



SAS® Viya® 3.5 Administration: Backup and Restore

Backup and Restore: Overview	2
Introduction to Backup and Restore	2
What Is Backed Up?	3
What Is Not Backed Up?	3
Backup and Restore: Concepts	4
Default File Locations	4
Backup and Restore Terms	5
Roles and Permitted Tasks	8
About Default Backup and Binary Backup	10
Tenancy and Backup and Restore	12
The Backup Directory Structure	12
Purge Backups	13
SAS Infrastructure Data Server, High Availability, and Backup and Restore	14
Backup and Restore: User Interface of SAS Backup Manager	14
View SAS Backup Manager	14
Understand SAS Backup Manager	14
View History of Backup and Restore	15
View Details of a Backup or Restore as a SAS Administrator or Tenant Administrator	16
View Details of a Backup or Restore for a Tenant as a Provider Administrator	17
Backup and Restore: How To (CLI)	18
CLI Examples: Backup	18
CLI Examples: Restore	19
Backup and Restore: Initial Tasks	19
Backup and Restore: Manage the Backup Configuration and Schedule	21
Manage the Backup Configuration	21
Manage Backup Schedules	23
Backup and Restore: Perform a Backup	25
Best Practices for Performing Backups	25

Perform an Immediate Backup Using SAS Backup Manager	26
Perform an Immediate Backup Using a Command-Line Interface	28
Backup and Restore: Cancel a Backup	28
Cancel in the User Interface	28
Cancel in the CLI	29
Backup and Restore: Perform a Restore	29
Overview of Performing a Restore	29
Best Practices for Performing Restores	31
Prerequisites for a Restore	32
Restore Using SAS Backup Manager	33
Restore Using a Command-Line Interface	35
Restore SAS Infrastructure Data Server from a Binary Backup Manually	37
Restore SAS Cloud Analytic Services	41
Backup and Restore: Perform a Restore to an Alternate Deployment	42
Overview of Performing a Restore to an Alternate Deployment	42
Terms	42
Prerequisites for Performing a Restore to an Alternate Deployment	43
Configuring a Shared Vault for Restore to an Alternate Deployment	44
Perform a Restore to an Alternate Deployment	44
Backup and Restore: Programming-Only Deployments	52
Back Up CAS Access Controls and Caslib Information	52
Understand the Backup Configuration	53
Restore Programming-Only Deployment	53
Restore the Most Recent Permstore on Linux in the Event of a Failover	54
Backup and Restore: Troubleshooting	54
Backup and Restore: Logs	54
Backup and Restore: Error and Warning Messages	55

Backup and Restore: Overview

Introduction to Backup and Restore

The SAS Viya platform 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 the SAS Viya platform 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, host names, 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 platform deployment

In the SAS Viya platform deployment, the deployment files that are included as part of the SAS Viya platform 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 platform solutions
- Data sources, such as:
 - Files for predefined caslibs in CASDATADIR
 - 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.

- For SAS Visual Investigator, external data store configuration information and OpenSearch indices

For more information about backing up these items, see [“Backing Up and Restoring” in SAS Visual Investigator: Administrator’s Guide](#).

Backup and Restore: Concepts

Default File Locations

After the SAS Viya platform 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 1 Default Locations

Location	Example Path on Windows System	Example Path on Linux System
<i>SAS-configuration-directory</i>	C:\ProgramData\SAS\Viya	/opt/sas/viya/config
<i>SASHome</i>	C:\Program Files\SAS\Viya	/opt/sas/viya/home

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:

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 deployment. The permissions for an alternate shared vault are the same as the shared vault. For more information, see [“shared vault”](#).

backup

the backup that can be initiated by a SAS administrator. The SAS Viya platform can be deployed on Linux and on Windows. There are two types of backup: default and binary. For more information, see [Table 2](#).

jobMaximumThreadpoolSize

the maximum number of parallel tasks that can be executed in the backup or restore operation. The default value for jobMaximumThreadpoolSize is 20. If the maximum number of tasks are already running, and a new task execution is requested, the request is added to the jobQueueCapacity.

jobQueueCapacity

the maximum number of tasks that can be added to the queue for backup and restore operation execution. The default value for jobQueueCapacity is 200.

Note: jobQueueCapacity is linked with jobMaximumThreadpoolSize. If the maximum number of tasks are already in the queue, the new task execution request is lost.

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”](#).

- 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.

restore

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

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.

Make sure to set up a shared vault as an initial task. For more information, see [“Backup and Restore: Initial Tasks”](#).

The shared vault directory must be accessible from every host in the deployment that has a data source configured. For example, hosts that have the following items need access:

- the primary CAS controller
- the secondary or backup CAS controller
- RabbitMQ
- Pgpool
- Consul
- Backup service

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.

slug

user-provided name for the backup or restore operation.

standard deployment

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

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.
- *canceled* 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:

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”](#).

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.

multi-tenant deployment

a SAS Viya platform 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 platform deployment.

In a multi-tenant deployment, a tenant is said to be onboarded when the SAS Viya platform 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.

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.

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 2 Roles and Permitted Tasks

Task	Standard Deployment on Windows and in Linux	Multi-tenant Deployment	
	SAS Administrator	Provider Administrator	Tenant Administrator
View backup configuration	✓	✓	✓
Edit backup configuration	✓	✓	–
View and edit a default backup schedule	✓	✓	–
View and edit a binary backup schedule	✓	✓	–
Perform an immediate default backup	✓	✓	✓
Perform an immediate binary backup	✓	✓	–
Create backup job and schedule it	–	✓	–
Perform a restore	✓	✓	✓
Perform a restore to an alternate deployment	✓	✓	–

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](#).

