# SAS® Viya® 3.4 Administration:
Backup and Restore

## Overview
- Introduction to Backup and Restore ........................................... 2
- What Is Backed Up? ............................................................... 2
- What Is Not Backed Up? ......................................................... 3

## Concepts
- Default File Locations .......................................................... 4
- Backup and Restore Terms ..................................................... 4
- Roles and Permitted Tasks ..................................................... 7
- About Default Backup and Binary Backup .................................. 8
- Tenancy and Backup and Restore ............................................ 9
- The Backup Directory Structure .............................................. 10
- Purge Backups ................................................................. 11
- SAS Infrastructure Data Server, High Availability, and Backup and Restore ....................................................... 12

## User Interface of SAS Backup Manager
- View SAS Backup Manager .................................................... 12
- Understand SAS Backup Manager .......................................... 12
- View History of Backup and Restore ....................................... 13
- View Details of a Backup or Restore as a SAS Administrator or as a Tenant Administrator ......................... 14
- View Details of a Backup or Restore for a Tenant as a Provider Administrator .................................................. 15

## Canceling a Backup ............................................................ 15

## Using the Command-Line Interface (CLI)
- Overview ............................................................................. 16
- Examples of CLI Commands for Backup ..................................... 16
- Examples of CLI Commands for Backup (Provider Administrator Only) .......................................................... 16
- Examples of CLI Commands for Restore .................................... 17
- Examples of CLI Commands for Restore (Provider Only) ............. 17

## Initial Tasks ............................................................................. 18

## Managing the Backup Configuration and Schedules
- Manage the Backup Configuration .......................................... 19
- Manage Backup Schedules ..................................................... 22

## Performing a Backup ............................................................ 24
Overview

Introduction to Backup and Restore

SAS Viya can be deployed with other SAS software at your site to gain insight from analytics and business intelligence. SAS Viya consists of many software components (including SAS Cloud Analytic Services (CAS)), servers and services (including SAS Compute Server, SAS Launcher Server, Identities service, and Audit service). You should have a strong backup and restore strategy and validate your backup and restore processes regularly. This ensures that your backup process is operational and that a restore can be successfully performed. A backup strategy should include tasks for backing up all software components and data in addition to running the Backup service.

You can run the Backup service functionality through the SAS Backup Manager or using a backup command-line interface (CLI). After SAS Viya is deployed, a backup schedule is created for the Backup service. Scheduled backups are automatically performed at specified times. In addition to scheduled backups, you can perform an immediate backup. From these backups, you can successfully restore your system if necessary.

What Is Backed Up?

- Content that users have generated and saved in the SAS Infrastructure Data Server is backed up. Content can be reports (including SAS Visual Analytics reports), comments, authorization rules, attachments, audit records, user preferences, and data source definitions. Content in any additional and required SAS Infrastructure Data Server instances is backed up.

- Infrastructure configuration settings and application configuration settings that you defined based on your business requirements are backed up. These settings are saved in the SAS Configuration Server. Infrastructure configuration settings include IP addresses, hostnames, paths, ports, and certificates.
Application configuration settings include user interface (UI) themes (for example, the SAS Visual Analytics UI theme), purge frequency, schedule frequency, and batch run date (for example, batch date of running SAS Visual Analytics reports).

- All SAS Message Broker exchanges, queues, bindings, users, virtual hosts, permissions, and parameters are backed up. Actual messages are not backed up.
- If CAS is configured for data management and analytics, CAS access controls and caslibs are backed up. Caslibs help with accessing data from a data source. A caslib consists of a data source definition and can include access controls. Access controls help with controlling user access to the data.
  
  In a clustered environment, caslibs and access controls of the CAS primary node are backed up.

All of this information might reside on a single host or on different hosts.

**What Is Not Backed Up?**

Backup and Restore does not support the backup and restore of several items. You must take alternative steps to back up and restore these items.

- **the operating environment**
  
  In the operating environment, the operating system libraries and packages, environment variables, kernel settings, user identifiers (UIDs), group identifiers (GIDs), mount points, symbolic links, the Windows registry, Windows security and local security policy settings, Windows users and groups, file systems, and so on, are not backed up.

- **SAS Viya deployment**
  
  In the SAS Viya deployment, the deployment files that are included as part of the SAS Viya deployment (such as scripts, executable files, binaries, and so on), the SAS installation directory, and the SAS configuration directory are not backed up.

- **User home directories**

- **Third-party applications that are used with SAS Viya**

- **Data sources, such as:**
  
  - Files for predefined caslibs in `/opt/sas/viya/config/data/cas/default/`
  - Third-party databases
  - Data that is stored outside of the SAS Infrastructure Data Server
  - SAS Infrastructure Data Server metadata such as database user information, roles, and permissions that are stored in the SAS Infrastructure Data Server
    
    If a binary backup is run, SAS Infrastructure Data Server metadata is backed up.
  - Data that is loaded to CAS
  - Data that is stored on local file systems (such as SAS data sets)
    
    For example, suppose that the SAS deployment contains Model Studio. Model Studio uses a SAS data set stored on the local file system and you back up the SAS deployment. To ensure that Model Studio has access to the SAS data set, you must manually back up the SAS data set that is stored on the local file system and restore it in an appropriate location on the target environment.
  - Data that is stored on remote file systems (such as path-based data sources including PATH, DNFS, and HDFS)
  - Database data sources (such as Oracle, ODBC, and Hive)

- **In a clustered CAS environment, CAS access controls and caslib information for the secondary CAS controller**
You do not need to manually back up the CAS access controls and caslib information for the secondary CAS controller because the `permstore` directory for the secondary controller (that contains the CAS access controls and caslib information) is always in sync with the `permstore` directory of the primary controller.

SAS Message Broker messages

Messages are not backed up.

## Concepts

### Default File Locations

After SAS Viya is installed, installation files are stored in a default location referred to as **SASHome**. For example, on Windows, SASHome is `C:\Program Files\SAS\Viya`.

Configuration files are stored in a default location referred to as **SAS-configuration-directory**. For example, on Windows systems, the SAS configuration directory is `C:\ProgramData\SAS\Viya`.

The following table lists the default locations of installation and configuration files.

<table>
<thead>
<tr>
<th>Location</th>
<th>Example Path on Windows System</th>
<th>Example Path on Linux System</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAS-configuration-directory</td>
<td><code>C:\ProgramData\SAS\Viya</code></td>
<td><code>/opt/sas/viya/config</code></td>
</tr>
<tr>
<td>SASHome</td>
<td><code>C:\Program Files\SAS\Viya</code></td>
<td><code>/opt/sas/viya/home</code></td>
</tr>
</tbody>
</table>

### Backup and Restore Terms

#### Common Terms

Here is a list of backup and restore terms that are used in a standard deployment on Windows and on Linux:

- **backup**
  - the backup that can be initiated by a SAS administrator. SAS Viya can be deployed on Linux and on Windows. There are two types of backup: default and binary. For more information, see Table 2 on page 7.

- **restore**
  - the process of restoring a backup. A SAS administrator can initiate the restore from a backup that is either marked ☑ or ☑.

- **local vault**
  - a local file system path located on the same host where the backup source resides. It is the location where the backup files for the data source are created. They are then moved to the shared vault. The location of the local vault is **SAS-configuration-directory/backup** on Linux and Windows by default and cannot be changed.

  It is a best practice that if a tenant administrator performs a local backup, the tenant administrator should copy the contents (local files) of the local vault to a shared vault.

- **pre-restore validations**
  - validations that are done before performing a restore using a given backup. A pre-restore validation includes the following validation checks:
- Does the provided backup exist?
- Is the backup completed?
- Is the backup purged?
- If SAS Infrastructure Data Server is being restored using the default type of backup, does the list of databases in the backup match the list of databases currently present in SAS Infrastructure Data Server? You can determine the backup contents by submitting the following command:

  `sas-admin backup show -i=<backup_ID>`

- If you are restoring a binary type of backup, was the include-all-sources property set to TRUE?

  The include-all-sources property has different names depending on where you are. In the REST API, it is includeAllSourcesForBinaryBackup. For the command-line interface, it is include-all-sources-for-binary-backup. In the user interface, it is the check box labeled Include remaining sources. It is referred to as the include-all-sources property. For more information, see “Restore SAS Infrastructure Data Server from a Binary Backup Manually” on page 30.

- In a multi-tenant environment where the tenant list is not provided, the Backup service checks to see whether the onboarded tenants and the tenants in the backup match. If the tenant list is provided in the restore request, then the Backup service checks to see whether all of the tenants specified in the restore request are onboarded.

**Retention period**

number of days that backups are stored before they are removed from the shared vault.

**Shared vault**

any network location that preserves the backups from all tiers. Backup files are moved from the local vault to the shared vault. The shared vault is set by the sharedVault property in the Backup service configuration.

The shared vault directory must be accessible from all hosts in the deployment. The locations of the shared vault and local vault must be different.

On Linux, ensure that the sas user has Read, Write, and Execute permissions to the shared vault directory.

On Windows, ensure that the CAS user has Read, Write, and Modify permissions to the shared vault directory.

It is a best practice to back up your shared vault.

**Alternate shared vault**

any alternate network location that contains backups. An alternate shared vault location might be used when performing a restore to an alternate host. The permissions for an alternate shared vault are the same as the shared vault. For more information, see “shared vault” on page 5.

**Standard deployment**

a SAS Viya deployment intended to be used only by a single tenant on Windows and on Linux.

**Slug**

user-provided name for the backup or restore operation.

**State**

state of a backup or restore operation. The possible values are:

- pending indicates that a backup or restore job has been created, but the operation has not yet started.
- running indicates that a backup or restore is in progress.
- completedWithWarning indicates that at least one tenant backup or restore has failed, the CAS controller host is not reachable, or the recovery of SAS Configuration Server is partially successful.
- completed indicates that the backup or restore operation has completed successfully.
- failed indicates that a backup or restore for one or more data sources failed.
- **unknown** indicates that either a backup agent is not installed on the source or the backup agent is not running. If the source does not have a backup agent, contact your administrator. If the source has a backup agent, then restart the Backup service.

- **canceling** indicates that the backup is being canceled. This state is applicable only to a backup.

- **canceled** indicates that the backup is canceled. This state is applicable only to a backup.

**trigger**

an event generated periodically by a scheduler that signals when a new instance of a job should be executed.

---

**Terms for Multi-Tenant Deployment**

Here is a list of backup and restore terms that are used in a multi-tenant deployment on Linux:

**deployment backup**

a multi-tenant deployment on Linux in which only a provider administrator can initiate backup for multiple tenants. If an explicit list of tenants is not provided, all onboarded tenants are backed up.

**deployment restore**

a multi-tenant deployment on Linux in which only a provider administrator can initiate a restore of a deployment backup (with at least one successful tenant backup) for multiple tenants. If an explicit list of tenants is not provided, all onboarded tenants and the provider tenant are restored. If all the tenants in the list are in the backup, then the restore is triggered for each of the tenants in the list. If any of the tenants in the list are not in the backup, then the restore does not proceed and it is marked as failed.

