SAS® Viya® 3.5 Administration: Using CAS Server Monitor

Introduction ................................................................. 3
  What Is CAS Server Monitor? ........................................ 3
  Accessing CAS Server Monitor .................................... 3
  Accessibility .............................................................. 4
  Preferences ............................................................... 4
  Signing Out ............................................................. 4

Stop a CAS Server .......................................................... 5

Monitor a CAS Server ..................................................... 6
  Preliminary Navigation ................................................ 6
  Monitor CAS Process Performance ................................. 6
  Monitor CPU Usage for a Session .................................. 7
  Monitor Host Performance .......................................... 7
  Monitor Process Information ....................................... 8
  Change the Monitoring Display Options .......................... 8

Enable Users to Add Caslibs ............................................. 9

Add or Delete a Global Caslib ......................................... 11
  Add a Global Caslib ................................................... 11
  Delete a Global Caslib ............................................... 12

Manage Access to a Global Caslib .................................... 13
  Preliminary Navigation ............................................... 13
  Examine Access to a Caslib ......................................... 13
  Provide Public Access to a Caslib ................................. 14
  Selectively Grant Access to a Caslib .............................. 14
  Selectively Limit Access to a Caslib .............................. 15
  Resolve Duplicate Access Controls ................................ 16

Manage CAS Roles ......................................................... 18
  Preliminary Navigation ............................................... 18
  Add a Member to a Role ............................................. 18
  Change a Role Assignment .......................................... 19
  Remove a Role Assignment ......................................... 19

Manage CAS Nodes .......................................................... 20
Preliminary Navigation .......................................................... 20
View Information .................................................................... 20
Add a Node ............................................................................ 20
Remove a Node ................................................................. 21
Stop a Node ........................................................................ 21

Manage CAS User Sessions .................................................. 22
  Preliminary Navigation ..................................................... 22
  Cancel a Session ............................................................. 22
  Terminate a Session ......................................................... 22

View Server Information ....................................................... 23
  View Configuration File Options .................................... 23
  View Properties and System Information ....................... 23
  View Start-Up Options and Environment Variables .......... 23

Remove CAS Worker Software ............................................. 24

Troubleshooting .................................................................... 25
  Insufficient Disk Space (CAS_DISK_CACHE) ...................... 25
  Cannot Access the Permstore ........................................... 25
  Cannot Monitor CPU Usage for a Session ....................... 25
  Delay in Execution of a Data Quality Operation ............... 25
Introduction

What Is CAS Server Monitor?
CAS Server Monitor is an embedded web application for a CAS server. CAS Server Monitor functions as a lightweight utility that provides monitoring and configuration information for a CAS server. CAS Server Monitor can also be used to perform some administrative tasks.

**IMPORTANT** CAS Server Monitor is intended for use in programming-only deployments. Otherwise, CAS Server Monitor is disabled by default.

Accessing CAS Server Monitor
1. If CAS Server Monitor is not currently enabled, set the environment variable `env.CAS_START_MONITOR_UI` to `TRUE`. See “Where Do I Set CAS Environment Variables?” in *SAS Viya Administration: SAS Cloud Analytic Services*.

2. If the CAS server is not already running, start it. See “SAS Cloud Analytic Services: How To (Scripts)” in *SAS Viya Administration: SAS Cloud Analytic Services*.

   **TIP** CAS Server Monitor is available only when the CAS server is running. When the CAS server terminates, CAS Server Monitor also terminates.

3. In a web browser, go to your equivalent of the following URL:

   ```
   https://reverse-proxy-server/cas-shared-deployment-instance-http
   ```

   Here is an example:

   ```
   https://host1.abc.com/cas-shared-default-http
   ```

   **TIP** For a tenant (in a multi-tenant environment), prepend the machine name with `tenant` and a dot (.), and specify the tenant’s deployment instance.

   Here is an example:

   ```
   https://acme.host1.abc.com/cas-acme-default-http
   ```

4. Sign in with an appropriate account.
Note: Not all features in CAS Server Monitor are available to all users. If you sign in with an account that is a member of the Superuser (CAS) role, all features are available. See “Manage CAS Roles”.