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](#).

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

Category	Default Backup	Binary Backup
General information	The default type of backup.	A different type of backup that is not a replacement of the existing default backup.
	Uses the pg_dump utility.	Uses the pg_basebackup utility.
Backup-related information	Backs up the following source types: ■ content of SAS Infrastructure Data Server ■ SAS Configuration Server ■ SAS Message Broker ■ CAS The default backup does not back up the metadata of the SAS Infrastructure Data Server.	Backs up the content and metadata of the SAS Infrastructure Data Server (such as database users, roles, and permissions). 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”.
	A logical backup of each database in the SAS Infrastructure Data Server. 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.	A binary copy of the database files as a TAR archive.

Category	Default Backup	Binary Backup
	In a multi-tenant deployment, you can select the tenants from a list of tenants to perform the default backup.	In a multi-tenant deployment, you can perform a binary backup of the entire deployment that includes all tenants.
Restore-related information	Use default backup to perform a logical backup of each database in the SAS Infrastructure Data Server.	Use binary backup to perform a binary copy of the database files in a SAS Infrastructure Data Server or in any additional required SAS Infrastructure Data Server instances. The binary copy is a TAR archive.
	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.	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”. Note: While restoring a binary backup, the SAS Infrastructure Data Server must be manually restored before all other source types. Otherwise, restoring the other source types might fail due to an unresponsive SAS Infrastructure Data Server.
	Use default backup for restoring to an alternate deployment or to the same deployment. You can use SAS Backup Manager or a command-line interface (CLI) to restore a default backup.	Use binary backup to perform a restore on the same deployment. You cannot use binary backup to restore to an alternate deployment.
	Do not use default backup if the SAS Infrastructure Data Server is unresponsive.	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.
	When you use default backup to restore in a multi-tenant deployment, only the tenants that were included in the default backup are restored.	When you use binary backup to restore in a multi-tenant deployment, the entire deployment (that includes all tenants) is restored.

Tenancy and Backup and Restore

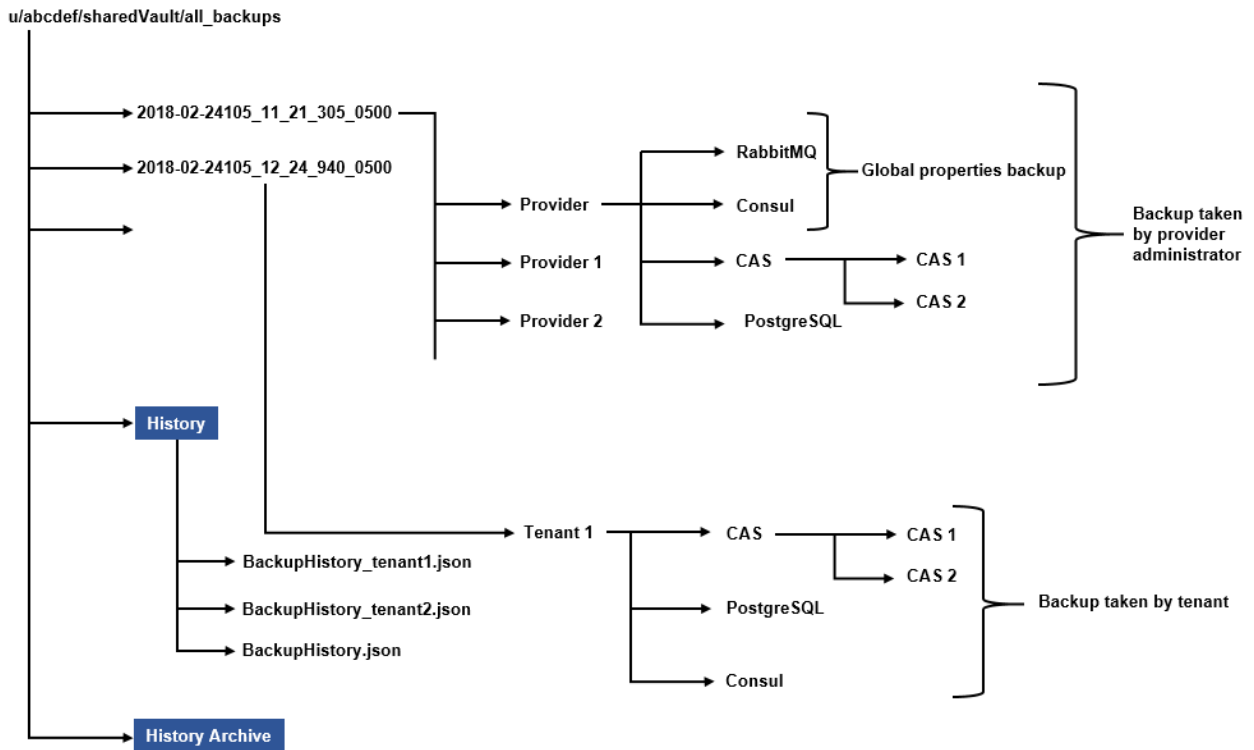
The following table shows the tenancy and deployment type for Linux and Windows.

Operating System	Tenancy	Deployment Type	Administrator
Linux	SAS Viya can be deployed for a single tenant and for multiple tenants.	Standard deployment for single tenant.	Members of the SAS Administrators group and individual users can perform backup and restore operations.
		Multi-tenant deployment for multiple tenants.	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.
Windows	SAS Viya can be deployed for a single tenant only.	Standard deployment for single tenant.	Members of the SAS Administrators group and individual users can perform backup and restore operations.