**tenant administrator**

a person within the tenant organization who has administrative privileges for a tenant environment. For example, assigning users to custom groups and managing access to SAS Viya content and CAS data are tenant administrator tasks. The tenant administrator must be a member of the SAS Administrators group to perform the backup and restore functions that are specific to the tenant.

**tenant environment**

a collection of software and the infrastructure for use by a single tenant. Customers might have separate tenant environments to support development, staging, and production instances of SAS services.

**multi-tenant deployment**

a SAS Viya deployment in which multiple tenants can access the same environment in isolation without impacting the data or processes of other tenants. A multi-tenant deployment has the provider tenant by default.

**provider administrator**

a person within the provider organization who has administrative privileges for a provider environment. The provider administrator must be a member of the SAS Administrators group to perform the backup and restore functions for all the tenants in a multi-tenant deployment.

**provider environment**

a collection of software and the infrastructure to support one or more tenant environments.

**provider tenant**

the initial tenant (that is, tenant zero) created when a multi-tenant system is deployed. This tenant has full access to all applications in the deployment, but is intended for provider administrator access only. Users in this tenant have access to information about the entire deployment, including other tenants.

**tenant**

one of the customers using a shared SAS Viya deployment.

In a multi-tenant deployment, a tenant is said to be onboarded when the SAS Viya infrastructure for that tenant is created. This includes the LDAP groups, the LDAP identities, the SAS Infrastructure Data Server databases, the schemas, and the CAS instance.
**alternate shared vault**

any alternate network location that contains backups. In a multi-tenant deployment on Linux, the alternate shared vault contains the backups of all tenants. You might want to use the alternate shared vault to migrate a few tenants or to restore the environment. The permissions for an alternate shared vault are the same as the shared vault.

For more information, see “shared vault” on page 5.

### Roles and Permitted Tasks

The following administrators can perform backups:

**SAS administrator**
- can perform a backup in a standard deployment.

**Provider administrator**
- can perform a backup of all onboarded tenants in a multi-tenant deployment.

**Tenant administrator**
- can perform a backup of that tenant in a multi-tenant deployment.

**Important:** In a multi-tenant deployment, a tenant administrator cannot perform a binary type of backup.

The following table describes the roles and permitted tasks for each role.

<table>
<thead>
<tr>
<th>Task</th>
<th>Standard Deployment on Windows and in Linux</th>
<th>Multi-tenant Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SAS Administrator</td>
<td>Provider Administrator</td>
</tr>
<tr>
<td>View backup configuration</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Edit backup configuration</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>View and edit a default backup schedule</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>View and edit a binary backup schedule</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Perform an immediate default backup</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Perform an immediate binary backup</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Create backup job and schedule it</td>
<td>–</td>
<td>✓</td>
</tr>
<tr>
<td>Perform a restore</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Perform a restore from an alternate host</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
About Default Backup and Binary Backup

Default backup
A default backup can be used in standard and multi-tenant deployments. During a default backup, you can select tenants from a list of tenants in a multi-tenant deployment.
For detailed information about a default backup, see Table 3 on page 8.

Binary backup
A binary backup must be used when you want to restore, but the SAS Infrastructure Data Server is not restarting or is unresponsive.
For detailed information about a binary backup, see Table 3 on page 8.

TIP Whenever you deploy SAS Viya or make changes to an existing SAS Viya deployment, always perform a default backup and a binary backup of the deployment immediately.

The following table describes the default backup and binary backup in detail.

Table 3 Detailed Information About Default Backup and Binary Backup

<table>
<thead>
<tr>
<th>Category</th>
<th>Default Backup</th>
<th>Binary Backup</th>
</tr>
</thead>
<tbody>
<tr>
<td>General information</td>
<td>The default type of backup.</td>
<td>A different type of backup that is not a replacement of the existing default backup.</td>
</tr>
<tr>
<td></td>
<td>Uses the pg_dump utility.</td>
<td>Uses the pg_basebackup utility.</td>
</tr>
<tr>
<td>Backup-related information</td>
<td>Backs up the following source types:</td>
<td>Backs up the content and metadata of the SAS Infrastructure Data Server (such as database users, roles, and permissions).</td>
</tr>
<tr>
<td></td>
<td>- content of SAS Infrastructure Data Server</td>
<td>If the include-all-sources property is set to TRUE while initiating the backup, the binary backup backs up remaining source types (such as SAS Configuration Server, SAS Message Broker, and CAS). For more information about the include-all-sources property, see “pre-restore validations” on page 4.</td>
</tr>
<tr>
<td></td>
<td>- SAS Configuration Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- SAS Message Broker</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- CAS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The default backup does not back up the metadata of the SAS Infrastructure Data Server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A logical backup of each database in the SAS Infrastructure Data Server.</td>
<td>A binary copy of the database files as a TAR archive.</td>
</tr>
<tr>
<td></td>
<td>When a default backup is restored, the Backup service re-creates each database in the SAS Infrastructure Data Server by retaining its state at the time of backup.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In a multi-tenant deployment, you can select the tenants from a list of tenants to perform the default backup.</td>
<td>In a multi-tenant deployment, you can perform a binary backup of the entire deployment that includes all tenants.</td>
</tr>
</tbody>
</table>
### Restore-related information

<table>
<thead>
<tr>
<th>Category</th>
<th>Default Backup</th>
<th>Binary Backup</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use default backup to perform a logical backup of each database in the SAS Infrastructure Data Server.</td>
<td>Use binary backup to perform a binary copy of the database files in a SAS Infrastructure Data Server. The binary copy is a TAR archive.</td>
<td></td>
</tr>
<tr>
<td>A default backup can be restored using the SAS restore operation. The restore operation includes SAS Infrastructure Data Server content, configuration data, and other source types.</td>
<td>The SAS Infrastructure Data Server portion of a binary backup must be restored manually. Suppose that the include-all-sources property is set to TRUE and the manual restore of the SAS Infrastructure Data Server is completed. In such a case, you can then use the restore operation to restore the other portions of the binary backup. For more information about the include-all-sources property, see “pre-restore validations” on page 4.</td>
<td></td>
</tr>
<tr>
<td>Use default backup for restoring to an alternate host or to the same host. You can use SAS Backup Manager or a command-line interface (CLI) to restore a default backup.</td>
<td>Use binary backup to perform a restore on the same host. You cannot use binary backup to restore to an alternate host.</td>
<td></td>
</tr>
<tr>
<td>Do not use default backup if the SAS Infrastructure Data Server is unresponsive.</td>
<td>Always use binary backup when you need to perform a backup and restore and the SAS Infrastructure Data Server does not start or is unresponsive.</td>
<td></td>
</tr>
<tr>
<td>When you use default backup to restore in a multi-tenant deployment, only the tenants that were included in the default backup are restored.</td>
<td>When you use binary backup to restore in a multi-tenant deployment, the entire deployment (that includes all tenants) is restored.</td>
<td></td>
</tr>
</tbody>
</table>

### Tenancy and Backup and Restore

The following table shows the tenancy and deployment type for Linux and Windows.
<table>
<thead>
<tr>
<th>Operating System</th>
<th>Tenancy</th>
<th>Deployment Type</th>
<th>Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Linux</strong></td>
<td>SAS Viya can be deployed for a single tenant and for multiple tenants.</td>
<td>Standard deployment for single tenant.</td>
<td>Members of the SAS Administrators group and individual users can perform backup and restore operations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Multi-tenant deployment for multiple tenants.</td>
<td>A provider administrator can perform backup and restore operations for all tenants. A tenant administrator can perform backup and restore operations for that tenant. The provider administrator and the tenant administrator must be members of the SAS Administrators group.</td>
</tr>
<tr>
<td><strong>Windows</strong></td>
<td>SAS Viya can be deployed for a single tenant only.</td>
<td>Standard deployment for single tenant.</td>
<td>Members of the SAS Administrators group and individual users can perform backup and restore operations.</td>
</tr>
</tbody>
</table>

**Note:** The Backup service does not take the place of operating system backups or file system backups. Furthermore, you cannot use the Backup service when SAS Viya is deployed on a container-enabled infrastructure.

**The Backup Directory Structure**

The following diagram explains the directory structure of the shared vault and how backups are stored within this structure.
Here are some details about the diagram.

1. This is the path of the shared vault. This directory contains the folders for backups.

2. A folder is named using the date and time at which the backup was performed. Each folder contains a folder for every tenant or provider included in the backup. In a standard deployment, only one folder named __default__ exists.

3. In a multi-tenant deployment, a tenantID folder is available.

4. Within each tenant or provider folder, there are folders for each source type to which the tenant or provider has access. Within each source type folder, you can find the backup files for that source type.

5. Within the shared vault, there is a folder named History. The History folder stores history files.

6. Within the shared vault, there is a folder named HistoryArchive. The HistoryArchive folder contains the backup of the History folder after each successful backup or restore operation.

7. The History folder stores the global history file (backuphistory.json) and tenant history files (backuphistory_<tenantId>.json, and so on).

**Purge Backups**

The backups are retained for a period that is set by an administrator. The default value for the retentionPeriod property is 30 days. The retentionPeriod property can be modified by selecting Backup service on the Configuration page in SAS Environment Manager. Click New/Edit Configuration, and then select sas.deploymentbackup.

The last successful backup of each type (regardless of the value for retentionPeriod) is retained. If a binary or default backup is performed for a deployment, the last successful backup for the default type is retained and the last successful backup for the binary type is retained. In a multi-tenant deployment, if a backup was explicitly performed by a tenant after a successful backup (default or binary), that backup is also retained.
Old backups are purged after the retention period. They are deleted from the file system. A previous backup for an onboarded tenant is purged in the next purge cycle after the retention period has passed. In a multi-tenant deployment, the backup of all onboarded tenants is purged after the retention period. The last successful backup of an offboarded tenant is not purged after the retention period. It permanently remains unless it is deleted manually.

**SAS Infrastructure Data Server, High Availability, and Backup and Restore**

By default, SAS Viya does not configure SAS Infrastructure Data Server for high availability. Before you configure it, you should perform a binary backup of the data and rely on that backup for a restore. SAS recommends that you perform a binary backup if the configuration or installation of the SAS Viya environment changes in any way. For information about restoring the SAS Infrastructure Data Server when the server is unresponsive due to SAS Infrastructure Data Server corruption or for any other reason, see “Restore SAS Infrastructure Data Server from a Binary Backup Manually” on page 30.

Suppose that the SAS Infrastructure Data Server is configured for high availability and the primary node is unresponsive. In this case, a standby node is promoted to the primary node, and the SAS Infrastructure Data Server can be started.

**User Interface of SAS Backup Manager**

**View SAS Backup Manager**

1. Log on to SAS Environment Manager as a provider administrator or a tenant administrator in a multi-tenant deployment. Or, log on as a SAS administrator in a standard deployment.

2. In the left pane, click Backup and Restore.

**Understand SAS Backup Manager**

You can perform the following common tasks in the SAS Backup Manager:

- View the history of backups and restores.
- View the backup configuration.