Accessibility

CAS Server Monitor for SAS Viya 3.5 has not been tested against U.S. Section 508 standards and W3C Web Content Accessibility Guidelines (WCAG). If you have specific questions about the accessibility of SAS products, send email to accessibility@sas.com or call SAS Technical Support.

Preferences

To specify a default view, click your user name in the upper right of the CAS Server Monitor window, and select Settings.

Signing Out

To sign out, click your user name in the upper right of the CAS Server Monitor window, and select Sign Out.

Note: CAS Server Monitor does not use a session time-out.
Stop a CAS Server

1. On the vertical navigation bar in CAS Server Monitor, click 🖼.

2. On the System State page, select Controller.

3. On the upper right side of the page, click Shutdown.

   Note: The Shutdown action is available to members of the Superuser (CAS) role.

   Note: For a distributed CAS server, the shutdown action stops all the CAS worker nodes and the backup controller (if present), in addition to stopping the main controller.

See Also

“SAS Cloud Analytic Services: How To (Scripts)” in SAS Viya Administration: SAS Cloud Analytic Services
Monitor a CAS Server

Preliminary Navigation


Monitor CAS Process Performance

The CAS processes that you can monitor correspond to SAS server processes. You can separately monitor each session that is started from the CAS server.

1. Select Add View ⇒ CAS Process CPU Usage.

   The Process CPU Usage panel displays a set of histograms. There is one histogram for each machine and the corresponding CAS server process. The histogram in the upper left is the CAS controller node. If you are not an administrator, only the histogram for the CAS controller node is displayed.

   Each histogram displays the percentage of CPU usage, from 0 to 100%.

   ![CPU Usage Histogram](image)

   Use these histograms to note patterns of CPU usage among the CAS nodes.

2. Select Add View ⇒ CAS Process Metrics.

   The CAS Process Metrics panel displays a set of histograms. There is one set of three histograms for each machine and the corresponding CAS server process. If you are not an administrator, only the set of histograms for the CAS controller node is displayed.

   Each set of histograms displays the percentage of CPU used, amount of resident memory used, and amount of virtual memory used for the CAS process.

   ![Memory Usage Histogram](image)
To stop metric collection, click ■. To resume collection, click ▶.

Monitor CPU Usage for a Session

Click Add Session View, and select a session.

The panel for the session displays a set of histograms, with one histogram for each machine in the grid. If you are not an administrator, only the histogram for the CAS controller node is displayed. The top half of the histogram displays the percentage of CPU load used by the session, and the bottom displays the amount of resident memory used for the session.

Monitor Host Performance

CAS Server Monitor displays histograms that enable you to view the CPU load and memory usage for all machines in your CAS server.

1 Select Add View ⇒ Host CPU Load Average.

The Host CPU Load Average panel displays a set of histograms. There is one histogram for each machine in the CAS grid. If you are not an administrator, only the histogram for the CAS controller node is displayed.

Each histogram displays the CPU load on the machine, using the same format as the Linux xload command. Each division on the histograms represents one load average point. The highest point on each histogram is displayed to the right of the histogram.

Use these histograms to observe usage patterns among the CAS nodes. For example, if you observe that the load on a worker node machine is significantly and consistently higher than the load on other machines, you can use Show Processes to check for other running processes or defunct processes. See “Monitor Process Information” for details.

2 Select Add View ⇒ Host Memory Usage.

The Host Memory Usage panel displays a set of histograms. There is one histogram for each machine in the CAS grid. If you are not an administrator, only the histogram for the CAS controller node is displayed.

Each histogram displays the percentage of memory used on the machine, from 0 to 100%. The percentage of memory used is displayed in green, at the top of the histogram. The percentage of virtual memory used is displayed in orange, at the bottom of the histogram.
Use these histograms to note patterns of memory usage among the CAS nodes. For example, if the memory usage is consistently high on a machine, its memory might need to be increased.