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.



In the diagram, the path `/u/abcdef/sharedVault/all_backups` is the path of the shared vault. This directory contains the folders for backups. Folders are named using the date and time at which the backup was performed. Each backup folder contains folders for the tenants included in the backup. In a standard deployment, only one folder named `__default__` exists. In a multi-tenant deployment, a `tenantID` folder is available. Within each tenant folder, there are folders for each source type to which the tenant has access. Within each source type folder, you can find the backup files for that source type.

Within the shared vault, there are folders named `History` and `HistoryArchive`. The `History` folder stores the history files. This includes the global history file (`backuphistory.json`) and tenant history files (`backup history_tenantId.json`). The `HistoryArchive` folder contains the backup of the `History` folder after each successful backup or restore operation.

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”](#).

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.

Backup and Restore: 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.
- Cancel a backup.
- 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.
- Cancel a backup.
- Perform a restore.

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 4 Description of Columns in Backup and Restore Details

Column Name	Description
Comments	Comments that were entered before performing a backup or restore.
Backup ID or Restore ID	Unique identifier of the backup or restore based on the date and time that it was started (for example, 2017-10-28T05_33_47_326-0400).
User ID	User ID of the user that ran the backup or restore or the identity name of the service that initiated the backup or restore.

Column Name	Description
Type	Type of backup: binary or default.
Size	Total size of the files that were backed up. (This value is not available for a provider in a multi-tenant environment.) This column is not displayed when you select Restore details .
Local Start Time	Date and time that the backup or restore started running.
Local End Time	Date and time that the backup or restore stopped running.
Status	Status of the backup or restore operation. One of the following icons is displayed:  The backup or restore is pending; it has not started.  The backup or restore is running.  The backup or restore completed without errors or warnings.  The backup or restore completed with warnings.  The backup or restore completed with errors. Click  to understand the reason for the failure.  The backup is purged.  The status of the backup or restore cannot be determined.  The backup is canceled.

View Details of a Backup or Restore as a SAS Administrator or 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 and the names of any additional SAS Infrastructure Data Server instances
- 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.
 - 5 (Optional) To collapse the data source, click .

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.

Backup and Restore: How To (CLI)

The following examples assume that you have already signed in to the SAS Viya platform at the command line. See [“Command-Line Interface: Preliminary Instructions” in SAS Viya Administration: Using the Command-Line Interfaces](#).

CLI Examples: Backup

The following examples are for the backup plug-in to the sas-admin CLI.

Example: List the first 50 backups.

```
sas-admin backup list --limit 50
```

Example: Show details of a backup with backup ID 2017-10-28T07_23_44_594-0400

```
sas-admin backup show -i=2017-10-28T07_23_44_594-0400
```

Example: Obtain help for LIST command for backup

```
sas-admin backup list -help
```

Example: Perform the backup

```
sas-admin backup start
```

Example: Cancel the backup

```
sas-admin backup cancel -i=2017-10-28T07_23_44_594-0400
```

CLI Examples: Restore

The following examples are for the restore plug-in to the sas-admin CLI.

Example: Show the history of restores

```
sas-admin restore list
```

Example: Show details of a restore with restore ID 2017-10-28T07_23_44_594-0400

```
sas-admin restore show -i=2017-10-28T07_23_44_594-0400
```

Example: Obtain help for LIST command for restore

```
sas-admin restore list -help
```

Example: Start a restore of a specified backup, and specify that the name of the restore is restoreA

```
sas-admin restore start --backup-name backup-ID --slug restoreA
```

Backup and Restore: Initial Tasks

Immediately after the SAS Viya platform 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”](#).
- 2 In SAS Environment Manager, click  **Jobs**¹, 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 the SAS Viya platform 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”](#).
For more information about jobs, see [SAS Viya Administration: Jobs and Flows](#).
- 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”](#).
- 4 If the SAS Viya platform is deployed on Linux, check the groups for users who are running SAS Viya platform services and CAS controllers.
 1. **Jobs and Flows** if the SAS Job Flow Scheduler is licensed.

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.

- 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:rw" 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 the SAS Viya platform 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 and Flows**.
- b On the **Scheduling** tab of the Jobs and Flows page, perform the following tasks:
 - Right-click `DEFAULT_BACKUP_SCHEDULE`, and select **Execute** to immediately run the backup.
 - Right-click `BINARY_BACKUP_SCHEDULE`, and select **Execute** to immediately run the backup.
- c On the **Monitoring** tab of the Jobs and Flows 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.

Backup and Restore: Manage the Backup Configuration and Schedule

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”](#). Make sure to set up a shared vault. For more information, see [“Backup and Restore: Initial Tasks”](#).

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 in the properties. 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”](#).

Consider the guidelines and best practices for configuring backups. For more information, see [“Guidelines and Best Practices for Configuring Backups”](#).

- 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 the SAS Viya platform. For more information about the sitedefault.yml file, see [“Configuration Properties: Overview” in SAS Viya Platform: Configuration Properties](#).