If you log on as a provider administrator in a multi-tenant deployment, you can perform the following tasks in addition to the common tasks:

- View the details of each backup and restore, such as the list of tenants involved in a backup or restore, start and end times, and status of each backup or restore.
- Perform an immediate (ad hoc) backup for all tenants or for selected tenants.
- View the details of a provider-specific backup and restore.
- Perform a restore.

If you log on as a SAS administrator in a standard deployment or as a tenant administrator in a multi-tenant deployment, you can perform the following tasks in addition to the common tasks:

- View the details of each backup and restore, such as the list of data sources in a backup or restore and details of each data source.
- Perform an immediate (ad hoc) backup.
## View History of Backup and Restore

To view the history of backups or restores:

- From View, select **Backup details** or **Restore details**.

By default, backups and restores are listed in descending order by **Local Start Time**. The list of backups and restores provides you with the following information:

- all backups or restores
- backups that have been purged due to retention period
- backups or restores currently running or that are waiting to run

Click 🔄 to refresh the details. The following table describes the information that you can view for each backup and restore.

<table>
<thead>
<tr>
<th>Table 4 Description of Columns in Backup and Restore Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Column Name</strong></td>
</tr>
<tr>
<td>Comments</td>
</tr>
<tr>
<td>Backup ID or Restore ID</td>
</tr>
<tr>
<td>User ID</td>
</tr>
<tr>
<td>Type</td>
</tr>
<tr>
<td>Size</td>
</tr>
<tr>
<td>Local Start Time</td>
</tr>
<tr>
<td>Local End Time</td>
</tr>
<tr>
<td>Status</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
View Details of a Backup or Restore as a SAS Administrator or as a Tenant Administrator

View Details of a Backup or Restore

1. Log on to SAS Environment Manager as a tenant administrator in a multi-tenant deployment. Or, log on as a SAS administrator in a standard deployment.

2. From **View**, select **Backup details** to view a list of all backups or select **Restore details** to view a list of all restores.

3. Select a backup or restore, and click **in the right pane.**

   A pane displays the following information for the selection:
   - Backup ID or Restore ID.
   - Status of the backup or restore.
   - Total size of the files that were backed up. This information is not available for restores.
   - Any comments that were entered before performing a backup or restore.
   - User ID of the user that ran the backup or restore or the identity name of the service that initiated the backup or restore.
   - Local start date and time for the backup or restore.
   - Local end date and time for the backup or restore.
   - Information about the remaining sources if they were included in the binary backup.

View Source Types of a Backup or Restore

1. Log on to SAS Environment Manager as a tenant administrator in a multi-tenant deployment. Or, log on as a SAS administrator in a standard deployment.

2. From **View**, select **Backup details** to view a list of all backups or select **Restore details** to view a list of all restores.

3. Select a backup or restore, and click **in the right pane.**

   The data sources for the selection are listed in the right pane. If you are viewing details for a restore, only the data sources that were restored are listed.

   By default, the data sources include the following:
   - SAS Message Broker (not available for a tenant in a multi-tenant deployment)
   - SAS Configuration Server
   - SAS Cloud Analytic Services
   - SAS Infrastructure Data Server

4. (Optional) Click ** to the left of the data source to view the following information. The icon to the right of the data source displays the status of the backup or restore.
   - Name of the host where the data source is deployed.
   - Status of the data source’s backup or restore.
   - Total size of the files that were backed up for this data source. This information is not available for restores.
View Details of a Backup or Restore for a Tenant as a Provider Administrator

1. Log on to SAS Environment Manager as a provider administrator in a multi-tenant deployment.

2. From View, select Backup details to view a list of all backups or select Restore details to view a list of all restores.

3. Double-click a backup or restore. Alternatively, right-click a backup or restore, and select Tenants.

   The following information is displayed for the selection:
   - Tenant name.
   - Local start date and time for the backup or restore for the tenant.
   - Local end date and time for the backup or restore for the tenant.
   - Status of the backup or restore for the tenant.

4. (Optional) If the provider environment is selected for backup or restore, click to view the details of the provider environment.

   If the provider tenant is included in the backup or restore, the provider administrator can view its details in the Operation Details (Provider) pane.

5. (Optional) If the provider environment is selected for backup or restore, click to view the data sources and the details of each data source that is a part of the provider environment.

   If the provider tenant is included in the backup or restore, the provider administrator can view the data sources of the provider tenant in the Data Sources (Provider) pane.

You can click to view a list of all backups or restores.

Canceling a Backup

The Cancel operation is new for SAS Viya 3.4 (July 2019 upgrade).

1. Using a command line, log on to SAS Viya.


2. Use the following command to cancel a backup:

   ```shell
   sas-admin backup cancel -i=<backup_job_id>
   ```

   On Windows, you can use the Microsoft Management Console Services snap-in to stop the SAS Backup Service.

   A cancel is an asynchronous operation. It returns the current state of the backup. The user can execute the SHOW command to determine whether the backup got canceled.

   ```shell
   sas-admin backup show -i=<backup_job_id>
   ```

   Ensure that the backup has a ◊ state.
Using the Command-Line Interface (CLI)

Overview

Use a command-line interface (CLI) to perform a backup or restore without using SAS Backup Manager in SAS Viya. You can enter commands on a command line and receive responses from the system. For more information, see “Command-Line Interface: Overview” in SAS Viya Administration: Using the Command-Line Interfaces.

Examples of CLI Commands for Backup

The following examples assume that you have already logged on to SAS Viya. For more information, see “Command-Line Interface: Preliminary Instructions” in SAS Viya Administration: Using the Command-Line Interfaces.

Table 5  Examples of CLI Commands for Backup

<table>
<thead>
<tr>
<th>Task</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>List the first 50 backups</td>
<td>sas-admin backup list --limit 50</td>
</tr>
<tr>
<td>Show details of a backup with backup ID</td>
<td>sas-admin backup show -i=2017-10-28T07_23_44_594-0400</td>
</tr>
<tr>
<td>2017-10-28T07_23_44_594-0400</td>
<td></td>
</tr>
<tr>
<td>Obtain help for LIST command for backup</td>
<td>sas-admin backup list -help</td>
</tr>
<tr>
<td>Perform the backup</td>
<td>sas-admin backup start</td>
</tr>
<tr>
<td>Perform a binary backup (back up only SAS</td>
<td>sas-admin backup start -t=binary</td>
</tr>
<tr>
<td>Infrastructure Data Server)</td>
<td></td>
</tr>
<tr>
<td>Cancel the backup.</td>
<td>sas-admin backup cancel -i=2017-10-28T07_23_44_594-0400</td>
</tr>
</tbody>
</table>

Note: Commands to perform a binary backup are not available to a tenant administrator in a multi-tenant SAS Viya environment. Commands to perform a binary backup are available to a provider administrator in a multi-tenant SAS Viya environment and to an administrator in a non-multi-tenant SAS Viya environment.

In a multi-tenant SAS Viya environment, the provider administrator has more command options.

Examples of CLI Commands for Backup (Provider Administrator Only)

The following examples assume that you have already logged on to SAS Viya. For more information, see “Command-Line Interface: Preliminary Instructions” in SAS Viya Administration: Using the Command-Line Interfaces.
Table 6  Examples of CLI Commands for Backup (Provider Administrator Only)

<table>
<thead>
<tr>
<th>Task</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform backup only for provider tenant</td>
<td><code>sas-admin backup start -p</code></td>
</tr>
<tr>
<td>List provider backups</td>
<td><code>sas-admin backup list -p</code></td>
</tr>
<tr>
<td>Show details of a backup with backup ID</td>
<td><code>sas-admin backup show</code></td>
</tr>
<tr>
<td>2017-10-28T07_23_44_594-0400 for provider only</td>
<td><code>-i=2017-10-28T07_23_44_594-0400</code> -p</td>
</tr>
<tr>
<td>Perform backup for acme and cyberdyne tenants</td>
<td><code>sas-admin backup start</code></td>
</tr>
<tr>
<td></td>
<td><code>--tenants=acme,cyberdyne</code></td>
</tr>
</tbody>
</table>

Examples of CLI Commands for Restore

The following examples assume that you have already logged on to SAS Viya. For more information, see “Command-Line Interface: Preliminary Instructions” in SAS Viya Administration: Using the Command-Line Interfaces.

Table 7  Examples of CLI Commands for Restore

<table>
<thead>
<tr>
<th>Task</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show history of restores</td>
<td><code>sas-admin restore list</code></td>
</tr>
<tr>
<td>Show details of a restore with restore ID</td>
<td><code>sas-admin restore show</code></td>
</tr>
<tr>
<td>2017-10-28T07_23_44_594-0400</td>
<td><code>-i=2017-10-28T07_23_44_594-0400</code></td>
</tr>
<tr>
<td>Obtain help for LIST command for restore</td>
<td><code>sas-admin restore list -help</code></td>
</tr>
<tr>
<td>Start a restore of a specified backup, and specify that the name of the restore is restoreA</td>
<td><code>sas-admin restore start</code></td>
</tr>
<tr>
<td></td>
<td><code>--&lt;backup-name&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>&lt;backup-ID&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>--slug restoreA</code></td>
</tr>
<tr>
<td>Start a restore of a specified backup in an alternate shared vault at /alternate/sharedvault</td>
<td><code>sas-admin restore start</code></td>
</tr>
<tr>
<td></td>
<td><code>--backup-name=&lt;backup_ID&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>--alternate-shared-vault-for-restore=/alternate/sharedvault</code></td>
</tr>
</tbody>
</table>

Note: Commands to perform a restore from an alternate shared vault are not available to a tenant administrator in a multi-tenant SAS Viya environment. Commands to perform a restore from an alternate shared vault are available to a provider administrator in a multi-tenant SAS Viya environment and to an administrator in a non-multi-tenant SAS Viya environment.

In a multi-tenant SAS Viya environment, the provider administrator has more command options.

Examples of CLI Commands for Restore (Provider Only)

The following examples assume that you have already logged on to SAS Viya. For more information, see “Command-Line Interface: Preliminary Instructions” in SAS Viya Administration: Using the Command-Line Interfaces.
Table 8  Examples of CLI Commands for Restore (Provider Only)

<table>
<thead>
<tr>
<th>Task</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show the history of restores for provider</td>
<td>sas-admin restore list -p</td>
</tr>
<tr>
<td>Show details of a provider restore with restore ID</td>
<td>sas-admin restore show</td>
</tr>
<tr>
<td>Start a restore of a specified backup in an alternate shared vault</td>
<td>sas-admin restore start</td>
</tr>
<tr>
<td>at /alternate/sharedvault for acme and cyberdyne tenants</td>
<td>--backup-name=&lt;backup_ID&gt; --alternate-shared-vault-for-restore=/</td>
</tr>
<tr>
<td></td>
<td>alternate/sharedvault --tenants=acme,cyberdyne</td>
</tr>
</tbody>
</table>

**Initial Tasks**

Immediately after SAS Viya is deployed, perform the following tasks:

1. Configure the backup by specifying the shared vault location.
   
   Check the default value of the retention period and change it if necessary.
   