3 To stop metric collection, click ■. To resume collection, click ▶.

Monitor Process Information

1 Open a view from the Add View or Add Session View menu.
2 Click ↓ to the right of a histogram, and select Show Processes.

The Processes window displays the following information:
- Metrics for the selected node, including uptime, number of processes, memory usage, CPU load, and file usage.
- A histogram of the CPU load for the node.
- A table containing the output from the top command for the selected node. The output includes metrics such as CPU usage, time, and threads for each process. If you are a SAS administrator, the window displays information about all processes. If you are not a SAS administrator, you can view information only about your own processes.

TIP You can also show processes from the Nodes tab on the System State page. Click ↓ at the end of a row, and select Show Processes.

Change the Monitoring Display Options

On the Resource Monitor page, you can control how the histograms are displayed.
- To change how quickly the graph data is refreshed, move the slider next to the Speed label.
- To change the size of the histograms, move the slider next to the Size label.
- The default layout for a histogram view is a grid. To change to a single column, click the column icon in the banner for a view. To return to a grid layout, click the grid icon.

To change the default view for the Resource Monitor page, select userid ➔ Settings in the upper right of the CAS Server Monitor window.

See Also

“Monitoring: How To (CAS Options)” in SAS Viya Administration: Monitoring
Enable Users to Add Caslibs

To enable non-administrators to add global caslibs:

1. On the vertical navigation bar in CAS Server Monitor, click 🔍.
2. On the Configuration page, select Access Controls.
3. In the Caslibs list, select Global Caslib Creation.

TIP The Global Caslib Creation caslib is visible to members of the Superuser (CAS) and Data roles.

4. On the upper right of the page, click Edit.
5. In the Edit Access Controls window, adjust values as needed.

<table>
<thead>
<tr>
<th>Intent</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable all users to add global caslibs.</td>
<td>For Authenticated Users, select the Grant radio button. Note: If there is not already a row for Authenticated Users, click Add Row and select Authenticated Users in the Applies To column.</td>
</tr>
<tr>
<td>Enable a group to add global caslibs.</td>
<td>Click Add Row. Select Group, enter the group name, and select the Grant radio button.</td>
</tr>
<tr>
<td>Enable an individual user to add global caslibs.</td>
<td>Click Add Row. Select User, enter the user name, and select the Grant radio button.</td>
</tr>
</tbody>
</table>

6. Click OK to save your changes.
7. Under Access Controls, review the results of your changes.
8. Verify that users who should be able to add global caslibs can add global caslibs.

Here are details:

- User and group names that you enter are not validated.
- Regardless of access controls, administrators can add and manage all caslibs.
- For the special caslibs (Global Caslib Creation and Session Caslib Creation), the only available value in the Activity column is Manage Access. The special caslibs are protected by role requirements, not by the ManageAccess permission. Granting or denying the ManageAccess permission on the special caslibs affects only the ability of non-administrators to manage other caslibs.
- To restrict the ability to manage session caslibs, select Session Caslib Creation in the Caslibs list. Add direct denials as needed.
See Also

“Caslib Management Privileges” in SAS Viya Administration: SAS Cloud Analytic Services
**Add or Delete a Global Caslib**

**Add a Global Caslib**

1. On the vertical navigation bar in CAS Server Monitor, click 

2. On the **System State** page, click **Global Caslibs**.

3. Click **Add**.

   **Note:** If the **Add** button is disabled, you are not authorized to add global caslibs. See “**Enable Users to Add Caslibs**”.