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

```
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”](#).

- 3 Save the sitedefault.yml file, and then proceed with the deployment of the SAS Viya platform.

Note: You cannot edit the backup configuration using the sitedefault.yml file.

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”](#).

- 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 the SAS Viya platform 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 5 Names of Services on Linux and Windows

Name on Linux	Name on Windows
sas-viya-identities-default	Identities service
sas-viya-scheduler-default	Schedule service
sas-viya-jobexecution-default	Job Execution service

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 and Flows**.
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 window, edit the required properties of the schedule.
- 4 (Optional) In the Edit Schedule window, 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 window, enter values.
You must enter values for **Name** and **Time** fields.
 - c Click **Save**.
- 5 Click **Save** again to close the Edit Schedule window.

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 window, enter the following information:

Table 6 Fields in the Create Backup Job Window

Field	Description
Name	Enter a name for the backup job.
Description	Enter a description for the backup job.
Select tenants	Select the tenants to perform the default backup.

- 4 Click **Create**.
- 5 In SAS Environment Manager, click  **Jobs and Flows**.

- 6 Click the **Scheduling** tab. From the list of scheduling jobs, select the newly created schedule, and click .
- 7 In the Edit Schedule window, edit the required properties.
- 8 (Optional) In the Edit Schedule window, 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 window, enter values.
You must enter values for **Name** and **Time** fields.
 - c Click **Save**.
- 9 Click **Save** again to close the Edit Schedule window.

Backup and Restore: Perform a Backup

Best Practices for Performing Backups

- Use the inventory plug-in to the sas-admin CLI to scan your SAS Viya content and create a report. Use the report to identify what you want to back up. The **CAS Inventory** and **Filesystem Inventory** tabs are particularly helpful.
 - NFS-mounted data locations need to be carefully considered. They might be backed up by another process. They might need to be manually backed up. Make sure you assess each NFS-mounted data location. Here are some specific examples:
 - ☐ Corporate data paths.
 - ☐ Personal casuser paths based on the CASHostAccountRequired custom group. See [“The CASHostAccountRequired Custom Group” in SAS Viya Administration: Identity Management](#) for more information.
 - ☐ Directories that support MAS publishing.
-
- Note:** For a clustered environment, MAS publishing destinations should be mounted to a shared NFS location.
-
- Manually back up any Model Studio project directories, which are located under **projects** in CASDATADIR.
 - Manually back up casuserlibraries (unless they are NFS mounted).
 - Manually back up the Models caslib, the Modelstore caslib, and the Vamodels caslib. These caslibs might be NFS mounted as a result of a CAS Failover requirement; you should still manually back them up.

- Manually back up usermod files. Manually back up etc paths for SAS and CAS.
- 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”](#).
- 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 Platform: 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.
- Back up your shared vault.
- If SAS Infrastructure Data Server has been upgraded, you need to clear the existing shared vault or change the shared vault to a new location. This prevents issues from a mismatch of server version. See [“Create and Edit a Backup Configuration”](#) for more information about changing the shared vault location.
- If you are running the backup-agent 2.31.0 and using the October 2024 (24w44) release of SAS Viya 3.5 you might encounter issues on restore. If you are using the October 2024 version, then follow the steps in [“Problems Restoring PostgreSQL Database” on page 61](#) to create a reliable backup.

This problem was corrected in the December 2024 (24w51) release.

Perform an Immediate Backup Using SAS Backup Manager

If necessary, you can perform an immediate backup.

- 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 window, provide information.

Table 7 *Fields in the Backup Window*

Field	Description
Comments	(Optional) Enter free-form comments describing the backup. Comments are recorded in the backup history and are displayed in the backup's Operation Details .
Backup type	
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
```

Backup and Restore: Cancel a Backup

Cancel in the User Interface

The **Cancel** button is new for the November 2019 release.

- 1 Log on to the SAS Viya platform 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**.
- 3 On the Backup and Restore page, start a new backup.

- 4 After the first auto refresh, the **Cancel** button is enabled.
- 5 Click **Cancel**. The following message is displayed:

Backup cancel in progress or complete.

Cancel in the CLI

The cancel operation is new for the May 2019 release.

- 1 Using a command line, log on to the SAS Viya platform as a provider administrator or a tenant administrator in a multi-tenant deployment. Or, log on as a SAS administrator in a standard deployment.

For more information, [“Command-Line Interface: Preliminary Instructions” in SAS Viya Administration: Using the Command-Line Interfaces](#).

- 2 Use the following command to cancel a backup:

```
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.

