



SAS[®] Viya[®] 3.4 Administration: Auditing

Auditing: Overview	1
Auditing: How To	2
View Audit Record Reports and Tables	2
List Audit Records	4
View a Detailed Audit Record	5
View a File of Audit Records	5
Reset Audit Record Extraction	5
Change Auditing Configuration	5
Change the Amount of Data Displayed in the User Activity Report	7

Auditing: Overview

An audit record is generated whenever these types of events occur:

- an action is performed on a resource (such as a folder or a job). Actions include access to the resource and any changes made to the resource (such as updating, creation, or deletion).
- a security-related action occurred, such as logging on to an application or changing an authorization rule

By default, these actions generate audit records:

- resource read failure
- resource created, updated, or deleted
- security actions (logon attempts, logoff attempts, accessing authorization rules, updating authorization rules)

See [“Change Auditing Configuration” on page 5](#) for information about changing the actions that generate an audit entry.

The audit records are stored in the SAS Infrastructure Data Server and, by default, are retained for seven days. Records older than seven days can be archived to a local storage location. See [“Change Auditing Configuration” on page 5](#) for information about changing the archiving behavior.

All audit records contain this information:

2

ID

generated identifier of the audit record

Description

description of the action that is recorded (for example, authorization rule access)

Time Stamp

the date and time that the action occurred

Type

the type of action (such as security or resource)

Action

the action that was performed (such as read, create, or update)

State

the outcome of the action (success or failure)

User ID

the user, application, or service that initiated the action

Trace ID

the trace ID of the record

Properties

information unique to the type of record

Application

the application or service that performed the action

In addition, other fields might be included depending on the type of audit record.

In order to access the information in the audit records, commands are provided to list all of the audit records or to list records based on criteria such as date, application name, and user ID. The command also enables you to view details about a specific audit record. See [“List Audit Records” on page 4](#) for more information.

SAS Viya operations infrastructure also includes a predefined task to process the audit records, create a CSV file of the extracted records, and then create a CAS table with the records. Predefined reports such as the User Activity report enable you to view detailed information about access to reports, applications data, and data plans; in addition to information about access by user and access failures. See [“View Audit Record Reports and Tables” on page 2](#) for more information.

Auditing: How To

View Audit Record Reports and Tables

The User Activity report is available from the SAS Environment Manager Dashboard. You can use it to view graphs and tables of the collected audit record data.

The genAudit task, which runs every two hours (by default), collects information from the audit records that is then used to create the User Activity report. Because the task runs using the credentials of the SAS install user (sas), it collects only those records to which the SAS install user has access. The SAS install user is not a SAS administrator ID. See [“View a File of Audit Records” on page 5](#) for more information about the genAudit task.

Note: This report is not available if you are a tenant administrator.

Follow these steps to view the reports.

- 1 On the SAS Environment Manager Dashboard, select **Show Reports**. A gallery of available reports is displayed at the bottom of the Dashboard.

- 2 Click in the **User Activity** report and select **Open**. Use the control to navigate through the report gallery to locate the **User Activity** report.
- 3 The **User Activity** report contains pages that display the audit information based on different criteria, such as user activity, report access, and data table access. Audit records are retained for seven days, so by default, the report displays information from all of the past seven days. Use the slider on each report page to view information only for a selected time range.

Select the page of the report that contains the type of information that you want to view. These pages are available:

Main

contains thumbnail graphs for the charts **Most active users**, **Activity counts**, **Most active data**, and **User Actions over time**.

Most Active Users

displays the **Most Active Users** and **Activity Over Time** charts, and a table of the audit records ordered by level of user activity. The table does not display audit records from SAS internal users. Select a bar in the **Most Active Users** chart to display the **Activity Over Time** chart for the selected user, and to list the audit records only for the selected user.

Application Usage

displays the **Most used Applications** and **Application Activity** charts, and a table of the audit records orders by level of application activity. Select a bar in the **Most used Applications** chart to display the **Application Activity** chart for the selected application, and to list the audit records only for the selected application.

Report Activity

displays the **Top Report Usage** chart and a table of the audit records for report access. By default, the chart and table display report activity for all users. To view the report usage and audit records only for a specific user, select the user in the **Users** menu.

Data Activity

displays the **Frequently Accessed Tables** chart and a table of the audit records for data table access. By default, the chart and table display data table activity for all users. To view the data table usage and audit records only for a specific user, select the user in the **Users** menu.

Data Plan Activity

displays the **Top Report Usage** chart and a table of the audit records for data plan access. By default, the chart and table display data plan activity for all users. To view the data plan usage and audit records only for a specific user, select the user in the **Users** menu.

Failures

displays the **Failed Requests per Application** and **Failed Activities** charts, and a table of the audit records only for failed requests. By default, the **Failed Activities** chart and the audit records table display failures for all applications. To view the **Failed Activities** chart and audit records for a specific application, select the application's bar in the **Failed Requests per Application** chart.