4. In the **Add Global Caslib** pane, specify general settings as follows:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caslib</td>
<td>Specifies a caslib name.</td>
</tr>
<tr>
<td>Description</td>
<td>Specifies a description for the caslib.</td>
</tr>
<tr>
<td>Path</td>
<td>Specifies data source-specific information.</td>
</tr>
<tr>
<td>Subdirectories</td>
<td>For a path-based caslib, identifies whether tables and files in subdirectories of the specified path are accessible from the caslib.</td>
</tr>
<tr>
<td>Create directory</td>
<td>For a path-based caslib, creates the host directory that you specify in the <strong>Path</strong> field, if that directory does not already exist.</td>
</tr>
<tr>
<td>Permission</td>
<td>For a path-based caslib, sets host-layer permissions on the directory. See “<strong>Using CAS to Modify Host Access</strong>” in <em>SAS® Viya Administration: CAS Authorization</em>.</td>
</tr>
<tr>
<td>Active on add</td>
<td>Specifies whether the new caslib becomes the active caslib in your current session.</td>
</tr>
<tr>
<td>Hidden</td>
<td>Makes the caslib and its tables unlisted in certain contexts. See “<strong>Reduced Visibility: Hidden Caslibs</strong>” in <em>SAS® Viya Administration: CAS Authorization</em>.</td>
</tr>
<tr>
<td>Transient</td>
<td>Specifies that the caslib is scoped to the current session only.</td>
</tr>
<tr>
<td>Data source</td>
<td>Specifies the type of source data for the caslib.</td>
</tr>
<tr>
<td>Data encryption password</td>
<td>Specifies the encryption password for the caslib.</td>
</tr>
</tbody>
</table>
### Setting

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption domain</td>
<td>Specifies the encryption domain for the caslib.</td>
</tr>
<tr>
<td>Backing store</td>
<td>Specifies the type of backing store. Select <strong>casdiskcache</strong>, unless you know that a different value is needed.</td>
</tr>
</tbody>
</table>

5 Specify additional settings as needed (if you are prompted for more information). For details about caslib properties, see “Add caslib” in *SAS Viya: System Programming Guide*.

6 Make sure that your settings are specified as intended. Caslib properties are not editable.

7 Click **OK**.

### Delete a Global Caslib

**CAUTION**

When you delete a caslib, all associated in-memory tables are immediately dropped.

---

Note: Deleting a caslib does not affect persisted files in the corresponding data source.

1 On the **System State** page, click **Global Caslibs**.

2 At the end of the row for the caslib, click **;**, and select **Drop Caslib**.

3 In the **Drop Global Caslib** pane, click **OK**.

### See Also

“Caslibs” in *SAS Cloud Analytic Services: Fundamentals*
Manage Access to a Global Caslib

Preliminary Navigation

1 On the vertical navigation bar in CAS Server Monitor, click.
2 On the Configuration page, select Access Controls.
3 In the Caslibs list, select a caslib.

Here are details:

- To manage access at the table, column, or row level, use another interface.
- All the global caslibs that you are authorized to see are listed.
- To see any new global caslibs, click. The Caslibs list is not updated automatically.
- Session and personal caslibs are not listed because you cannot set access controls on them. Resources in session and personal caslibs are not sharable with other users.
- The Global Caslib Creation and Session Caslib Creation caslibs do not contain data. These special caslibs determine which non-administrators can add and delete caslibs. See “Enable Users to Add Caslibs”.
- Any predefined caslibs have appropriate access controls.

Examine Access to a Caslib

On the Configuration page, under Access Controls, the columns for the selected caslib are populated as follows:

<table>
<thead>
<tr>
<th>Column</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applies To</td>
<td>Specifies a type of access control principal.</td>
</tr>
<tr>
<td>Identity</td>
<td>Specifies the name (unique identifier) for an access control principal.</td>
</tr>
<tr>
<td>Grant</td>
<td>A check mark indicates that access to the selected caslib is authorized for the specified principal and permission.</td>
</tr>
<tr>
<td>Deny</td>
<td>A check mark indicates that access to the selected caslib is not authorized for the specified principal and permission.</td>
</tr>
<tr>
<td>Activity</td>
<td>Specifies a permission, such as Select.</td>
</tr>
</tbody>
</table>

The rows for a new custom caslib are initially populated as follows:
For the user who added the caslib, there is initially a row for every permission, because that user has a direct setting for each permission.

For Authenticated Users, there is always a row for every permission, because Authenticated Users has an inherited setting for each permission.