```
sas-admin backup show -i=backup_job_id
```

Ensure that the backup has a  state.

Backup and Restore: Perform 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”](#).

- Restore a binary backup where the include-all-sources property was set to FALSE.

In this case, you must first manually restore SAS Infrastructure Data Server. For more information, see [“Restore SAS Infrastructure Data Server from a Binary Backup Manually”](#).

For more information about the include-all-sources property, see [“pre-restore validations”](#).

- Restore a binary backup where the include-all-sources property was set to TRUE.

In this case, you must first manually restore SAS Infrastructure Data Server. For more information, see [“Restore SAS Infrastructure Data Server from a Binary Backup Manually”](#).

For more information about the include-all-sources property, see [“pre-restore validations”](#).

Then, you use SAS Backup Manager or a CLI to restore the remaining data sources, which include:

- ☐ SAS Configuration Server
- ☐ SAS Message Broker

Note: When using the SAS Backup Manager or a CLI, you do not have the option of selecting a specific data source to restore from the above data sources. Both data sources are restored from the selected backup.

Then, manually restore CAS. For more information, see [“Restore SAS Cloud Analytic Services”](#).

Note: In the case of a binary backup, the SAS Backup Manager or a CLI ignores the restoration of SAS Infrastructure Data Server content. The SAS Infrastructure Data Server was restored before the other data sources were restored.

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 an unresponsive SAS Infrastructure Data Server. For more information, see [“Restore SAS Infrastructure Data Server from a Binary Backup Manually”](#).
- 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”](#) or [“SAS Infrastructure Data Server, High Availability, and Backup and Restore”](#).
 - ☐ 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.
For more information, see [“Restore SAS Infrastructure Data Server from a Binary Backup Manually”](#).

Best Practices for Performing Restores

- While performing a restore, ensure that the system is not being actively used by stopping unnecessary services. Keep running the following services, which are required for the restore process:
 - ☐ sas-viya-authorization-default
 - ☐ sas-viya-backup-agent-default
 - ☐ sas-viya-backupmanager-default
 - ☐ sas-viya-cachelocator-default
 - ☐ sas-viya-cacheserver-default
 - ☐ sas-viya-cas-administration-default
 - ☐ sas-viya-configuration-default
 - ☐ sas-viya-consul-default
 - ☐ sas-viya-credentials-default
 - ☐ sas-viya-cascontroller-default
 - ☐ sas-viya-deploymentBackup-default
 - ☐ sas-viya-environmentmanager-default
 - ☐ sas-viya-httpproxy-default
 - ☐ sas-viya-identities-default
 - ☐ sas-viya-saslogon-default
 - ☐ sas-viya-notifications-default
 - ☐ sas-viya-rabbitmq-server-default
 - ☐ sas-viya-sasdatasvrc-postgres-node0-consul-template-operation_node
 - ☐ sas-viya-sasdatasvrc-postgres-node0
 - ☐ sas-viya-sasdatasvrc-postgres-node0-consul-template-pg_hba
 - ☐ sas-viya-sasdatasvrc-postgres-pgpool0-consul-template-operation_node
 - ☐ sas-viya-sasdatasvrc-postgres-pgpool0
 - ☐ sas-viya-sasdatasvrc-postgres-pgpool0-consul-template-pool_hba
 - ☐ sas-viya-tenant-default (only in the case of a multi-tenant deployment)
 - ☐ sas-viya-themecontent-default
 - ☐ sas-viya-themes-default
 - ☐ sas-viya-thumbnails-default
 - ☐ sas-viya-vault-default

Note: The backup-agent service must be running on all of the data sources that need to be restored. SAS Infrastructure Data Server (PostgreSQL) services for all the nodes should be running. Stop all SAS services except those above and ensure that the processes have been stopped before initiating a restore. Manually stop any SAS processes that are still running.

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.

- 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.
 - 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 Platform: Configuration Properties](#).
- Because they are created by default, do not restore the following paths:

□ UNIX:

```
/opt/sas/viya/config/data/cas/default/appData
/opt/sas/viya/config/data/cas/default/formats/sassuppliedformats.sashdat
/opt/sas/viya/config/data/cas/default/casuserlibraries/sas.* files
/opt/sas/viya/config/data/cas/default/referenceData
/opt/sas/viya/config/data/cas/default/samples
/opt/sas/viya/config/data/cas/default/search
/opt/sas/viya/config/data/cas/default/sysData
```

□ Windows:

```
C:\ProgramData\SAS\Viya\data\cas\default\appData
C:\ProgramData\SAS\Viya\data\cas\default\formats\sassuppliedformats.sashdat
C:\ProgramData\SAS\Viya\data\cas\default\casuserlibraries\sas.* files
C:\ProgramData\SAS\Viya\data\cas\default\referenceData
C:\ProgramData\SAS\Viya\data\cas\default\samples
C:\ProgramData\SAS\Viya\data\cas\default\search
C:\ProgramData\SAS\Viya\data\cas\default\sysData
```

Prerequisites for a Restore

- Submit the following code to make sure that no table is locked by a service or process, which can prevent the restore process from updating it:

```
select t.relname,l.locktype,page,virtualtransaction,pid,mode,granted from pg_locks l,
pg_stat_all_tables t where l.relation=t.relid and l.mode='AccessExclusiveLock' order by relation asc;
```

From the output, identify the service or process with the lock, stop or kill it, and then rerun the restore process.

- 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 .
- Suppose that you upgraded in place. Or, you migrated to the latest version of the SAS Viya platform. And, you now want to restore a backup. In any case, you cannot use a backup from the previous version of the SAS Viya platform for the restore. Restoring a backup from a previous version is not supported.
- The backup-agent service (called SAS Backup Agent Service on Windows) must be running on all data sources that need to be restored.
- If SAS Infrastructure Data Server has been upgraded, you need to clear the existing shared vault or change the shared vault to a new location. This prevents issues from a mismatch of server version. See [“Create and Edit a Backup Configuration”](#) for more information about changing the shared vault location.

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”](#).
 - 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”](#).

For more information, see [“Restore SAS Infrastructure Data Server from a Binary Backup Manually”](#).
- 3 On the **Backup and Restore** page, select a backup, and click **Restore**.
- 4 In the Restore window, 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  or . Select **Provider** to restore the provider tenant.

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

When the restore is initiated by the provider administrator in a multi-tenant deployment, the selected onboarded tenants that are included in the backup are restored. You should offboard any tenant that is not included in the backup before restoring. Otherwise, these tenants will be unusable after the restore.

Note: It is recommended that when you include the provider tenant in the restore, that you also include all the tenants that were part of the backup. Equivalently, if you select a subset of tenants to restore, do not include the provider tenant.

5 Click **Restore**.

After the restore is completed, a message is displayed with its status as , , or .

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”](#).

7 Check whether there are any errors or warnings in the SAS Infrastructure Data Server (PostgreSQL) pgrestore utility log. If there is an error such as `Error: large object ### does not exist`, stop the unnecessary services and run the restore process again.

8 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: `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=RESUMED`

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

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.

- 9 (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.

- 10 After the restore is complete, check the pg_dump restore logs for errors. Certain pg_restore errors can go undetected. Manual inspection is necessary.

The log files for the restore are found in the following directory:

`sharedVault/backup_ID/tenant_ID/postgres/restore/`

The logs are named:

`restore_ID_SharedServices_pg_dump.dmp_logon_restore.log`

`restore_ID_SharedServices_pg_dump.dmp_restore.log`

Restore Using a Command-Line Interface

- 1 Identify the backup that you want to restore.
- 2 Using a command line, log on to the SAS Viya platform. For more information, see [“Command-Line Interface: Preliminary Instructions” in SAS Viya Administration: Using the Command-Line Interfaces](#).

When you log on to the SAS Viya platform 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”](#).
- 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”](#).

For more information, see [“Restore SAS Infrastructure Data Server from a Binary Backup Manually”](#).

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”](#).