Details

displays a table of audit records. By default, the table displays all audit records. To filter the table, use the menus at the top of the table to display only those records matching your selected criteria. You can filter by user, application, action, and state, and multiple criteria are allowed

Note: If the User Activity report is blank or displays the message `Cannot find the requested data source`, you must verify that the command-line interface (CLI) was deployed properly in your SAS Viya environment. See [“Edit the Inventory File” in SAS Viya for Linux: Deployment Guide](#) for more information.

By default, the User Activity report displays seven days' worth of data. If you want to change the amount of data displayed in the report, you must change both of these values:

- the `-d` argument on the `genAudit` task, which specifies the number of days' worth of data that is collected from the audit table, copied to the `audit.csv` file, and made available in the AUDIT CAS system data caslib, where it is used in the User Activity report
- the `localRetention` property, which specifies the number of days that audit records are retained in the audit table in the SAS Configuration Data Server before they are archived

See [“Change the Amount of Data Displayed in the User Activity Report” on page 7](#) for more information.

List Audit Records

Use the command `sas-admin audit list` to list all of the audit records that have been collected. Because the list of records that are returned can be long, you can use these options to manage the records that are returned and more easily locate the records that you want to see:

```
sas-admin audit list --limit "number_of_records"
    returns only the specified number of audit records. The default value is 50.
```

```
sas-admin audit list --action action_name
    returns only audit records that contain the specified action
```

```
sas-admin audit list --after YYYY-MM-DDTHH:MM:SS.ssssssZhh:mm
    returns only audit records that occur after the specified date and time
```

```
sas-admin audit list --application application_name
    returns only audit records that contain the specified application name
```

```
sas-admin audit list --application-contains application_string
    returns only audit records whose application name contains the string application_string
```

```
sas-admin audit list --before YYYY-MM-DDTHH:MM:SS.ssssssZhh:mm
    returns only audit records that occur before the specified date and time
```

```
sas-admin audit list --description description
    returns only audit records that contain the specified description
```

```
sas-admin audit list --description-contains description_string
    returns only audit records whose description contains the string description_string
```

```
sas-admin audit list --remote-address address
    returns only audit records that contain the specified remote address
```

```
sas-admin audit list --remote-address-contains address_string
    returns only audit records whose remote address contains the string address-string
```

```
sas-admin audit list --state state
    returns only audit records that contain the specified state
```

```
sas-admin audit list --type type
    returns only audit records that contain the specified type
```

```
sas-admin audit list --user-id user_ID
    returns only audit records that contain the specified user ID
```

```
sas-admin audit list --user-id-contains user_ID_string
    returns only audit records whose user ID contains the string user_ID_string
```

```
sas-admin audit list --user-id-starts-with user_ID_string
    returns only audit records whose user ID starts with the string user_ID_string
```

View a Detailed Audit Record

Use the `sas-admin audit show-info --id` command to display detailed information about a single audit record. The information returned look like this:

```

ID                c680aeed-479c-493d-921d-5bfd1c5921f3
Description       Authorization rule access
Time Stamp       2017-10-04T11:07:51.673Z
Type             security
Action           update
State            success
User ID          sas.folders
Trace ID         0ef7f213f8085b6a
Properties        id : 4b7514e2-eb7b-40f2-97d8-a665e8bdbdae
                 objectUri : /folders/folders
                 principal : sasapp
                 type : GRANT
Application      authorization

```

View a File of Audit Records

The genAudit task is included in the default task list for the SAS Viya operations infrastructure agent server. The task runs automatically every two hours and performs these functions:

- extract the audit records for reports, data plans, CAS management, and CAS access management
- write the extracted audit records to a CSV file in a cache location
- remove audit records in the CSV file from the eighth day of collection
- use the CSV file to create a table in the SystemData caslib called AUDIT

You can use the extracted audit data in the AUDIT table to perform analysis or create reports.

Reset Audit Record Extraction

If the data created by the audit record extraction process becomes corrupted or incorrect, you can reset the extraction process. This action does not alter or remove any of the original audit records. It deletes only the data in the CSV file that is extracted by the genAudit task.


This is an example of a scenario where you should reset the process. The CSV file is designed to hold seven days of audit records, so one step in the process is to remove records only from the eighth day of collection. It does not remove records that are older than the eighth day. If something prevents the genAudit task from running on a particular day, the eighth-day records are not removed, and they remain in the CSV file from that point forward.

You should reset the extraction process if the `sas-ops-agentsrv` process is down for more than 24 hours.


To reset the record extraction process, delete all of the files in the directory `/opt/sas/viya/config/var/cache/auditcli` on the Operations host (as specified in the Ansible inventory.ini file). The genAudit task creates new extracted audit data when the task runs again after two hours.

Change Auditing Configuration

Follow these steps to edit configuration properties that specify aspects of the audit process:

- 1 In SAS Environment Manager, select  **Configuration**.
- 2 In the **View** field, select **Definitions**.
- 3 To change the configuration for how audit records are archived, select **sas.audit.archive** in the definition list.