For other identities, there is a row for each direct setting. For example, if UserA has a direct grant of the Select permission, there is a Select row for UserA.

Provide Public Access to a Caslib

To give all users access to a new global caslib that you added:

1. On the Configuration page, select Access Controls.
2. In the Caslibs pane, select the caslib.
3. Click Edit.
4. In the Edit Access Controls window, adjust settings as follows:
   a. In the Authenticated Users row for Read Info, select the Grant radio button.
   b. Click Add Row. In the new row at the end of the page, select Authenticated Users, the Grant radio button, and the Select activity.
   c. To also provide Write access, add rows that grant the following additional permissions to Authenticated Users: Insert, Update, Delete, Create Table, Drop Table, Delete Source, Alter Table, Limited Promote, Promote Table (Promote).

   **TIP** As an alternative to adding each row individually, click Add Set, and select Add Set from the drop-down list. In the new Authenticated Users rows for Alter Caslib and Manage Access, click to delete those direct access controls. In the remaining new rows, select the Grant radio button.

Note: To provide access to guest users, you must grant access to Guest. Guest is not affected by access controls that are assigned to Authenticated Users. By default, guest access is not enabled.

5. Click OK to save your changes.
6. Under Access Controls, review the results of your changes.

Selectively Grant Access to a Caslib

This example gives UserA Read and Write access to a new global caslib that you added:

1. On the Configuration page, under Access Controls, select the caslib.
2. Click Edit.
3 In the **Edit Access Controls** window, click **Add Set**, and select **Add User Set** from the drop-down list.

4 In the next window, enter **UserA** in the **User name** field. Click **OK**.

5 In the **Edit Access Controls** window, select the **Grant** radio button in each **UserA** row, except the **Alter CASLib** and **Manage Access** rows.

6 At the end of UserA’s **Alter CASLib** and **Manage Access** rows, click \( \text{✓} \).

7 Click **OK** to save your changes.

8 Under **Access Controls**, review the results of your changes.

---

Note: UserA does not have rows for **Alter CASLib** and **Manage Access**, because you did not give UserA direct access controls for those permissions. Unless UserA is a member of a group that has direct access controls for those permissions, UserA’s effective access for those permissions comes from Authenticated Users.

---

Here are some additional details about editing access controls:

- To add a single row, click **Add Row**.
- To provide a complete set of editable rows for an identity, click **Add Set** and then select the appropriate item:
  - For a group, select **Add Group Set**.
  - For a user, select **Add User Set**.
  - For Authenticated Users, select **Add Set**.
  - For guest users, select **Add Guest Set**.

  Note: By default, guest access is not enabled.

- To delete a direct access control, click \( \text{✗} \).
- You cannot change or delete inherited settings. You can add a direct access control that has precedence over an inherited setting.

---

### Selectively Limit Access to a Caslib

---

### About Setting Direct Denials

**CAUTION**

**Identity names that you enter are not validated.** For sensitive data, do not grant access to Authenticated Users and then rely on selective direct denials. The safer practice is to verify that access is broadly denied, and then grant access selectively.

---

**CAUTION**
**Do not block your own access.** Before you add a direct denial for a group that you belong to, make sure you have a higher precedence (offsetting) direct grant. If you are a CAS administrator (Superuser) or Data administrator, this precaution is not strictly necessary.

---

**Block All Access for an Identity**

1. On the **Configuration** page, under **Access Controls**, select the caslib.
2. Click **Edit**.

   **Note:** If the **Edit** button is disabled, you are not authorized to set permissions for the selected caslib.

3. In the **Edit Access Controls** window, click **Add Row**.
4. In the new row, select an identity type, enter a name (unique identifier), make sure the **Deny** radio button is selected, and select the **Read Info** activity.
5. Click **OK** to save your changes.
6. Under **Access Controls**, review the results of your changes.

