SAS® Viya™ 3.2 Administration: Orientation to Authorization

Two Authorization Systems **2**
- Introduction 2
- Similarities 2
- Differences 2
- Influences 3
- Key Terms 3
- Demonstration 3

Impact of Assumable Memberships **7**
- Introduction 7
- Effective Access 7
- Access Outcomes 7
- Demonstration 7

Two Authorization Systems

Introduction

Note: This topic is not applicable to a programming-only deployment because that type of deployment does not include the general authorization system.

Authorization is the aspect of security that determines which resources are available to which users. This document introduces the SAS Viya authorization layer, which consists of two authorization systems:

- Cloud Analytic Services (CAS) authorization system
- general authorization system

Each system uses a distinct model to protect a distinct class of resources.

Similarities

- Both systems can share the same identity provider.
- Both systems implicitly disallow any access that is not granted.
- Both systems can be administered in SAS Environment Manager.

Differences

	CAS Authorization System	General Authorization System
Basis:	DBMS-style access control.	Attribute-based access control.
Targets:	CAS objects, such as caslibs and tables.	Most other objects, such as folders and reports.
Inheritance:	Through a hierarchy of objects (for example, from a caslib to its tables).	Through a hierarchy of containers (for example, from a folder to its members).
Precedence:	By object hierarchy (closest wins), then by identity type (user wins), and then by type of setting (denial wins).	By type of setting (Prohibit always wins).
Row-level access:	You can attach a filter to a grant of the Select permission on a table.	(Not applicable).
Conditional access:	(Not applicable).	You can attach a Boolean expression to any rule.
Highest privileges:	An assumable role (Superuser) is exempt from all authorization requirements throughout a CAS server.	An assumable group (SAS Administrators) is granted broad access throughout the general authorization system.*

* The SAS Administrators group is not unrestricted (exempt from authorization requirements). Access is provided by a predefined rule.

Influences

In the CAS authorization system, memberships, inheritance, and row-level filters can influence access.

In the general authorization system, information about the requesting user , the target resource, and the environment can influence access. Each access request has a context that includes environmental data such as time and device type. Environmental constraints can be incorporated using conditions.

Key Terms

Access control or rule	A composite of authorization elements. CAS example: An access control grants the ReadInfo permission to groupA on caslibA. General example: A rule grants the Add permission to groupA on folderA.
Setting	An indication of whether (and to what extent) access is provided. CAS values: Grant, Row-Level Grant, Deny General values: Grant, Conditional Grant, Prohibit, Conditional Prohibit
Permission	A type of access. CAS values: ReadInfo, Select, LimitedPromote, Promote, CreateTable, DropTable, DeleteSource, Insert, Update, Delete, AlterTable, AlterCaslib, ManageAccess General values: Create, Read, Update, Delete, Secure, Add, Remove
Principal	The user, group, or construct to which an access control or rule is assigned. Examples: UserA, GroupA, Authenticated Users
Target	A resource or set of resources. CAS examples: tableA, caslibA General examples: folderA, reportA
Condition	In a conditional rule, the constraint expression. General example: `currentUser() == #preferenceOwner`
Filter	In a row-level grant, the constraint expression. CAS examples: `User='SUB::SAS.Userid',sales>1000`
Effective access	A context-neutral description of the net result of all relevant access controls or rules. Effective access does not incorporate evaluation of conditions. CAS values: Authorized, Not Authorized, Row-Level General values: Authorized, Not Authorized, Conditional
Access outcome	The authorization decision for a specific access request. CAS values: Authorized, Not Authorized, Row-Level Authorization General values: Authorized, Not Authorized

Demonstration

In this demonstration, you enable a set of users to access a caslib and a folder.

- Users can read and write data in the caslib and objects in the folder.
- Administrators can manage the caslib and the folder.

Note: This demonstration assumes that you are a member of the SAS Administrators group, and that the initial settings and memberships for that group are in place.

1. Sign in to SAS, and opt in to your assumable groups.
2. To represent the set of users, create a group.
   a. In the side menu (≡), under **SAS Environment Manager**, click **Users**.
   b. At the top of the navigation pane, make sure **Custom Groups** is selected.
   c. Click ✱.
   d. In the New Custom Group window, enter `groupA` as the name and as the ID. Click **Save**.
   e. In the right pane, click ✎ for the **Members** section.
   f. In the Edit Members window, assign members by moving them to the **Selected Identities** pane. Click **OK**. (In this demonstration, this step is optional.)