   For more information, see “Create and Edit a Backup Configuration” on page 20.

2. In SAS Environment Manager, click Jobs, and then click the Scheduling tab to ensure that the DEFAULT_BACKUP_SCHEDULE and BINARY_BACKUP_SCHEDULE jobs are created.
   
   These jobs are created automatically after SAS Viya is deployed and the Backup service starts.
   
   The DEFAULT_BACKUP_SCHEDULE job is set to run every Sunday at 1:00 a.m. The BINARY_BACKUP_SCHEDULE is set to run on the first Saturday of every month at 5:00 a.m.
   
   For more information about managing backup schedules, see “Manage Backup Schedules” on page 22.
   
   For more information about jobs, see SAS Viya Administration: Jobs.

3. (Optional) Consider your business requirements and determine the frequency of the scheduled backups. Edit the backup schedule if necessary.
   
   For more information about editing the backup schedule, see “Edit a Backup Schedule” on page 22.

4. If SAS Viya is deployed on Linux, check the groups for users who are running SAS Viya services and CAS controllers.
   
   Backup and restore uses the sas user to back up and restore data sources from each machine that is included in the backup. It creates a local vault on each machine where data sources are available such as the SAS Configuration Server, SAS Infrastructure Data Server, SAS Message Broker, and CAS.
   
   If a CAS controller is running with a different user (a user who is not part of the sas group), perform the following steps to set appropriate permissions on the local vault for a successful backup and restore. Perform these steps for each user running a CAS controller.
   
   **Important:** In a multi-tenant deployment, an appropriate setfacl command must be submitted before a tenant administrator can perform a backup.
   
   1. Navigate to the SAS-configuration-directory.
2 Set appropriate access control on the local vault directory for the user running a CAS controller. For example, if a cas user is running a CAS controller, submit the following command:
setfacl -Rdm "u:cas:wx" backup/

3 Set appropriate access control on the local vault directory for the sas user so that the sas user can access directories created by the cas user. For example, submit the following command:
setfacl -Rdm "u:sas:rwx" backup/
The setfacl permissions need to be set only on machines where CAS controllers (primary and secondary CAS controller nodes) are available.

Note: Here are some important details to remember. During SAS Viya installation, the sas user is created with the sas group automatically. Access control lists (ACLs) should be enabled on the UNIX operating system. Whenever a new tenant is added or onboarded, set the setfacl permissions on the local vault directory on the machine where the CAS controller is available for that tenant.

5 Run the DEFAULT_BACKUP_SCHEDULE job and the BINARY_BACKUP_SCHEDULE to ensure that the backups are performed successfully.

To run the backup schedule, perform the following steps:

a In SAS Environment Manager, click Jobs.
b On the Scheduling tab of the Jobs page, perform the following tasks:
   - Right-click DEFAULT_BACKUP_SCHEDULE, and select Run to immediately run the backup.
   - Right-click BINARY_BACKUP_SCHEDULE, and select Run to immediately run the backup.
c On the Monitoring tab of the Jobs page, ensure that the jobs are running without any warnings and errors.

If you do not perform these tasks, the default backup runs every Sunday at 1:00 a.m. The binary backup runs on the first Saturday of every month at 5:00 a.m.

---

### Managing the Backup Configuration and Schedules

#### Manage the Backup Configuration

**About the Backup Configuration**
The Backup service has its own configuration. You must create the configuration initially and set the following properties:

- **retentionPeriod**—the number of days that backups are stored before they are deleted from the shared vault. Backups cannot be recovered after they are deleted.
- **sharedVault**—a shared network location for backups. For more information about a shared vault and its access rights, see "shared vault" on page 5.

**View a Backup Configuration**

1 In SAS Environment Manager, click Backup and Restore.
2 On the Backup and Restore page, click Backup Configuration.
Create and Edit a Backup Configuration

Create and Edit a Backup Configuration Using SAS Environment Manager

1. Log on to SAS Environment Manager as a provider administrator in a multi-tenant deployment. Or, log on as a SAS administrator in a standard deployment.

2. Click **Configuration** in the left pane.

3. Select **View ➔ Basic services**.

4. Click **Backup service**.

   The ✅ and ⚫ icons next to the service indicate whether information is entered for the backup configuration. The ✅ icon indicates that the backup configuration is created. You can view it and edit it if necessary. The ⚫ icon indicates that the backup configuration is not created. You must create it.

5. If the backup configuration is not created, scroll down until you see `sas.deploymentbackup`, and click ⚫ to the right of the service.

   If the backup configuration is already created and you want to edit it, scroll down until you see `sas.deploymentbackup`, and click ✅ to the right of the service.

6. Enter information for the `sharedVault` property and other configuration properties as necessary.

   For more information about a shared vault and its access rights, see "shared vault" on page 5.

   Consider the guidelines and best practices for configuring backups. For more information, see "Guidelines and Best Practices for Configuring Backups" on page 21. For more information about backups, see "Backup Service" in *SAS Viya Administration: Configuration Properties*.

7. Click **Save**.

Create a Backup Configuration Using the `sitedefault.yml` File

You can specify backup configuration information in the `sitedefault.yml` file before deploying SAS Viya. For more information about the `sitedefault.yml` file, see “Operations” in *SAS Viya Administration: Configuration Properties*.

1. Open the `sas_viya_playbook/roles/consul/files/sitedefault.yml` file. Copy the following code below the config property:

   ```yaml
   deploymentBackup:
     sas.deploymentbackup:
       sharedVault: /opt/sas/viya/config/SharedVault
       jobTimeout: 600
       retentionPeriod: 30
       custom:
         restore.filter.sas.configuration.config.sas.deploymentbackup: ***
       scheduledBackupAllowed: false
   
   Note: Copying code can lead to extraneous characters being included in your `sitedefault.yml` file. Review the `sitedefault.yml` file carefully.

2. In the preceding code, change the values of `sharedVault`, `jobTimeout`, and `retentionPeriod` if necessary.

   You must specify a value for the `sharedVault` property. For more information about a shared vault and its access rights, see "shared vault" on page 5.

3. Save the `sitedefault.yml` file, and then proceed with the deployment of SAS Viya.
Note: You cannot edit the backup configuration using the site\default.yml file.

Edit the Shared Vault Location Using SAS Environment Manager

1. Create a new directory for a new shared vault location.
   - For more information about a shared vault and its access rights, see “shared vault” on page 5. Consider the guidelines and best practices for configuring backups. See “Guidelines and Best Practices for Configuring Backups” on page 21 for more information. For more information about backups, see “Backup Service” in SAS Viya Administration: Configuration Properties for more information.

2. Determine whether you want to save all of the existing backups.
   - a. If you do, copy the contents from the old shared vault location to the new shared vault location created in step 1.
   - b. If you do not, you will not be able to see any of the existing backups in the new shared vault.

3. Log on to SAS Environment Manager as a provider administrator in a multi-tenant deployment. Or, log on as a SAS administrator in a standard deployment.

4. Click Configuration in the left pane.

5. For View, select Basic services.

6. Click Backup service.
   - The ◻ and ◻ icons next to the service indicate whether information is entered for the backup configuration. The ◻ icon indicates that the backup configuration is created. You can view it and edit it if necessary. The ◻ icon indicates that the backup configuration is not created. You must create it using the steps in “Create and Edit a Backup Configuration Using SAS Environment Manager” on page 20.

7. Scroll down until you see sas.deploymentbackup, and click ◻ to the right of the service.

8. Update the value of sharedVault. Set it to the path of the directory created in step 1.

9. Click Save.

10. In SAS Environment Manager, click ◻ Backup and Restore. Click ◻ to refresh the backup details.

11. If backups were saved in step 2, then the backup details will include them. Otherwise, there will be no backup details.


Guidelines and Best Practices for Configuring Backups

- Always ensure the values of the sharedVault property and retentionPeriod property are set immediately after a new installation, an upgrade, or any modifications to your SAS deployment.
  - For more information about a shared vault and its access rights, see "shared vault" on page 5.

- The shared vault location must be different from the local vault location. The local vault location is SAS-configuration-directory/backup on Linux and SAS-configuration-directory\backup on Windows. The local vault location is located on machines that have SAS Configuration Server, CAS (controller node), SAS Infrastructure Data Server, or SAS Message Broker.

- Set the retentionPeriod property so that you always have at least the last four backups available at any point in time. For example, if you are doing daily backups, the retention period must be four days. If you are doing weekly backups, the recommended retention period is 30 days.
Always initiate a binary backup after a tenant is onboarded or offboarded.

**Manage Backup Schedules**

**About Backup Schedules**

After SAS Viya is deployed, the following backup schedules are created automatically whenever the backup runs for the first time:

- default backup schedule
- binary backup schedule

**Default Backup Schedule**

After the default backup schedule is created, the following message appears in the Backup and Restore log located at `SAS-configuration-directory\var\log\deploymentBackup\default`:

```
Default schedule created for BackupService to run backup job every Sunday 1AM. You can also view the backup schedule in SAS Environment Manager.
```

**Binary Backup Schedule**

After the binary backup schedule is created, the following message appears in the Backup and Restore log:

```
Binary schedule created for BackupService to run backup job on the first Saturday of every month at 5AM. You can also view the backup schedule in SAS Environment Manager.
```

The following services must be running to run the backup schedules:

**Table 9  Names of Services on Linux and Windows**

<table>
<thead>
<tr>
<th>Name on Linux</th>
<th>Name on Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>sas-viya-identities-default</td>
<td>SAS Identities service</td>
</tr>
<tr>
<td>sas-viya-scheduler-default</td>
<td>SAS Scheduling service</td>
</tr>
<tr>
<td>sas-viya-jobdefinitions-default</td>
<td>SAS Job Definition service</td>
</tr>
<tr>
<td>sas-viya-jobexecution-default</td>
<td>SAS Job Execution service</td>
</tr>
<tr>
<td>sas-viya-restexecutionprovider-default</td>
<td>SAS REST Execution Provider service</td>
</tr>
</tbody>
</table>

If one of the services is not running when the Backup service starts, then the Backup service retries every 5 minutes 25 times to schedule the backup. If after 25 tries the backup is still not scheduled or one of the dependent services is still not running, then the following error message is displayed:

```
Cannot schedule backup since maximum retry attempt is reached and one of the dependent services is still not running. Ensure that all required services are running, and then restart the Backup service to schedule the backup.
```

**Edit a Backup Schedule**

1. In SAS Environment Manager, click **Jobs**.

   On the **Scheduling** tab, all scheduling jobs including the default backup schedule and binary backup schedule are listed.

2. Select a job, and click **.**
3 In the Edit Schedule dialog box, edit the required properties of the schedule.

4 (Optional) In the Edit Schedule dialog box, perform the following steps to add a trigger to the schedule:
   a Click ‣ to add a trigger to the schedule.
   b In the New Trigger dialog box, enter values.
      You must enter values for Name and Time fields.
   c Click Save.

5 Click Save again to close the Edit Schedule dialog box.

Create a Backup Job

A provider administrator can select tenants and schedule a job.

1 In the left pane of SAS Environment Manager, click Backup and Restore.

2 On the Backup and Restore page, click Create Backup Job.

3 In the Create Backup Job dialog box, enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the backup job.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the backup job.</td>
</tr>
<tr>
<td>Select tenants</td>
<td>Select the tenants to perform the default backup.</td>
</tr>
</tbody>
</table>

4 Click Create.

5 In SAS Environment Manager, click Jobs.

6 Click the Scheduling tab. From the list of scheduling jobs, select the newly created schedule, and click .

7 In the Edit Schedule dialog box, edit the required properties.

8 (Optional) In the Edit Schedule dialog box, perform the following steps to add a trigger to the schedule.
   a Click ‣ to add a trigger to the schedule.
   b In the New Trigger dialog box, enter values.
      You must enter values for Name and Time fields.
   c Click Save.

9 Click Save again to close the Edit Schedule dialog box.
Performing a Backup

Best Practices for Performing Backups

- Always use Backup and Restore to perform backups of the content and configuration of SAS Viya components. Backup and Restore automatically discovers the services that are deployed. It finds any new services so that they can be included in the backup. Backup and Restore also finds content and configuration data from the SAS Viya deployment. It backs up this data at the same point in time, which is required for a same point-in-time restore.

- Edit the backup configuration properties immediately after a new installation, an upgrade, or any modifications to your SAS Viya deployment. For more information, see “Create and Edit a Backup Configuration” on page 20.

- Perform a backup after any modifications to your SAS Viya deployment. Examples include but are not limited to deploying SAS Viya, installing software updates, changing the topology, modifying the SAS Viya configuration, and changing configuration properties.

- Backups are purged after the retention period. If you do not want any backups to be deleted after the retention period, you must manually archive the backups before they are purged.

- After an upgrade in place or a migration, perform an immediate backup. Do not wait for the scheduled backup to run. Use this immediate backup for a restore. Do not use previous backups of SAS Viya for a restore.

- Turn on notifications to see whether the backup failed. Use the Notifications service in SAS Environment Manager. For more information, see “Notifications Service” in SAS Viya Administration: Configuration Properties.

- If a tenant administrator performs a local backup, the tenant administrator should copy the contents (local files) of the local vault to a shared vault.

- It is a best practice to back up your shared vault.

Perform an Immediate Backup Using SAS Backup Manager

If necessary, you can perform an immediate backup.

**Important:** In a multi-tenant deployment, an appropriate setfacl command must be submitted before a tenant administrator can perform a backup. For more information, see Step 4 on page 18.

1. In the left pane of SAS Environment Manager, click **Backup and Restore**.

2. On the Backup and Restore page, click **Backup**.

3. In the Backup dialog box, provide information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Comments</strong></td>
<td>(Optional) Enter free-form comments describing the backup. Comments are recorded in the backup history and are displayed in the backup’s <strong>Operation Details</strong>.</td>
</tr>
<tr>
<td><strong>Backup type</strong></td>
<td></td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
**Binary** | Select this option if you want the pg_basebackup utility to back up all binaries in SAS Infrastructure Data Server. This includes metadata (such as user information, roles, and permissions).

A binary backup includes all onboarded tenants in a multi-tenant deployment by default.

**Include remaining sources** | Select this check box to back up remaining data sources (such as SAS Configuration Server, SAS Message Broker, and CAS).

*Note:* This check box is available when you select the **Binary** option.

**Default** | Select this option if you want the pg__dump utility back up the content of the SAS Infrastructure Data Server, SAS Configuration Server, SAS Message Broker, and CAS. A default backup does not include SAS Infrastructure Data Server metadata (such as user information, roles, and permissions). Use a default backup when SAS Infrastructure Data Server metadata is not significantly changed. A default backup can be fully restored using the Backup service. The restore includes SAS Infrastructure Data Server content, configuration data, and other data sources. A default backup includes all onboarded tenants in a multi-tenant deployment by default. However, SAS Backup Manager enables you to select tenants if you do not want all of them backed up.

**Tenants** | If the user is a provider administrator in a multi-tenant deployment, select the tenants to be backed up from the onboarded tenants. Select **Provider** to back up the provider tenant.

If the user is a tenant administrator in a multi-tenant deployment or a SAS administrator in a standard deployment, the tenant list is not displayed.

*Note:* Because a tenant administrator can perform only a default backup, the **Binary** backup type is not displayed.

4 Click **Backup** to start the backup.

A new row is added to the table with a running `✓` status. After the backup is completed, a message about the status of the backup is displayed. To see the status of the backup on the main page, refresh your browser.

5 *(Optional)* In the left pane of SAS Environment Manager, click **Logs** to view the log of a backup or restore.

---

**Perform an Immediate Backup Using a Command-Line Interface**

1 Using a command line, log on to SAS Viya.

For more information, see “Command-Line Interface: Preliminary Instructions” in *SAS Viya Administration: Using the Command-Line Interfaces*.

2 Use one of the following variations of the command **sas-admin backup start**:

- Use one of the following commands to perform a default backup with a comment:

  ```
  sas-admin backup start -c="sample comment"
  sas-admin backup start --backup-type=default -c="sample comment"
  ```

- Use the following command to perform a default backup of multiple tenants with a comment:

  ```
  sas-admin backup start --backup-type=default -c="sample comment" --tenants=<tenant1_ID>,<tenant2_ID>
  ```

- Use the following command to perform a binary backup with a comment:

  ```
  sas-admin backup start --backup-type=binary -c="sample comment"
  ```
Use the following command to perform a binary backup with all data sources:

```
sas-admin backup start --backup-type=binary --includeAllSourcesForBinaryBackup=true
```

## Performing a Restore

### Overview of Performing a Restore

Use one of the following scenarios for a restore or recovery:

- **Restore a default backup.**
  
  In this case, use SAS Backup Manager or a command-line interface (CLI) to restore the following data sources:
  - SAS Infrastructure Data Server
  - SAS Configuration Server
  - SAS Message Broker
  
  You must manually restore CAS. For more information, see “Restore SAS Cloud Analytic Services” on page 34.

- **Restore a binary backup where the include-all-sources property was set to FALSE.**
  
  In this case, you must manually restore SAS Infrastructure Data Server. For more information, see “Restore SAS Infrastructure Data Server from a Binary Backup Manually” on page 30. For more information about the include-all-sources property, see “pre-restore validations” on page 4.

- **Restore a binary backup where the include-all-sources property was set to TRUE.** For more information about the include-all-sources property, see “pre-restore validations” on page 4.
  
  In this case, you must first manually restore SAS Infrastructure Data Server. Then, use SAS Backup Manager or a CLI to restore the following data sources:
  - SAS Configuration Server
  - SAS Message Broker
  
  Then, manually restore CAS. For more information, see “Restore SAS Cloud Analytic Services” on page 34.

You cannot use SAS Backup Manager or a CLI to perform the following tasks:

- **Resolve a problem where the SAS Infrastructure Data Server cannot start by redeploying SAS Infrastructure Data Server, and then attempting to restore from a backup to that redeployment.**

- **Restore only a specific data source from a backup.**

- **Restore an unresponsive SAS Infrastructure Data Server.** For more information, see “Restore SAS Infrastructure Data Server from a Binary Backup Manually” on page 30.

- **Perform a restore if the SAS Infrastructure Data Server does not respond for reasons such as the following:**
  - If the SAS Infrastructure Data Server is configured for high availability and the primary node is unresponsive, you must first promote a standby node to the primary node before performing a restore.
    
    For more information, see “Restore SAS Infrastructure Data Server from a Binary Backup Manually” on page 30 or “SAS Infrastructure Data Server, High Availability, and Backup and Restore” on page 12.
  - If the SAS Infrastructure Data Server is not configured for high availability and it is unresponsive, restore it first and then restore from the latest binary backup.
Best Practices for Performing Restores

- While performing a restore, ensure that the system is not being actively used.
- Always use SAS Backup Manager or a CLI to perform restores to ensure a same point-in-time restore of content and configuration data.
- Always choose the most recent and successful backup to perform a restore.
- The backup-agent service (called SAS Backup Agent Service on Windows) must be running on all data sources that need to be restored.
- After performing a restore, stop and restart all services that are mentioned in "General Servers and Services: Operate (Linux)" in SAS Viya Administration: General Servers and Services.
  
  Note: Stopping and restarting services is applicable only for the restore of a standard deployment and for the restore of an entire multi-tenant deployment. It is not applicable for a tenant restore.

- Turn on notifications to see whether the restore failed. Use the Notifications service in SAS Environment Manager. For more information, see "Notifications Service" in SAS Viya Administration: Configuration Properties.

- Suppose that you upgraded in place or migrated to the latest version of SAS Viya, and you now want to restore a backup. In this case, you cannot use a backup from the previous version of SAS Viya for the restore.

Prerequisites for a Restore

- SAS Infrastructure Data Server must be running and responding to requests.

- In a standard deployment, the status of the backup that you want to restore must be or . If you are a provider administrator in a multi-tenant deployment, the status of the backup that you want to restore for the tenant must be or . If you are a tenant administrator in a multi-tenant deployment, the status of the backup that you want to restore must be or .

Restore Using SAS Backup Manager

1 Identify the backup that you want to restore.

2 Select one of the following options:

   - If the backup is a default backup, log on to SAS Environment Manager as a provider administrator or a tenant administrator in a multi-tenant deployment. Or, log on as a SAS administrator in a standard deployment.

   - If the backup is a binary backup where the include-all-sources property was set to FALSE, you must restore SAS Infrastructure Data Server manually. Do not perform the remaining steps. For more information about the include-all-sources property, see "pre-restore validations" on page 4.

   - If the backup is a binary backup where the include-all-sources property was set to TRUE, you must restore SAS Infrastructure Data Server manually first. Then, log on to SAS Environment Manager as a provider administrator in a multi-tenant deployment or as a SAS administrator in a standard deployment. For more information about the include-all-sources property, see "pre-restore validations" on page 4.

For more information, see “Restore SAS Infrastructure Data Server from a Binary Backup Manually” on page 30.
3 On the **Backup and Restore** page, select a backup, and click **Restore**.

4 In the Restore dialog box, provide information.

- **Comments**—(Optional) Free-form comments describing the restore. Comments are recorded in the restore history and are displayed in the restore’s **Operation Details**.
- **Force restore if some databases don’t match**—Select this check box if you want to force a restore if the databases do not match.
- **Tenants**—Select the tenants to be restored from the onboarded tenants in the backup whose backup status is ![Checkmark] or ![Checkmark]. Select **Provider** to restore the provider tenant.

  Note: The tenant list is displayed only for a provider administrator in a multi-tenant deployment.

5 Click **Restore**.

After the restore is completed, a message is displayed with its status as ![Checkmark], ![Checkmark], or ![Checkmark].

6 After a successful restore, stop and restart all services. Then, manually restore the CAS server.

For more information, see “Restore SAS Cloud Analytic Services” on page 34.

7 To restore scheduled jobs in a standard deployment on Windows and on Linux, the SAS administrator must perform the following tasks. To restore scheduled jobs for a tenant in a multi-tenant deployment on Linux, the provider administrator must perform the following tasks.

   a Pause the Schedule service.

   Use the following command on Windows to pause the Schedule service:
   ```bash
state?value=PAUSED
```

   Use the following command on Linux to pause the Schedule service:
   ```bash
state?value=PAUSED
```

   b Restore the schedules.

   Use the following command on Windows to restore the schedules:
   ```bash
restore
```

   Use the following command on Linux to restore the schedules:
   ```bash
```

   c Resume the Schedule service.

   Use the following command on Windows to resume the Schedule service:
   ```bash
state?value=RESUME
```

   Use the following command on Linux to resume the Schedule service:
   ```bash
state?value=RESUME
```

For more information about obtaining an access token, see “Obtain an Access Token Using Password Credentials” in **SAS Viya Administration: Authentication**.

Note: If the restore of the schedules fails, stop the Schedule service and delete the scheduler schema. Then, start the Schedule service, and perform a restore.

8 (Optional) In the left pane of SAS Environment Manager, click ![Logs] to view the logs.

Alternatively, the provider administrator or SAS administrator can view log paths.
For Linux:

*SAS-configuration-directory/var/log/deploymentBackup/default*

*SAS-configuration-directory/var/log/backup-agent/default*

For Windows:

*SAS-configuration-directory\var\log\deploymentBackup\default*

*SAS-configuration-directory\var\log\backupagent\default*

**Note:** If a failure occurs in any operation initiated by a tenant administrator, the tenant administrator must contact the provider administrator.

**Restore Using a Command-Line Interface**

1. Identify the backup that you want to restore.

2. Using a command line, log on to SAS Viya. For more information, see “Command-Line Interface: Preliminary Instructions” in *SAS Viya Administration: Using the Command-Line Interfaces*.

   **When you log on to SAS Viya at the command line, consider the following points:**

   - If the backup is a default backup, log on to SAS Environment Manager as a provider administrator or a tenant administrator in a multi-tenant deployment. Or, log on as a SAS administrator in a standard deployment.
   - If the backup is a binary backup where the include-all-sources property was set to FALSE, you must restore SAS Infrastructure Data Server manually. Do not perform the remaining steps. For more information about the include-all-sources property, see “pre-restore validations” on page 4.
   - If the backup is a binary backup where the include-all-sources property was set to TRUE, you must restore the SAS Infrastructure Data Server manually first. Then, log on to SAS Environment Manager as a provider administrator in a multi-tenant deployment or as a SAS administrator in a standard deployment. For more information about the include-all-sources property, see “pre-restore validations” on page 4.

   For more information, see “Restore SAS Infrastructure Data Server from a Binary Backup Manually” on page 30.

3. Use one of the following variations of the command `sas-admin restore start`:

   - Use the following command to restore a default backup or a binary backup where the include-all-sources property was set to TRUE. For more information about the include-all-sources property, see “pre-restore validations” on page 4.

     ```
     sas-admin restore start --backup-name=<backup_ID>
     ```

   - Use the following command to restore a backup even if the database validation fails:

     ```
     sas-admin restore start --backup-name=<backup_ID> force=true
     ```

   - Use the following command to restore a backup from an alternate shared vault location:

     ```
     sas-admin restore start --backup-name=<backup_ID> --alternate-shared-vault-for-restore=<path_of_alternate_sharedVault>
     ```

   - Use the following command to restore multiple tenants:

     ```
     sas-admin restore start --backup-name=<backup_ID> --tenants=<tenant1_ID>,<tenant2_ID>
     ```

   - Use the following command to restore multiple tenants from an alternate shared vault location:

     ```
     sas-admin restore start --backup-name=<backup_ID> --alternate-shared-vault-for-restore=<path_of_alternate_sharedVault> --tenants=<tenant1_ID>,<tenant2_ID>
     ```
When the restore is initiated by the provider administrator in a multi-tenant deployment, all onboarded tenants that are available in the backup are restored.

When the restore is initiated by a tenant administrator in a multi-tenant deployment, data for that tenant is restored.

When the restore is initiated by a SAS administrator in a standard deployment, the selected backup is restored.

4 After the restore of the backup is completed, restart all services. You must manually restore the CAS server. For more information, see “Restore SAS Cloud Analytic Services” on page 34.

5 To restore the scheduled jobs for a tenant, the provider administrator must perform the following tasks:

   a  Pause the Schedule service.

   Use the following command on Windows to pause the Schedule service: curl.exe -XPUT -H "Authorization: bearer <token>" <protocol>://<host>:<port>/scheduler/jobs/state?value=PAUSED

   Use the following command on Linux to pause the Schedule service: curl -XPUT -H "Authorization: bearer <token>" <protocol>://<host>:<port>/scheduler/jobs/state?value=PAUSED

   b  Restore the schedules.

   Use the following command on Windows to restore the schedules: curl.exe -XPUT -H "Authorization: bearer <token>" <protocol>://<host>:<port>/scheduler/jobs/restore

   Use the following command on Linux to restore the schedules: curl -XPUT -H "Authorization: bearer <token>" <protocol>://<host>:<port>/scheduler/jobs/restore

   c  Resume the Schedule service.

   Use the following command on Windows to resume the Schedule service: curl.exe -XPUT -H "Authorization: bearer <token>" <protocol>://<host>:<port>/scheduler/jobs/state?value=RESUME

   Use the following command on Linux to resume the Schedule service: curl -XPUT -H "Authorization: bearer <token>" <protocol>://<host>:<port>/scheduler/jobs/state?value=RESUME

For more information about obtaining an access token, see “Obtain an Access Token Using Password Credentials” in SAS Viya Administration: Authentication.

Note: If the restore of the schedules fails, stop the Schedule service and delete the scheduler schema. Then, start the Schedule service, and perform a restore.

**Restore SAS Infrastructure Data Server from a Binary Backup Manually**

**Restore SAS Infrastructure Data Server on Linux**

1 Stop all services including the SAS Infrastructure Data Server service using the following command on Linux:

   sudo /etc/init.d/sas-viya-all-services stop

2 Archive or rename the existing node0 directory using the following command on Linux:

   cd <sas-configuration-directory>/data/sasdatasvrc/<postgresql-instance-name>
Here is an example:

cd  /opt/sas/viya/config/data/sasdatasvrc/postgres
mv node0 node0_original

3 Create a new node0 directory with permissions and ownership similar to the old node0 directory. The new node0 directory and its extracted content should be owned by the old node0 directory owner. Submit the following command:

mkdir node0
chown sas:sas node0
chmod 700 node0
cd node0

4 Extract the contents of the base.tar.gz file into the node0 directory.

   - In a multi-tenant deployment, use the following command:

   tar -p -xvf ../sharedVault/<backup-Id>/provider/<postgresql-instance-name>/base.tar.gz

   Here is an example:

   tar -p -xvf ../sharedVault/<backup-Id>/provider/postgres/base.tar.gz

   - In a standard deployment, use the following command:

   tar -p -xvf ../sharedVault/<backup-Id>/__default__/<postgresql-instance-name>/base.tar.gz

   Here is an example:

   tar -p -xvf ../sharedVault/<backup-Id>/_default_/postgres/base.tar.gz

5 Ensure that the permissions of the files extracted in node0 are the same as they are in node0_original. If they are not the same, update the permissions using the following command:

sudo chown --from=<old-user>:<old-user-group> <new-user>:<new-user-group> node0 * -R

For example, if the files are owned by a PostgreSQL user from the PostgreSQL group after extraction, and the files in the node0_original directory are owned by a SAS user from the SAS group, then you can use the following command:

sudo chown --from=postgres:postgres sas:sas node0 * -R

6 Ensure that the Hot_Standby property is set to OFF in the SAS-configuration-directory/data/sasdatasvrc/postgres/node0/postgresql.conf file.

   Use the following command to set the Hot_Standby property to OFF:

   echo "hot_standby = off" >> postgresql.conf

7 Perform steps 2 through 6 for every SAS Infrastructure Data Server instance.

8 Start the Consul service (SAS Configuration Server).

   See “Infrastructure Servers: Overview” in SAS Viya Administration: Infrastructure Servers for instructions about how to start the Consul service.

9 Start the SAS Vault service (SAS Secrets Manager).

   See “Operate” in SAS Viya Administration: Infrastructure Servers for instructions about how to start the Vault service.

10 Start the SAS Infrastructure Data Server instance.

   On Red Hat Enterprise Linux 7.x (or an equivalent distribution) and SUSE Linux Enterprise Server 12.x:

   sudo systemctl start sas-viya-sasdatasvrc-<postgresql-instance-name>
For example:

```bash
sudo systemctl start sas-viya-sasdatasvrc-postgres
```

On Red Hat Enterprise Linux 6.x (or an equivalent distribution):

```bash
sudo service sas-viya-sasdatasvrc-<postgresql-instance-name> start
```

For example:

```bash
sudo service sas-viya-sasdatasvrc-postgres start
```

See “Operate a Cluster” in *SAS Viya Administration: Infrastructure Servers* for instructions about how to start the SAS Infrastructure Data Server instance.

11 Ensure that the SAS Infrastructure Data Server service started successfully without any issues and that it has a status of UP.

```bash
sudo /etc/init.d/sas-viya-sasdatasvrc-<postgresql-instance-name> status
```

For example:

```bash
sudo /etc/init.d/sas-viya-sasdatasvrc-postgres status
```

Checking status of sas-viya-sasdatasvrc-postgres...

```
PGPool is running with PID=4733
```

```
PGPool is running with PID=32413
Checking Postgresql nodes status...

<table>
<thead>
<tr>
<th>node_id</th>
<th>hostname</th>
<th>port</th>
<th>status</th>
<th>lb_weight</th>
<th>role</th>
<th>select_cnt</th>
<th>load_balance_node</th>
</tr>
</thead>
</table>
```

```
Checking Postgresql nodes status...

<table>
<thead>
<tr>
<th>node_id</th>
<th>hostname</th>
<th>port</th>
<th>status</th>
<th>lb_weight</th>
<th>role</th>
<th>select_cnt</th>
<th>load_balance_node</th>
</tr>
</thead>
</table>
| 0       | myhost.domain.com | 5432 | up     | 1.000000  | primary | 0          | true              | 0
```

12 Set the Hot_Standby property in the postgresql.conf file back to ON.

```bash
echo "hot_standby = on" >> postgresql.conf
```

13 Repeats steps 10 through 12 for every SAS Infrastructure Data Server instance.

14 Move the contents of your old shared vault location to the new shared vault location. Follow the first two steps in “Edit the Shared Vault Location Using SAS Environment Manager” on page 21.

15 Ensure that the old shared vault directory is empty.

16 Start all services.

