupname` option is used to specify the group to use with the secure copy.

**Example: Copying Files**

The following example copies the `/etc/hosts` file to each machine in the cluster:

```bash
/opt/webmin/utilbin/simcp /etc/hosts /etc/
```

You can also use the `simcp` command to copy files recursively. For example, if the `/home/sas/inst` directory has multiple files, the following example copies the files to `/tmp`:

```bash
/opt/webmin/utilbin/simcp /home/sas/inst /tmp/
```

**Example: Retrieving the Copy Return Code**

You can also use the `-r` option to retrieve the return code for the copy. The following example:

```bash
/opt/webmin/utilbin/simcp -r /home/sas/inst /data1/inst/
```

```
grid001.example.com:0:/home/sas/inst copied
grid002.example.com:0:/home/sas/inst copied
...
grid016.example.com:0:/home/sas/inst copied
```

The return code is presented after the host name. A zero indicates success. Any other value indicates an error.

**Example: Copying Files to Some Machines Only**

The following example uses a group that is named `datanodes`. A file that is named `slaves` is copied to all the machines in the group:

```bash
./simcp -g datanodes slaves /hadoop-0.23/hadoop-0.23.1/etc/hadoop
```
When you specify a group name with the -g option, `simcp` uses the `/etc/simgroups` file to identify the machines to use.

**See Also**

“Creating a Group” on page 68
Index

C

CGroup Resource Management 55
CPU utilization 55
cube data files
SAS High-Performance Risk 49

G

Greenplum Database
drop temporary tables 47
superuser privilege 45
terminate long running queries 46
gridhosts file 63
location and format 64

I

IP address and port number 5

L

logs
configuring 9

N

network
IP address and port number 5

R

recursive copy 74
resource management 55
return code
simcp 74
simsh 72

S

security
limit logon access 38
simcp 73
simsh 71
simultaneous utilities machine
group
simcp 74
simsh 73
simultaneous utilities machine
groups 67
SSH keys 30
  generating and propagating 33
SSH lockout 38, 41

**U**

UNIX groups
  creating 34
  members 35
UNIX user accounts
  creating 30
  deleting 34

secondary group membership 35
SSH keys 30
user management
  audit SSH logon activity 36
  creating users 30
  deleting users 34
  force log off console user 20
  group membership 35
  logged on users 37
  prevent SSH logons 38
Users
  displayed in italics 29