SAS® Viya™ 3.3 Administration: What's New

What's New in Administration of SAS Viya 3.3: Highlights

Here are the key administrative features that are introduced in SAS Viya 3.3:

- By default, data in motion is protected. You can increase the default security by replacing the default certificates with custom certificates and upgrading the default cryptography. See *Encryption in SAS Viya: Data in Motion*.
- You can enable guest users to view reports. See *SAS Viya Administration: Authentication*.
- You can easily script common administrative tasks. See *SAS Viya Administration: Command-Line Interfaces*.
- You can easily import and manage batch loading of data with provided job definitions. See *SAS Viya Administration: Data*.
- You can use a new common interface to import data. See *SAS Data Explorer: User's Guide*.
- You can load Geographic Polygon data as a CAS table.
- You can manage your stored credentials (personal passwords). See *SAS Viya Administration: External Credentials*.
- At installation time, you can enable support for multiple tenants in a single deployment. See *SAS Viya Administration: Multi-tenancy*.
- In SAS Environment Manager, you can customize the administrative dashboard, view new widgets on the dashboard, and view new administrative reports. New and enhanced interfaces help you manage licenses, view logs, monitor machines, schedule jobs, perform backups, manage personal passwords, and manage user-defined formats. See *SAS Viya Administration: Using SAS Environment Manager*.

See Also

- *What's New in SAS 9.4 and SAS Viya*
- "What's New In Administration of SAS Viya 3.3: Details" on page 2

What's New In Administration of SAS Viya 3.3: Details

This topic provides details. A summary of highlights on page 1 is available.

Authorization

- You can use a command-line interface to script CAS access controls and general authorization rules.
- You can view information about the source of an effective access result.
  - In CAS authorization, origins information identifies the highest precedence access control (or access controls) that cause a particular result.
  - In general authorization, origins information identifies all rules that are applicable to a particular result.
- You can preview the results of your unsaved changes to CAS access controls and general authorization rules.
- In the initial configuration, only members of the SAS Administrators group can create top-level folders.
- In SAS Environment Manager, the **Rules** page provides faceted filtering and paged results.
- In SAS Environment Manager, the **Rules** page no longer supports sorting of the data within a column.
- In SAS Environment Manager, the filtering on the **Rules** page is now case-sensitive.
- In SAS Environment Manager, the Authorization windows always include a row for you, the currently connected user.
- In CAS authorization, the Access Control action set has the following new actions:

startTransaction	Initiates an access control transaction in the current client session. Within a transaction, changes are private. Within a transaction, only exclusively reserved (checked-out) objects and their children can be updated. A transaction terminates when it is committed or rolled back.
checkOutObject	Reserves an object (and all of its children) for update by only the current client session. Prevents an object (and all of its parents) from being checked out exclusively by another session if checkOutType=Shared .
commitTransaction	Persists all changes in an access control transaction to the server, releases all checked-out objects, and terminates the transaction.
rollbackTransaction	Discards all changes in an access control transaction, releases all checked-out objects, and terminates the transaction.
statusTransaction	Shows whether client session has an active transaction.
whatCheckoutsExist	Lists check-outs held on an object, its parents, and its children.
checkInAllObjects	Releases all objects that are checked out. Use this action if the current client session does not have a transaction.

- In CAS authorization, the accessControl.whatIsEffective and accessControl.listAllPrincipals actions have a new parameter, includeMyInfo.

- In CAS authorization, the Anonymous identity type is replaced with the Guest identity type.
- In CAS authorization, when you examine your own effective access information, the returned information does not reflect your CAS role status.
- In CAS authorization, roles no longer provide unrestricted access to data.
- In CAS authorization, the way that access controls for database caslibs are stored has changed. After you upgrade from SAS Viya 3.2, see "Preserve Access Controls for Database Caslibs" in SAS Viya for Linux: Deployment Guide .
- In general authorization, a new principal type, Guest, facilitates guest access.
- In general authorization, the Update permission on a parent is no longer required in order to move a member to a different location.

Encryption

- You can encrypt data at rest with additional encryption options. By default, data at rest is presumed to be behind the firewall and is not encrypted.
  - To manage encryption of data files interactively, use SAS Environment Manager.

    To programmatically encrypt data files, use the CASLIB Statement.
- For data in motion, in a full deployment of SAS Viya, all external communication paths are secured by default. You can increase the level of security provided by default in the following ways.
  - The default Apache httpd (reverse proxy server) security configuration can be strengthened. You can replace the default self-signed certificates with your own custom certificates and can strengthen the default cryptography.
  - Trusted CA certificates used for connecting to CAS are signed by HashiCorp Vault-generated root CA and intermediate certificates. These default certificates can be replaced with your own custom certificates post deployment.
  - You can take steps to enable TLs encryption between the data provider (for example, Hadoop or Teradata) and the CAS server, If you are using a SAS Data Connect Accelerator, the data that is transferred between the data provider and the CAS server is not encrypted by default.
  - You can use Ansible utilities to update certificates and distribute them to the truststores in the deployment.