```bash
sudo /etc/init.d/sas-viya-all-services-default start
```

17 Check whether the Backup service is running. Verify that no backup or restore details are visible in the SAS Backup Manager.

18 Using SAS Environment Manager, point the location of the old shared vault to the new shared vault that you created in step 14. Follow steps 3 through 12 in “Edit the Shared Vault Location Using SAS Environment Manager” on page 21.

Note: (Optional) If you want to reset the shared vault back to its original location, follow the steps in “Edit the Shared Vault Location Using SAS Environment Manager” on page 21. Skip step 1 because the original shared vault directory already exists and it includes all backups.
**Restore SAS Infrastructure Data Server on Windows**

1. In Microsoft Management Console, stop the SAS Services Manager service. Then, ensure that all other services are stopped.

2. Archive or rename the existing `<SAS-configuration-directory>\data\sasdatasvrc\postgresql-instance-name>\node0` directory.
   
   For example:
   ```
   <SAS-configuration-directory>\data\sasdatasvrc\postgres\node0
   
   You might want to rename the directory to `node0_original`.
   ```

3. Create a new `node0` directory.

4. Extract the contents of the base.tar file from the required backup ID of the shared vault location into the `node0` directory using any utility such as WinZip.

5. Change the ownership of the `node0` directory to the SAS Infrastructure Data Server user and provide all permissions.
   
   Perform the following steps to change the ownership:
   ```
   a. Right-click the `node0` directory, and then select Properties.
   
   
   c. In the Advanced Security Settings dialog box, change the owner to the SAS Infrastructure Data Server user, select Replace owner on subcontainers and objects, and click OK.
   
   d. In the Properties dialog box, click Edit.
   
   e. In the Permissions dialog box, select the SAS Infrastructure Data Server user, and provide Full control permissions to the SAS Infrastructure Data Server user.
   ```

6. Perform steps 2 through 5 for every SAS Infrastructure Data Server instance.

7. Start the Consul service (SAS Configuration Server). See "Infrastructure Servers: Overview" in SAS Viya Administration: Infrastructure Servers for instructions about how to start the Consul service.

8. Open the Windows PowerShell command prompt as an administrator, and then enter code to start the SAS Infrastructure Data Server.
   
   For example, for the default SAS Infrastructure Data Server:
   ```powershell
   cd "SASHome\libexec\sasdatasvrc\script"
   .\Invoke-StartStopPostgres.ps1 -action start -batchJob
   
   PS C:\Windows\system32> cd "C:\Program Files\SAS\Viya\libexec\sasdatasvrc\script"
   .\Invoke-HealthCheck.ps1 -batchJob
   ```

9. Verify that the SAS Infrastructure Data Server has started without any issues. Here is an example:
   ```
   Config Environment Variable file located: C:\ProgramData\SAS\Viya\etc\sasdatasvrc\postgres\node0\ConfigEnvironmentVariables.ps1
   myhost.domain.com:5432 - accepting connections
   ```

10. Repeat steps 8 through 9 for every SAS Infrastructure Data Server instance.
11 Move the contents of your old shared vault location to the new shared vault location. Follow the first two steps in “Edit the Shared Vault Location Using SAS Environment Manager” on page 21.

12 Ensure that the old shared vault directory is empty.

13 In Microsoft Management Console, start the SAS Services Manager service.

14 Log on to SAS Backup Manager using SAS Administrator credentials. Verify that no backup details or restore details are visible.

15 Using SAS Environment Manager, point the location of the old shared vault to the new shared vault that you created in step 12. Follow steps 3 through 12 in “Edit the Shared Vault Location Using SAS Environment Manager” on page 21.

Note: (Optional) If you want to reset the shared vault back to its original location, follow the steps in “Edit the Shared Vault Location Using SAS Environment Manager” on page 21. Skip step 1 because the original shared vault directory already exists and it includes all backups.

**Restore SAS Cloud Analytic Services**

1 Stop the server.

For more information, see “SAS Cloud Analytic Services: How To (Scripts)” in SAS Viya Administration: SAS Cloud Analytic Services.

2 Replace the content of `SAS-configuration-directory/etc/cas/default/permstore/<hostname>` on Linux and `SAS-configuration-directory\etc\cas\default\permstore\<hostname>` on Windows with the content of the `hostname` directory that is located in the shared vault.

The `permstore` directory is in the `<backupID>/<tenantID>/cas-shared-default` directory in the shared vault. `<tenantID>` in the path is the ID of the tenant in the multi-tenant deployment. In a standard deployment, use _Default_ instead of `<tenantID>`. The cas user needs Read, Write, and Execute access (on Linux) to the `permstore` directory.

If you specified a location in the PATH=" " option when creating a backup, then that content is what you should restore.

**Note:** When you are restoring CAS to an alternate host, the name of the host name directory in the source environment and in the target environment might be different.

3 Restart the server.

For more information, see “SAS Cloud Analytic Services: How To (Scripts)” in SAS Viya Administration: SAS Cloud Analytic Services.

---

**Performing a Restore to an Alternate Host**

**Overview of Performing a Restore to an Alternate Host**

The following terminology is used in this section:

**Source machine**

machine where the backups were performed. These backups need to be restored on another machine.
Target machine
alternate machine that has the same SAS Viya software installed on it as the source machine. The restore operation is executed on this alternate machine from the backup performed on the source machine.

Source shared vault
shared vault location for the source machine.

Target shared vault
network location where the content from the source shared vault was copied to.

Alternate shared vault
alternate shared vault location for the restore.

You cannot use a binary backup to perform a restore to an alternate machine. A provider administrator must perform the restore to an alternate machine in a multi-tenant deployment. A SAS administrator can perform the restore to an alternate machine in a standard deployment.

Note: The information in this section can be used as a part of any disaster recovery strategy at a customer site. The steps in this section restore the information that the Backup service backed up. The data sources outside of SAS Infrastructure Data Server are not backed up.

Prerequisites for Performing a Restore to an Alternate Machine

- On the source machine, do not set the source shared vault location to the path of the target shared vault. Instead, copy the content in the source shared vault to some other network location that is accessible to the target machine. This location is referred to as the target shared vault.
- The target shared vault location has the same access rights as the source shared vault location.
- The SAS Viya deployment (such as the version of SAS Viya and any hot fixes applied to it) in the source environment and in target environment must be the same.
- All the services are started on the target machine.

Perform a Restore to an Alternate Machine

Perform a Restore from a Target Shared Vault
To perform a restore from a target shared vault using CLI commands:

1. Copy the content of the source shared vault to the target shared vault.
2. Set the sharedVault property to the location of the target shared vault.

   For more information about setting the sharedVault location, see “Create and Edit a Backup Configuration” on page 20.

   After the shared vault is changed, if a backup or restore is requested or if the Backup service is restarted, the system evaluates whether to synchronize the local history with the SAS Infrastructure Data Server tables. The system checks to ensure that the last successful backup from the global history is available in the SAS Infrastructure Data Server tables. If it is not available, local history files are synchronized with the SAS Infrastructure Data Server tables.

3. Using the command line, log on to SAS Viya. For more information, see “Command-Line Interface: Preliminary Instructions” in SAS Viya Administration: Using the Command-Line Interfaces.

4. On the target machine, use the following command to view the backup list:

   sas-admin backup list
5 Select a backup to restore.

6 In a multi-tenant deployment, perform the following tasks:
   a. Restore the provider tenant using the following command:
      
      ```
      sas-admin restore start --backup-name=<backup_ID> --tenants=<provider>
      ```
   b. Restart all services.
   c. Restore the remaining tenants using the following command:
      
      ```
      sas-admin restore start --backup-name=<backup_ID> --tenants=<tenant1_ID>,<tenant2_ID>
      ```

   In a standard deployment, use the following command to restore the backup:
   
   ```
   sas-admin restore start --backup-name=<backup-id>
   ```

7 (Optional) Make a note of the `<jobID>` printed on the console.

8 (Optional) To view the details of a restore, submit the following command until you receive a status of completed or failed:
   
   ```
   sas-admin restore show -id-=<jobID>
   ```

   You might need to submit this command multiple times because when the restore is running and SAS Infrastructure Data Server is being restored, all of the services might not be able to respond. The command might not return the expected response and you might get a 403 Forbidden error.

9 (Optional) If a restore fails, review the logs. Make any necessary changes.
   If the status of the restore is $\infty$, review the backup-agent log. Make any necessary changes.
   The backup-agent log is located on Linux at `SAS-configuration-directory/var/log/backup-agent/default`.
   The backup-agent log is located on Windows at `SAS-configuration-directory\var\log\backupagent\default`.

10 After the restore is completed, restart all services.

11 Restore scheduled jobs.
   For more information, see Step 5 on page 30.

12 After all services are restarted, restore SAS Cloud Analytic Services.
   For more information, see "Restore SAS Cloud Analytic Services" on page 34.

13 Restore any required applications.

---

**Perform a Restore from an Alternate Shared Vault**

To perform a restore from an alternate shared vault using commands:

1 Using the command line on the target machine, log on to SAS Viya. For more information, see "Command-Line Interface: Preliminary Instructions" in *SAS Viya Administration: Using the Command-Line Interfaces*.

2 From the alternate shared vault, select a backup to restore.

3 In a multi-tenant deployment, perform the following tasks:
   a. Restore the provider tenant using the following command:
      
      ```
      sas-admin restore start --backup-name=<backup_ID>
      ```
b Restart all services.

c Restore the remaining tenants using the following command:

```
  sas-admin restore start --backup-name=<backup_ID>
  --alternate-shared-vault-for-restore=<path_of_alternate_sharedVault> --tenants=<tenant1_ID>,<tenant2_ID>
```

In a standard deployment, use the following command to restore the backup:

```
  sas-admin restore start --backup-name=<backup_ID>
  --alternate-shared-vault-for-restore=<path_of_alternate_sharedVault>
```

4 (Optional) Make a note of the `<jobID>` printed on the console.

5 (Optional) To view the details of a restore, submit the following command until you receive a status of completed or failed:

```
  sas-admin restore show -id-=<jobID>
```

   You might need to submit this command multiple times because when the restore is running and SAS Infrastructure Data Server is being restored, all of the services might not be able to respond. The command might not return the expected response and it might give a 403 error.

6 (Optional) If a restore fails, review the logs. Make any necessary changes.

   If the status of the restore is , review the backup-agent log. Make any necessary changes.

   The backup-agent log is located on Linux at `SAS-configuration-directory/var/log/backup-agent/default`.

   The backup-agent log is located on Windows at `SAS-configuration-directory\var\log\backupagent\default`.

7 After the restore is completed, restart all services.

8 Restore scheduled jobs.

   For more information, see Step 5 on page 30.

9 After all services are restarted, restore SAS Cloud Analytic Services from the backup that was selected on the alternate shared vault.

   For more information, see “Restore SAS Cloud Analytic Services” on page 34.

10 Restore any required applications.

---

**Backing Up and Restoring Programming-Only Deployments**

**Back Up CAS Access Controls and Caslib Information**

**Important:** After global-scope caslibs and access controls are modified, you must back up each CAS server’s stored access control and caslib information.

SAS administrators can perform a backup programmatically using the `createBackup` and `completeBackup` actions as follows:

1 Run the following code in SAS Studio, replacing the PATH location with your location:
cas casauto host="cloud.example.com" port=5570;

proc cas;
accessControl.assumeRole /
   adminRole="SuperUser";
accessControl.createBackup /
   path="/my/backup/location";
accessControl.completeBackup;
accessControl.dropRole / adminRole="SuperUser";
quit;

2 Copy the backup location directory to a location where it can be saved. The cas user needs Write access to the location. If the location does not exist and the cas user has Write and Execute permission (on Linux), the location is created.

If you do not specify path=" ", the backup location is the directory named backup. This directory is in the PERMSTORE option location. It is under the directory with the fully qualified DNS name of the machine that runs the main controller. The cas user must have Read, Write, and Execute permission (on Linux) to both the permstore and backup directories.

Understand the Backup Configuration

The configuration information about Linux is stored in the following files for the hosts in the [sas-casserver-primary] host group in the inventory file:

SAS-configuration-directory/etc/cas/default/casconfig.lua
SAS-configuration-directory/etc/cas/default/cas.hosts

The configuration information about Windows is stored in the following file for the hosts in the [sas-casserver-primary] host group in the inventory file:

SAS-configuration-directory/etc/cas/default/casconfig.lua

The configuration information is stored in the following files for the hosts in the [programming] host group in the inventory file:

SAS-configuration-directory/etc/sasstudio/default/init_usermods.properties
SAS-configuration-directory/etc/sasstudio/default/appserver_usermods.sh
SAS-configuration-directory/etc/spawner/default/spawner_usermods.sh
SAS-configuration-directory/etc/workspaceserver/default/autoexec_usermods.sas
SAS-configuration-directory/etc/workspaceserver/default/sasv9_usermods.cfg
SAS-configuration-directory/etc/workspaceserver/default/workspaceserver_usermods.sh

If your site created global folder shortcuts for SAS Studio, you must back up the directory that contains the shortcuts. By default, the shortcuts are stored in the following directory:

SASHome/SASFoundation/GlobalStudioSettings

Note: Your site might have configured a different directory for the shortcuts. For more information, see “Configuring Global Folder Shortcuts” in SAS Viya Administration: Configuration Properties.

Restore Programming-Only Deployment

1 Stop the CAS server.

2 Identify the location of the permstore. Copy all content to a safe location, and then remove it from the permstore.

The default location of the permstore is `SAS-configuration-directory/etc/cas/default/permstore/<fully-qualified-domain-name>`.

3 Copy the content of the backup directory to the permstore directory.

Ensure that the cas account has Read and Write access to all the permstore files.

4 Start the server.

For more information about stopping and starting CAS, see "SAS Cloud Analytic Services: How To (Scripts)" in *SAS Viya Administration: SAS Cloud Analytic Services*.

**Restore the Most Recent Permstore on Linux in the Event of a Failover**

If the backup controller has taken over for the primary controller, perform the following steps to restore the most recent permstore from the backup controller:

1 Stop the CAS server.


2 Identify the location of the primary controller’s permstore. Copy all content to a safe location, and then remove it from the primary controller’s permstore.

   The default location of the primary controller’s permstore is `SAS-configuration-directory/etc/cas/default/permstore/<fully-qualified-domain-name>`.

3 Copy the content of the backup controller’s permstore to the primary controller’s permstore.

   The default location of the backup controller’s permstore is `SAS-configuration-directory/etc/cas/default/permstore/<fully-qualified-domain-name>`.

   Ensure that the cas account has Read and Write access to all the permstore files.

4 Copy the content of the backup controller’s permstore to a safe location.

5 Start the CAS server.

For more information about stopping and starting CAS, see “SAS Cloud Analytic Services: How To (Scripts)” in *SAS Viya Administration: SAS Cloud Analytic Services*.

**Troubleshooting**

**Backup and Restore: Logs**

Backup and Restore generates the following logs that can be used in troubleshooting:

- On the host where Backup and Restore is deployed, service logs are created in the following paths. The name of the log files is based on the time at which the backup was started.

  On Linux: `SAS-configuration-directory/var/log/deploymentBackup/default`

  On Windows: `SAS-configuration-directory\var\log\deploymentBackup\default`
On each of the data sources, backup logs are created in the following paths. The name of the log files is based on the time at which the backup-agent service was started.

On Linux: \texttt{SAS-configuration-directory/var/log/backup-agent/default}

On Windows: \texttt{SAS-configuration-directory/var\log\backupagent\default}

If a restore of the SAS Infrastructure Data Server fails, the log files for the restore are dumped to the following directory:

\texttt{<sharedVault>/<backup_ID>/<tenant_ID>/postgres/restore/<restore_ID>...<restore.log>}

This directory is on the host where the data source resides. This is the location of the local vault.

**Backup and Restore: Error and Warning Messages**

This service is not available which is required for scheduling default backup: "Access token denied." Cannot schedule backup since the maximum retry attempt is reached and one of the dependent services is still not running.

If a service that is starting fails to register itself with SASLogon, the service tries multiple times to register the client until the client registration is done. In this case, the default backup is not created because it cannot generate client tokens to access other services, such as Schedule or Job Execution.

If the DEFAULT_BACKUP_SCHEDULE does not exist, you must restart the sas-deploymentBackup service and check again.

This service is not available which is required for scheduling default backup: \%name-of-service\%. Cannot schedule backup since the maximum retry attempt is reached and one of the dependent services is still not running.

Although the Backup service is starting, other services have not yet started. Ensure that all required services are started. In this scenario, the sas-deploymentBackup service retries 25 times with an interval of 5 minutes to schedule the backups. If one or more of the services is not running after 25 retries, you get the error message.

If the DEFAULT_BACKUP_SCHEDULE does not exist, you must restart the sas-deploymentBackup service and check again.

Note: \%name-of-service\% is the name of the service that did not start.

**A Backup or Restore Is Already in Progress**

This message indicates that a backup or restore is in progress. You cannot initiate multiple backups and restores at the same time.

1. In SAS Viya, restart the SAS Backup and Restore service. For more information, see “Start and Stop a Specific Server or Service” in SAS Viya Administration: General Servers and Services. Alternatively, in Microsoft Management Console on Windows, stop and then start the SAS Backup and Restore.

2. Ensure that the previous backup failed.

3. Perform a backup.

   For more information, see “Performing a Backup” on page 24.

Here is how to stop a restore that is in progress:

1. On the command line in Linux, enter `sudo /etc/init.d/sas-viya-deploymentBackup-default restart`. 

In SAS Viya, restart the SAS Backup and Restore service. For more information, see “Start and Stop a Specific Server or Service” in SAS Viya Administration: General Servers and Services.
On Windows, use the Microsoft Management Console Services snap-in on Windows to stop the SAS Backup Service.

2. Ensure that the restore has a state.

3. Restart the SAS Backup Service.

4. Perform a restore.
   
   For more information, see “Performing a Restore” on page 26.

Database Lists in the Backup and SAS Infrastructure Data Server Database Do Not Match

The database list in the backup `<source list in backup>` and the database list in SAS Infrastructure Data Server `<source list in database>` do not match. Set the FORCE option in a restore request to TRUE to force the restore.

This indicates that the databases in SAS Infrastructure Data Server at the time of the backup and the databases in SAS Infrastructure Data Server do not match. The Backup and Restore service does not restore a database that is missing.

If you still want to restore the remaining databases, enter the following command: `sas-admin restore start --backup-name=<backup_ID> force=true`

Configuration with the ID {0} Was Not Found

This indicates that the configurationId provided in the backup request is not available or supported.

TIP Currently only the DEFAULT value is supported for configurationId. Modify the backup request to set the configurationId to default and try again.

Error Code 403 While Retrieving Information Related to Restore Operation

While a SAS Infrastructure Data Server restore is running, it might take some time for all services to respond. In this case, the user might see a 403 Forbidden error message.

Request Contains Invalid Values for the Start or Limit Parameters

The request contains invalid values for the start ({0}) or limit ({1}) parameter. Use positive integers as values for the start and limit parameters and resubmit the request.

Specified Backup Does Not Have a Directory in the Shared Vault or in the History File

The specified backup is not found in the shared vault or history file. This might occur because the database mode of the environment from which the backup was performed is different from the target environment. Ensure that you are using compatible environments and start another backup to initiate the restore.

Invalid Shared Vault Location

The shared vault location is invalid. The location of the shared vault and local vault must be different. Set a valid shared vault location in SAS Environment Manager. For more information, see “Create and Edit a Backup Configuration” on page 20.
List Can Only Contain Onboarded Tenants
The list of tenants should contain only tenants with a state of onboarded. Remove tenants that are not onboarded or are not valid.

backupType Value of Binary Contains a List of Tenants
A list of tenants should not be provided for the backupType value of binary. A binary backup cannot back up a subset of tenants. Remove the list of tenants or perform a default backup. In addition, a binary backup can be performed only by a provider administrator in a multi-tenant deployment.

Multi-Tenant Deployment Can Be Triggered Only by a Provider Administrator
In a multi-tenant deployment, a backup can be performed only by a provider administrator.

Shared Vault Is Not Accessible
The shared vault is not accessible. Make the shared vault accessible and restart the job. For more information about a shared vault and its access rights, see "shared vault" on page 5.

Specified Backup ID Is Incompatible with the Target System
The specified backup ID is incompatible with the target environment. The database mode of the target environment should be the same as the source environment. Use a different backup ID to restore to the target environment.

Backups or Restores Are in Pending State Even After Restarting All Services
Even after starting all services, you might see backups or restores in the pending state. This occurs because the Backup service was started before the Tenant service. Ensure that the Tenant service is running and then restart the Backup service.

After Performing UIP, the Default Backup Schedule Is Not Working
After performing an upgrade in place to SAS Viya 3.4, the default backup schedule might not work. Delete the default backup schedule and restart the Backup service. For more information about deleting the backup schedule, see "Jobs: How To" in SAS Viya Administration: Jobs.

Access Denied to Vault
A tenant administrator’s attempt to perform a backup fails.

java.nio.file.AccessDeniedException: /opt/sas/viya/config/backup/2019-06-06T05_53_52_635-0400/__default__/cas-shared-default

In a multi-tenant deployment, an appropriate setfacl command must be submitted before a tenant administrator can perform a backup.

Backup Failed or Is Taking Too Much Time
If the backup failed because it timed out or if the backup is taking longer to complete than previously, check the backup details to see which data sources are taking the most time. If any solution-specific SAS Infrastructure Data Server is taking more time than expected, see the solution documentation for more information about how to handle this issue.
Scheduled Backups Are Failing or If You Are Unable to Initiate an Ad Hoc Backup or Restore

Check whether all services, specifically SAS Infrastructure Data Server, SAS Message Broker, SAS Configuration Server, SAS Cloud Analytic Services, and any additional SAS Infrastructure Data Servers are running. Check whether each node on which any of the above services is running also has backup agent installed and running.