```
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
```

- To restore a backup from an alternate shared vault location, see [“Backup and Restore: Perform a Restore to an Alternate Deployment”](#) for complete instructions.

- 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 included in the backup are restored. You should offboard any tenant that is not included in the backup before restoring. Otherwise, these tenants will be unusable after the restore.

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”](#).

5 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: `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=RESUMED`

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

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.

- 6 After the restore is complete, check the pg_dump restore logs for errors. Certain pg_restore errors can go undetected. Manual inspection is necessary.

The log files for the restore are found in the following directory:

`sharedVault/backup_ID/tenant_ID/postgres/restore/`

The logs are named:

`restore_ID_SharedServices_pg_dump.dmp_logon_restore.log`
`restore_ID_SharedServices_pg_dump.dmp_restore.log`

Restore SAS Infrastructure Data Server from a Binary Backup Manually

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 [“Operate \(Linux\)” 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:

```
sudo systemctl start sas-viya-sasdatasvrc-postgres-node0
```

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

```
sudo service sas-viya-sasdatasvrc-postgresql-instance-name start
```

For example:

```
sudo service sas-viya-sasdatasvrc-postgres-node0 start
```

See [“Operate a Cluster \(Linux\)” in SAS Viya Administration: Infrastructure Servers](#) 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.

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

For example:

```
sudo /etc/init.d/sas-viya-sasdatasvrc-postgres-node0 status
```

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

PGPool is running with PID=4733
Checking Postgresql nodes status...
node_id | hostname | port | status | lb_weight | role | select_cnt | load_balance_node |
replication_delay
-----+-----+-----+-----+-----+-----+-----+-----+
0 | myhost.domain.com | 5432 | up | 0.250000 | primary | 0 | true |
0 | | | | | | | |
(1 row)
```

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

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

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

14 Create a new Shared Vault. For more information, see [“shared vault” on page 6](#). Move the contents of your old shared vault location to the new shared vault location.

15 Ensure that the old shared vault directory is empty.

16 Start all services.

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

Note that in a multi-machine environment, services are started in a particular order. For more information, see [“General Servers and Services: Operate \(Linux\)” in SAS Viya Administration: General Servers and Services](#).

- 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, edit the `sharedVault` property. Update the path from the old shared vault to the new shared vault that you created in step 14.

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\postgres\node0` directory.
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 newly created `node0` directory to match the owner of the original `node0` directory that was renamed in Step 2.

Perform the following steps to change the ownership:

- a Right-click the `node0` directory, and then select **Properties**.
- b On the **Security** tab, click **Advanced**.
- c In the **Advanced Security Settings** window:
 - Change the **Owner** to the user who was the owner of the original (renamed) `node0` directory.
 - Select **Replace owner on subcontainers and objects**.
 - Click **OK**.
- d In the Properties window, click **Edit**.
- e In the Permissions window:
 - Select the same user.
 - Grant **Full control** permissions.
 - Click **OK**.
- 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 the following code to start the SAS Infrastructure Data Server:

```
cd "SASHome\libexec\sasdatasvrc\script"
```

```
.\Invoke-StartStopPostgres.ps1 -action start -batchJob
```