Licensing

- You can use a command-line interface to query SAS license information.
- In SAS Environment Manager, the new **Licensed Products** page provides faceted filtering and paged results.

SAS Environment Manager

Dashboard

- New widgets are provided on the **Dashboard** to monitor the availability of machines, services, and service instances; to view the number of log messages from the top five producers; and to access system monitoring reports.
- You can customize the **Dashboard** by choosing which widgets and predefined system reports to display.

- You can select reports to pin to the **Dashboard** so that the report is displayed together with the predefined system reports.

Monitoring

- In SAS Environment Manager, the availability of machines, services, and service instances is displayed on the **Dashboard**.
- In SAS Environment Manager, the new **Machines** page enables you to view CPU usage and memory usage for each machine.
- In SAS Environment Manager, the **Machines** page enables you to view the status of health checks for each machine.
- In SAS Environment Manager, the **Machines** page enables you to view the status of each service running on each machine.
- In SAS Environment Manager, the **Machines** page displays the properties, system metrics, SAS packages, and system limits for each machine.
- In SAS Environment Manager, reports are provided from the **Dashboard** that enable you to view metric data for application activity, CAS activity, disk space, SAS Infrastructure Data Server tables, message queue activity, system activity, and user activity.
- An operations infrastructure monitors and collects metric data, log events, and notification messages; sends the collected information to message queues; and publishes the information to a data mart. The data is then displayed in SAS Environment Manager and can also be used to generate reports.
- Audit data is automatically collected to track access attempts for folders, data plans, CAS management, and CAS data management, and is automatically displayed in system reports.

Logging

- In SAS Environment Manager, a graph on the **Dashboard** shows the number of logged issues from the top five sources over the previous 30 minutes.
- In SAS Environment Manager, the new **Logs** page displays graphs of the number of log messages, a table of log messages, and provides controls to filter the messages by time range, message content, level, and source.

Scheduling

- In SAS Environment Manager, the new **Scheduling** page enables you to schedule a job using time-based criteria.
- In SAS Environment Manager, the **Scheduling** page enables you to run an available job immediately.

Content Management

- In SAS Environment Manager, the **Content** page enables you to export the reports in a folder to a package file.
- In SAS Environment Manager, the **Content** page enable you to import the reports in an exported package file to a folder.
- In SAS Environment Manager, the **Content** page provides the ability to pin a report to the **Dashboard** so that the report is displayed together with the predefined system reports.

Servers and Services

- There is a new SAS Compute Server that enables clients to submit SAS code.
- There is a new SAS Launcher Server that enables you to start processes in the SAS Viya environment.
- There is a new server to manage secrets.
- SAS Cloud Analytics Services (CAS) enables you to define CAS backup controllers to support fault tolerance.
- CAS has been enhanced with session zero processing to enable SAS applications

  that require application-specific configuration and start-up before SAS Cloud Analytic Services begins processing client requests.
- The following CAS server configuration file options have been added:
  - cas.INITIALBACKUPS
  - cas.NODE
  - cas.STARTUP
  - cas.STARTUPDIR
  - cas.TAG
  - cas.TENANTID
- The following CAS server configuration file options have been discontinued:
  - cas.ADDFMTLIB
  - cas.FMTCASLIB
  - cas.TIMEZONE
- In SAS Environment Manager, there is enhanced CAS functionality:
  - You can stop a CAS controller.
  - You can add and remove CAS worker nodes.
- In SAS Environment Manager, the **Contexts** page

  enables you to create server contexts for the SAS Compute and the SAS Launcher servers.
- There are new SAS Cache Locator services (cachelocator and cacheserver) that replace geodelocator and geodeserver.

Tenancy

- You can configure your deployment to comprise multiple tenants. Activating multi-tenancy is a deployment-time decision. Ensure you understand the implications of this choice before deploying.
- Creation and activation (onboarding) of tenants is achieved by running an Ansible playbook.
- As an overall administrator, you can view and manage tenants from SAS Environment Manager.
- You can create tenant-level administrators whose role is day-to-day administration of the specified tenant.
- Each tenant is completely isolated from other tenants. For example, a use-case would be a tenant for your Human Resources department, to guarantee that access to sensitive data is restricted to appropriate personnel.

- All users of all tenants must share a single LDAP server. The provider and each tenant must be described by a single OU. All tenant OUs must be peers in the LDAP system.