   For details, see *SAS Viya Administration: Identity Management*.
3. To hold shared data, add a caslib.
   a. In the side menu (≡), under **SAS Environment Manager**, click **Data**.
   b. In the **View** drop-down list, select **Libraries**.
   c. Click ✱.
   d. In the New CAS Library window, provide information as follows:
      i. Select a server.

      Note: The **Server** drop-down list includes only those servers to which you are authorized to add global caslibs.

      ii. Make sure the selected data source type is **PATH**.
      iii. Enter a path that is relative to and accessible by the CAS server.
      iv. Enter the name `caslibA`.
      v. In the **Data Source** section, make sure the **Enable encryption** check box is not selected.
      vi. Click **Save**.

      For details, see *SAS Viya Administration: Data*.
   e. Give groupA appropriate access to caslibA.
      i. On the **Data** page, in the **Libraries** view, select **caslibA**. Right-click, and select **Authorization**.
      ii. In the Authorization window, click **+**, and add groupA to the window.

      TIP In the **Select Identities** window, make sure **Custom Groups** is selected in the drop-down list. Move groupA to the **Selected Identities** list. Click **OK**.

iii In the Authorization window, notice that groupA has an effective access value of ⊘ (Not Authorized) for all permissions. In the **Access Level** column, adjust groupA's gauge to the **Write** access level.

iv In the table toolbar, click 💾.

v Below the table, click **Close**.

4 To hold shared reports, create a folder.

a In the side menu (☰), under **SAS Environment Manager**, click **Content**.

b In the drop-down list at the top of the navigation pane, make sure **Folders** is selected. Click 📁+ to create a new top-level folder. Enter the name `folderA`.

For details, see *SAS Viya Administration: Content Management*.

c Give groupA access to folderA.

i Select **folderA**, right-click, and select **Authorization**.

ii In the Authorization window, click +, and add groupA.

> **TIP** In the **Select Identities** window, make sure **Custom Groups** is selected in the drop-down list. Move groupA to the **Selected Identities** list. Click **OK**.

iii In folderA's Authorization window, click the effective access icon for groupA's Read permission. In the pop-up window, select **Grant** as the direct setting. Repeat that process for groupA's Add and Remove permissions.

Note: The Unknown icon (◯) is displayed when the net result of an unsaved change is not known. In the general authorization system, adding a direct grant does not always yield a net result of **Authorized**, because any relevant prohibit setting has absolute precedence.

iv In the table toolbar, click 💾. Review the results of your changes.

Note: A gray diamond indicates that a net result comes from a direct setting.

d Give groupA conveyed access to folderA's members.

i In folderA's Authorization window, click the effective access icon in groupA's **Read (convey)** column. In the pop-up window, select **Grant** as the direct setting. Repeat that process in groupA's **Update (convey)** and **Delete (convey)** columns.

ii In the table toolbar, click 💾. Review the results of your changes.

For details, see "Inheritance" in SAS Viya Administration: General Authorization.

e Below the table, click **Close**.

5 (Advanced) View direct rules that affect access to folderA.

a In the side menu (☰), under **SAS Environment Manager**, select **Security** ⇨ **Rules**.

b In the **Filter by** drop-down list, select **Object URI**.

c Click 📂.

d In the Choose an Item window, select **folderA**. Click **OK**.

e To ensure that you are seeing all available information, click 🔄. Notice that there are two rules that target folderA's object URI:

- The rule that grants all permissions to you was automatically generated because you added folderA as a top-level folder. Lower level folders do not have automatically generated rules.
- The first set of changes that you saved in the Authorization window created the rule that grants the Read, Add, and Remove permissions to groupA.

Note: For groups and users, the **Principal** column on the **Rules** page contains IDs, not display names.