---

**Block Write Access for an Identity**

1. On the **Configuration** page, under **Access Controls**, select the caslib.
2. Click **Edit**.

   **Note:** If the **Edit** button is disabled, you are not authorized to set permissions for the selected caslib.

3. In the **Edit Access Controls** window, click **Add Set**, and select **Add Group Set** or **Add User Set**.
4. In the next window, enter the user or group name (unique identifier). Click **OK**.
5. In the identity’s **Read Info** and **Select** rows, click **[ ]**.
6. In the identity’s remaining rows, make sure that the **Deny** radio button is selected.
7. Click **OK** to save your changes.
8. Under **Access Controls**, review the results of your changes.

---

**Resolve Duplicate Access Controls**

You cannot save more than one direct setting for a particular caslib, principal, and permission. Here are examples:

- You cannot save two direct grants of the Update permission for UserA on caslibA.
You cannot save both a direct denial and a direct grant of the ReadInfo permission for UserA on caslibA.

If the error message Access control has duplicates is displayed twice in the Edit Access Controls window, there is one duplicate direct setting. Delete one of the settings that have the error message. One error message remains. You can now save your changes by clicking OK again.

See Also

- SAS® Viya Administration: CAS Authorization
Manage CAS Roles

Only members of the Superuser (CAS) role can manage CAS roles.

Preliminary Navigation

1. On the vertical navigation bar in CAS Server Monitor, click.
2. On the Configuration page, select Administrators.

Here are details about the display:

- In CAS Server Monitor, the Superuser role is referred to as the CAS role.
- In CAS Server Monitor, you do not explicitly assume a role. Your roles are assumed for you as needed.

Add a Member to a Role

1. Click Add.

   Note: If the Add button is not present, you are not signed in as a member of the Superuser (CAS) role.

2. In the Add Administrator window:
   a. Enter a user or group name.

      Note: The name that you enter is not validated. You can enter any user or group name from your identity provider.

   b. Select the corresponding identity type (User or Group).

   c. Select a role type (Data or CAS).

3. Click OK to save your changes.

4. Verify that full administrative privileges are available when designated users sign in to CAS Server Monitor. For example, any user who sees the Add button on the Administrators tab is a member of the Superuser (CAS) role.
Change a Role Assignment

1  Click in the appropriate row, and select **Modify**.

   Note: You cannot change the assignment for the account that starts the server.

2  In the Edit Administrator window, select **Data** or **CAS**, and click **OK**.

Remove a Role Assignment

To remove a role assignment, click in the appropriate row, and select **Delete**.

   Note: You cannot remove the account that starts the server.

See Also

“CAS Roles” in *SAS Viya Administration: SAS Cloud Analytic Services*
Manage CAS Nodes

Note: This topic applies to a distributed CAS server only.

Preliminary Navigation

1. On the vertical navigation bar in CAS Server Monitor, click
2. On the System State page, select Nodes.

View Information

Next to the node that you want to view process information about, click , and select Show Processes.

Add a Node

Only members of the Superuser (CAS) role can perform this task.

Note: Before you add a new node to your cluster, you must add the CAS worker node software to the machine. See "Convert SMP CAS Server to MPP CAS Server" in SAS Viya Administration: SAS Cloud Analytic Services.

1. Click Add Nodes.

   Note: If the Add Nodes action is not available, you are not signed in as a member of the Superuser (CAS) role.

2. In the Add Nodes window, enter a host name (such as mygrid011) in the Hostname field, and click OK.

   CAS Server Monitor runs the CAS addNode action, which starts (or restarts) the node and adds it to the cluster.

   Here are details:
   - Separate multiple host names with a comma.
   - If your hosts are named in numeric order (for example, host002, host003, and so on) you can enter a range of host names. Use the following form:
Remove a Node

Only members of the Superuser (CAS) role can perform this task.

The process of removing a node preserves active and backup copies of table blocks before the node is removed. It requires that all sessions complete their actions and then pause before the blocks are moved. Long-running actions are canceled, and occasionally, a session might need to be killed so that the action can proceed. The redistribution of data often takes only a few minutes.

Next to the node that you want to remove, click ☐, and select Remove Nodes.

CAS Server Monitor runs the CAS removeNode action, which stops the node and redistributes its data to other nodes in the cluster.