- 9 Verify that the SAS Infrastructure Data Server has started without any issues. Here is an example:

```
PS C:\Windows\system32> cd "C:\Program Files\SAS\Viya\libexec\sasdatasvrc\script"

PS C:\Program Files\SAS\Viya\libexec\sasdatasvrc\script> .\Invoke-HealthCheck.ps1 -batchJob

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 Create a new Shared Vault. For more information, see [“shared vault” on page 6](#). Move the contents of your old shared vault location to the new shared vault location.
- 12 Ensure that the old shared vault directory is empty.
- 13 In the 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, edit the `sharedVault` property. Update the path from the old shared vault to the new shared vault that you created in step 12.

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 must be the owner of the `permstore` directory. If an alternative name for the cas user account was used at deployment time, that user must own the `permstore` directory. If the deployment is multi-tenant, then the user account running the tenant CAS controller must own 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 deployment, the host name directory in the source deployment and in the target deployment 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](#).

Backup and Restore: Perform a Restore to an Alternate Deployment

Overview of Performing a Restore to an Alternate Deployment

Restoring to an alternate deployment means that you can restore a default backup from a source deployment to a target deployment that has machines with different host names and IP addresses. You cannot use a binary backup to restore to an alternate deployment. Performing a restore to an alternate deployment does not deploy the target deployment.

In a standard (non-multi-tenant) deployment, a SAS administrator can perform a restore to an alternate deployment.

In a multi-tenant deployment, only a provider administrator can perform a restore to an alternate deployment.

The steps in this section restore information that the Backup service backed up. For more information about what is backed up, see [“Backup and Restore: Overview”](#).

Note: The information in this section can be used as a part of a disaster recovery strategy. See the [SAS Disaster Recovery Policy for SAS Viya 3.5](#) for more information.

Note: SAS Anti-Money Laundering 8.3 does not support the backup and restore to an alternate deployment.

Terms

The following terminology is used in this section:

Source deployment

deployment where the backups were performed. These backups need to be restored on another (target) deployment.

Target deployment

alternate deployment that has the same SAS Viya platform software installed on it as the source deployment. The restore operation is executed on this target deployment using the backup performed on the source deployment.

Source shared vault

shared vault location for the source deployment. Contains the backup performed in the source deployment.

Target shared vault

shared vault location for the target deployment. This is the existing shared vault location that is used for backup and restore validation prior to performing a restore to an alternate deployment.

Alternate shared vault

alternate shared vault location (that is accessible to the target deployment) where the content from the source shared vault was copied to for the restore.

Prerequisites for Performing a Restore to an Alternate Deployment

Target Deployment

- The SAS Viya platform deployment (such as the version of the SAS Viya platform and any hot fixes applied to it) in the target deployment must be the same as the SAS Viya platform deployment in the source deployment
- The version of SAS Infrastructure Data Server must be the same on both the target deployment and source deployment.
- Tenancy on the target deployment must be the same as tenancy on the source deployment. In other words, the deployment type must both be either non-multi-tenant or multi-tenant.
- PGPool and PostgreSQL topologies, including cluster configuration, must be the same as the source deployment.
- For a multi-tenant deployment, `sas.multi.tenancy.db.mode` configuration must be the same as the source deployment.
- For a multi-tenant deployment, the tenants must match the source deployment. You must have the same tenants in both source and target and the name of the tenants (the tenant IDs) must be the same.
- If the deployment is multi-tenant, restore to alternate deployment supports only restoring a full backup that contains all tenants including the provider tenant.
- The deployment on the target must have been completed successfully and all post-installation and validation tasks, as described in the *SAS Viya for Linux: Deployment Guide* or the *SAS Viya for Windows: Deployment Guide*, have been completed. These steps include:
 - configuring the connection to your LDAP-based identity provider
 - verifying that you can access the deployment using an account other than sasboot
 - creating a backup configuration

- You have adequately tested and successfully performed both a backup and a restore in the target deployment. This prerequisite must be met prior to performing a restore to an alternate deployment.

Configuring a Shared Vault for Restore to an Alternate Deployment

Before restoring a backup to an alternate deployment, you must first create an alternate shared vault to use for the restore. You must copy all content from the source shared vault to the alternate shared vault.

IMPORTANT Do not change the backup configuration in the target deployment to use the shared vault of the source deployment. Do not copy content from the shared vault of the source deployment into the shared vault that you previously configured for the target deployment.

The alternate shared vault must be accessible from every machine in the target deployment that has a configured data source. It must be granted the same access rights as the source shared vault.

Copy the entire content of the source shared vault to the alternate shared vault.

IMPORTANT All content in the source shared vault should be copied to the alternate shared vault, not just a portion of it, such as copying a single backup ID.

For example, you should copy from `source:/sharedVault` to `target:/alternatesharedVault`.

Perform a Restore to an Alternate Deployment

There are two methods for accessing the alternate shared vault for performing the restore to an alternate deployment. Both methods perform the same restore. *If you choose one of the methods and the restore fails, then you should not try the other method.*

- In method A, before performing the restore to an alternate deployment, change the backup configuration in the target deployment. Set the `sharedVault` property to be the path of the alternate shared vault.
- In method B, use a parameter to specify the path to the alternate shared vault on the command line. In this approach, the backup configuration in the target deployment is not changed.

Method A

- 1 If you have not already done so, copy the content of the source shared vault to the alternate shared vault.
- 2 Set the sharedVault property to the location of the alternate shared vault.
For more information about setting the sharedVault property, see [“Create and Edit a Backup Configuration”](#).
- 3 Using the command-line interface, log on to the SAS Viya platform. For more information, see [“Command-Line Interface: Preliminary Instructions”](#) in *SAS Viya Administration: Using the Command-Line Interfaces*.
- 4 On the target deployment, use the following command to view the backup list:
- 5 Confirm that the backup ID intended for restore is listed. Always choose the most recent and successful backup to perform a restore.
- 6 Make sure the target system is not actively being used. Stop all SAS Viya services by running the SAS Viya Multi-Machine Services Utilities playbooks.