6 (Advanced) View direct rules that affect access that folderA conveys to its members.

a At the right edge of the table, click ⋮, and select **Columns**.

b In the **Columns** window, move **Container URI** to the **Displayed columns** pane.

c In the **Displayed columns** pane, select **Container URI**, and click ⤒. Click **OK**.

d On the **Rules** page, select **Container URI** from the **Filter by** drop-down list.

e Click 🗁.

f In the Choose an Item window, select **folderA**. Click **OK**.

g To ensure that you are seeing all available information, click ↻. Notice that there are two rules that target folderA's container URI:

- The rule that grants all permissions to you was automatically generated because you added folderA as a top-level folder. Notice that the generated rule targets both folderA's object URI and folderA's container URI.
- The second set of changes that you made in the Authorization window created the rule that targets folderA's container URI, granting the Read, Delete, and Update permissions to groupA. That rule provides conveyed access to the members of folderA.

Note: The **Rules** page does not display CAS access controls. To generate a list of direct access controls for a CAS object (such as a caslib or table), use the listAcsData action in the Access Control action set. See *SAS Viya: System Programming Guide*.

Impact of Assumable Memberships

Introduction

Most memberships are always in effect. For example, if UserA is a member of GroupA, that membership affects UserA all of the time. UserA cannot temporarily opt in or opt out of experiencing the effects of his membership in GroupA.

The most highly privileged memberships are assumable. Assumable memberships are in effect in only certain circumstances. Here are examples:

- In a programming interface or SAS Environment Manager, members of a CAS role can temporarily experience that role's elevated privileges by assuming that role at any time.
- In a visual interface that is accessed using SAS Logon Manager, members of the SAS Administrators group can temporarily experience that group's elevated privileges by opting in to that group at sign-in time.

For details, see *SAS Viya Administration: Identity Management*.

Effective Access

When you examine effective (net) access for a user who has assumable memberships, information about whether those memberships are currently in effect is not available. Effective access information presumes that all assumable memberships are in effect.

Note: If you examine your own effective access to a CAS object, the results reflect your current status.

Access Outcomes

When a user who has assumable memberships makes an access request, the outcome of that request is affected by whether those memberships are currently in effect.

Demonstration

This demonstration uses SAS Environment Manager to explore the availability of access that you get exclusively through your assumable memberships. This demonstration is not applicable to a programming-only deployment.

Note: This demonstration assumes that you are a member of the SAS Administrators group, and that the initial settings and memberships for that group are in place.

1. Examine the availability of your elevated privileges in the general authorization system.
   a. If you are currently signed in to SAS, click your user name in the banner, and select **Sign out**.
   b. In the Sign in to SAS window, click **Sign In**, and sign back in. In the Assumable Groups window, click **No**.
   c. In the side menu (≡), under **SAS Environment Manager**, notice that there is no **Users** item.
   d. Sign out, and then sign in again. In the Assumable Groups window, click **Yes**.
   e. In the side menu (≡), under **SAS Environment Manager**, notice that additional items are present, including a **Users** item.
2. Examine the availability of your elevated privileges in the CAS authorization system.

a In the side menu (≡), under **SAS Environment Manager**, click **Data**.

b In the **View** drop-down list, select **Servers**.

c Select a CAS server, right-click, and select **Properties**.

i In the Server Properties window, notice that none of the sections have an edit icon (✎).

ii Expand the **Superuser Role Membership** section. Verify that you are an indirect member of the Superuser role through your membership in the SAS Administrators group.

iii Click **Close**.

d Right-click the CAS server again, and select **Assume the Superuser role**. Notice that a message at the bottom of the page indicates your elevated status.

e Right-click the CAS server again, and select **Properties.** Notice that several of the sections have an edit icon (✎). Click **Close**.

Note: The Superuser role provides unrestricted access to all objects and actions within a CAS server.

f Right-click the CAS server again, and select **Relinquish the Superuser role**.

3 Examine the relationship between your assumable memberships in the SAS Administrators group and the Superuser role.

a Click your user name in the banner, and select **Sign out**.

b Sign back in. In the Assumable Groups window, click **No**, so that your membership in the SAS Administrators group is not in effect.

c Navigate back to the **Servers** view on the **Data** page in SAS Environment Manager.

d Select the CAS server that you used in the preceding steps, right-click, and select **Assume the Superuser role**. A message indicates that you cannot assume the Superuser role in your current session.

Note: Initially, your membership in the Superuser role is indirect, through the SAS Administrators group. If you opt out of your assumable membership in SAS Administrators, you do not experience any of the privileges that you obtain exclusively from that membership.

TIP If you want to always be able to assume the Superuser role, add yourself to that role in a way that does not involve the SAS Administrators group. For example, make yourself a direct member of the Superuser role.