**TIP** Removing a node is best suited for times when the system is mainly processing batch jobs, where a delay is not a concern.

Stop a Node

Only members of the Superuser (CAS) role can perform this task.

**CAUTION** Stopping a node might not release resources (for example, mapped memory and memory involving database connections, and so on). Before you stop a node, try to remove the node.

Next to the node that you want to stop, click ☐, and select Terminate Server Instance.

CAS Server Monitor runs an action to immediately kill the node.

See Also

“Distributed Server” in SAS Cloud Analytic Services: Fundamentals
Manage CAS User Sessions

Preliminary Navigation

1. On the vertical navigation bar in CAS Server Monitor, click [Menu].

Here are details about the display:

- To obtain the current list of sessions, click ![Refresh](https://example.com). Sessions that are terminated are removed from the list.
- The session view is displayed until you close it. It is also displayed even if the session has terminated.

Cancel a Session

At the end of the row for the session that you want to cancel, click ![Cancel Session](https://example.com), and select Cancel Session.

Note: Only members of the Superuser (CAS) role can cancel a session for another user.

Terminate a Session

**CAUTION**

Terminating a session might not release resources (for example, mapped memory and memory involving database connections, and so on). Before you terminate a session, try to cancel the session.

At the end of the row for the session that you want to terminate, click ![Terminate Session](https://example.com), and select Terminate Session.

See Also

“Sessions” in SAS Cloud Analytic Services: Fundamentals
View Server Information

View Configuration File Options

1. On the vertical navigation bar in CAS Server Monitor, click 

2. On the Configuration page, select CAS Configuration.
   The current list of CAS Server options and their values is displayed.

View Properties and System Information

1. On the vertical navigation bar in CAS Server Monitor, click 

2. On the System State page, select Controller.

   IMPORTANT After a CAS license is renewed, the License File field is not updated until the CAS server is restarted.

View Start-Up Options and Environment Variables

1. On the vertical navigation bar in CAS Server Monitor, click 


See Also

- SAS Viya Administration: SAS Cloud Analytic Services
Remove CAS Worker Software

1. Remove the CAS worker node whose software you want to remove. See “Remove a Node”.

2. Remove the CAS worker software. See steps 3-7 in “Remove CAS Worker Software” in SAS Viya Administration: SAS Cloud Analytic Services.
Troubleshooting

Insufficient Disk Space (CAS_DISK_CACHE)

**Issue:** An upload fails with a message such as Failed to open temporary file for upload (80BFE801): /tmp/cascache1/_f_43d6c87c_7f5d854996e8.sas7bdat

**Explanation:** Disk space in CAS_DISK_CACHE on the CAS controller is insufficient.

**Resolution:** Add disk space.

Cannot Access the Permstore

**Issue:** An attempt to start a server fails with a message that indicates that a CAS server that is already running. This message is displayed: exclusive access to the access control storage location

**Explanation:** This error message is displayed when a CAS server fails to access the permstore and terminates because the permstore is already being accessed by another CAS server.

Cannot Monitor CPU Usage for a Session

**Issue:** On the Resource Monitor page, the session view stops responding while processing session node information.

**Explanation:** Your browser might interpret a coordinate as a Not-a-Number value, which prevents the display of the graph.

**Resolution:** If you are using Google Chrome, try a different browser such as Microsoft Edge.

Delay in Execution of a Data Quality Operation

**Issue:** The first data quality operation that is performed after CAS starts takes longer than normal to execute.

**Explanation:** Data quality operations require access to the CAS table containing the QKB on all workers in the analytics cluster. Loading this table takes longer for the first data quality operation after CAS starts because the table has not been loaded before. (Subsequent loads take less time.) CAS automatically loads this table when it starts. However, CAS tables for all non-default QKBs are not loaded automatically.

**Resolution:** If CAS sessions use non-default QKBs, load these non-default QKBs as part of starting CAS. In the CAS configuration file, casstartup_usermods.lua, add a qkb.loadQKB() action for each non-default QKB.