6

- 4 Click  **Edit**. You can modify these properties:

batchSize

specifies the number of audit records archived at a time.

enabled

specifies whether to archive audit records. If enabled, records older than the specified retention period are removed from the archive table. If not enabled, the records are not archived and remain in the table.

localRetention

specifies the number of days that audit records are retained in the audit table in the SAS Configuration Data Server before they are archived. This property does not change the number of days' worth of audit data that is displayed in the User Activity report.

scanSchedule


specifies the time at which the archive process starts (the default value is 000**?, which specifies midnight each day).

storage.local.destination

specifies the location where archived records are stored if the **storageType** property is set to **local**.

storageType

specifies whether records that are removed from the table are archived to a file (specify a value of **local** and specify a location in the **storage.local.destination** property) or discarded (specify a value of **none**).

- 5 Select **Save** to save your changes.
- 6 To change the configuration for the actions that generate an audit record, select **sas.audit.record** in the definition list.
- 7 Click  **Edit**. You can modify these properties:

application

specifies recording of entries from a specified application or service. Select **+ Add property** to add a property for an application. In the Add Property window, specify the property in the **Name** field using the format `sas.audit.record.application.application.enabled`. Specify the value for the property in the **Value** field.

For example, specify `sas.audit.record.application.identities.enabled` in the **Name** field and `false` in the **Value** field to disable recording of entries from the Identities service.

type

specifies recording of entries for a specified action or audit type. Select **+ Add property** to add a property for an application. In the Add Property window, specify the property in the **Name** field.

For actions, use the format `sas.audit.record.type.resource.action.action_type.enabled`. Specify the value for the property in the **Value** field. For example, specify `sas.audit.record.type.resource.action.read.enabled` in the **Name** field and `false` in the **Value** field to disable recording of all read records.

For audit types, use the format `sas.audit.record.type.audit_type.enabled`. Specify the value for the property in the **Value** field. For example, specify `sas.audit.record.type.resource.enabled` in the **Name** field and `false` in the **Value** field to disable recording of all resource records.

- 8 Select **Save** to save your changes.

See “[Configuration Properties: How to Configure Services](#)” in *SAS Viya Administration: Configuration Properties* for more information.

Change the Amount of Data Displayed in the User Activity Report

By default, the User Activity report displays seven days' worth of data. If you want to change the amount of data displayed in the report, you must change both of these values:

- the `-d` argument on the `genAudit` task, which specifies the number of days' worth of data that is collected from the audit table, copied to the `audit.csv` file, and made available in the AUDIT CAS system data caslib, where it is used in the User Activity report.
- the `localRetention` property, which specifies the number of days that audit records are retained in the audit table in the SAS Configuration Data Server before they are archived.

Follow these steps to change the number of days' worth of audit data that is displayed in the User Activity report.

- 1 Export the current ops-agent task list. Use this command:

```
/opt/sas/viya/home/bin/sas-ops-agent export -name ops-agentsrv
-tasks /tmp/ops-agentsrv-tasks.json
```

- 2 Edit the file `/tmp/ops-agentsrv-tasks.json` and locate the entry for the `genAudit` task.

```
{
  "version": 1,
  "taskName": "genAudit",
  "description": "Extract audit records. Generate a CSV files for given
applications",
  "hostType": "any",
  "runType": "periodic",
  "frequency": "2h0m0s",
  "visibility": "all",
  "controlAccess": "read update",
  "roles": "ALL ETL",
  "maxRunTime": "2h30m0s",
  "timeOutAction": "restart",
  "errorAction": "ignore",
  "command": "ev-genaudit",
  "commandArgs": "-a reports,dataPlans,casManagement,casAccessManagement
-l 1000 -d 7",
  "commandType": "ext",
  "publisherType": "none"
},
```

- 3 The value `-d 7` in the `commandArgs` line specifies the number of days of data that `genAudit` extracts from the SAS Infrastructure Data Server SAS Audit service, which is then used in the User Activity report. Change this value to the number of days of data that you want to display (for example, `-d 30` specifies 30 days).

- 4 Save the file `/tmp/ops-agentsrv-tasks.json`.

- 5 Import the revised ops-agent task list. Use this command:

```
/opt/sas/viya/home/bin/sas-ops-agent import -name ops-agentsrv -tasks
/tmp/ops-agentsrv-tasks.json -f
```

- 6 Restart the `sas-ops-agentsrv` service. See [“Start and Stop a Specific Server or Service” in SAS Viya Administration: General Servers and Services](#) for information about restarting the service on Linux. See [“Start and Stop a Specific Server or Service” in SAS Viya Administration: General Servers and Services](#) for information about restarting the service on Windows.

8

- 7 Verify that the task was modified correctly. Use this command to list the genAudit tasks so that you can verify that the task was updated as expected:

```
/opt/sas/viya/home/bin/ops-config -base config/ops-agentsrv list | grep genAudit
```

- 8 Use the steps in “[Change Auditing Configuration](#)” on page 5 to change the localRetention property. The value of the localRetention property should be greater than or equal to the value that you specified in the genAudit task.

Note: If you update your installation of SAS Viya, the changes that you make to the genAudit task are not retained.