```
sas-admin backup list
```

```
ansible-playbook viya-ark/playbooks/viya-mmsu/viya-services-stop.yml
```

- 7 Start the minimally required set of services before starting the restore operation.
- ```
ansible-playbook viya-ark/playbooks/viya-mmsu/viya-services-start-restore.yml
```

- 8 List the status of all SAS Viya services:

```
ansible-playbook viya-ark/playbooks/viya-mmsu/viya-services-status.yml
```

The following services that are running are listed:

- sas-viya-authorization-default
- sas-viya-backup-agent-default
- sas-viya-backupmanager-default
- sas-viya-cachelocator-default
- sas-viya-cacheserver-default
- sas-viya-cas-administration-default
- sas-viya-configuration-default
- sas-viya-consul-default
- sas-viya-credentials-default
- sas-viya-cascontroller-default
- sas-viya-deploymentBackup-default
- sas-viya-environmentmanager-default
- sas-viya-httpproxy-default
- sas-viya-identities-default

- sas-viya-saslogon-default
- sas-viya-notifications-default
- sas-viya-rabbitmq-server-default
- sas-viya-sasdatasvrc-postgres-node0-consul-template-operation\_node
- sas-viya-sasdatasvrc-postgres-node0
- sas-viya-sasdatasvrc-postgres-node0-consul-template-pg\_hba
- sas-viya-sasdatasvrc-postgres-pgpool0-consul-template-operation\_node
- sas-viya-sasdatasvrc-postgres-pgpool0
- sas-viya-sasdatasvrc-postgres-pgpool0-consul-template-pool\_hba
- sas-viya-tenant-default (only in the case of a multi-tenant deployment)
- sas-viya-themecontent-default
- sas-viya-themes-default
- sas-viya-thumbnails-default
- sas-viya-vault-default

---

**Note:** The backup-agent service must be running on all of the data sources that need to be restored. SAS Infrastructure Data Server (PostgreSQL) services for all the nodes should be running. Stop all SAS services except those above and ensure that the processes have been stopped before initiating a restore. Manually stop any SAS processes that are still running except the services listed above.

---

9 Perform the following steps depending on your deployment type.

For a multi-tenant deployment:

**IMPORTANT** If your deployment is configured between 22nd August 2022 and 24th September 2023, then perform Steps 9a - 9g else skip these steps and perform only the Steps 9h - 9j.

a Restore all the non-provider tenants using the following command:

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

b Restore the provider tenant using the following command:

```
sas-admin restore start --backup-name=backup_ID --tenants=provider
```

c Add the following properties to the Consul KV store at **/config/application**

- sas.bootstrap.enabled=false
- sas.bootstrap.oauth2.enabled=true
- sas.bootstrap.tenant.integration.force=true
- sas.bootstrap.tenant.integration.enabled=true
- sas.bootstrap.configuration.enabled=true

The properties can be added using the following commands:

```
. /opt/sas/viya/config/consul.conf
export CONSUL_HTTP_TOKEN=$(sudo cat /opt/sas/viya/config/etc/
SASSecurityCertificateFramework/tokens/consul/default/client.token)
```

For every key-value pair, run the following command:

```
/opt/sas/viya/home/bin/sas-bootstrap-config kv write --force config/application/key value
```

Here is an example:

```
/opt/sas/viya/home/bin/sas-bootstrap-config kv write --force config/application/
sas.bootstrap.enabled false
```

d Restart all services.

e Wait until all tenants are onboarded. View the **Tenants** tab in SAS Environment Manager for the status of the tenants.

f Remove the properties that you added to the `/config/application` in [Step C on page 46](#) by using the following command.

```
/opt/sas/viya/home/bin/sas-bootstrap-config kv delete config/application/key
```

Here is an example:

```
/opt/sas/viya/home/bin/sas-bootstrap-config kv delete config/application/
sas.bootstrap.enabled
```

g Restart all the services again.

h Restore the provider tenant using the following command:

**IMPORTANT** If your deployment is configured after 24th September 2023, perform only the Steps 9h - 9j:

```
sas-admin restore start --backup-name=backup_ID --tenants=provider
```

i Restart all services.

j Restore the remaining tenants using the following command:

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

10 For a standard (non-multi-tenant) deployment, restore the backup using the following command:

```
sas-admin restore start --backup-name=backup-id
```

11 Note the *jobID* printed on the console.

12 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.

---

**Note:** If you receive a failed status, see the [“Backup and Restore: Troubleshooting”](#) for possible causes and logs.

---

- 13 After the restore is complete, check the pg\_dump restore logs for errors. Certain pg\_restore errors can go undetected. Manual inspection is necessary.

The log files for the restore are found in the following directory:

***sharedVault/backup\_ID/tenant\_ID/postgres/restore/***

The logs are named:

```
restore_ID_SharedServices_pg_dump.dmp_logon_restore.log
restore_ID_SharedServices_pg_dump.dmp_restore.log
```

- 14 Stop all services. Restore SAS Cloud Analytic Services.

For more information, see [“Restore SAS Cloud Analytic Services”](#).

- 15 Start all services and then restore scheduled jobs.

For more information, see [Step 5: To restore jobs, the administrator must perform the following tasks](#).

## Method B

- 1 If you have not already done so, copy the content of the source shared vault to the alternate shared vault.
- 2 Using the command-line interface, log on to the SAS Viya platform. For more information, see [“Command-Line Interface: Preliminary Instructions” in SAS Viya Administration: Using the Command-Line Interfaces](#).
- 3 Inspect the alternate shared vault and note the backup ID that you intend to restore. Always choose the most recent and successful backup to perform a restore.
- 4 Make sure the target system is not actively being used. Stop all SAS Viya services by running the SAS Viya Multi-Machine Services Utilities playbooks.

```
ansible-playbook viya-ark/playbooks/viya-mmsu/viya-services-stop.yml
```

- 5 Start the minimally required set of services before starting the restore operation.

```
ansible-playbook viya-ark/playbooks/viya-mmsu/viya-services-start-restore.yml
```

- 6 List the status of all SAS Viya services:

```
ansible-playbook viya-ark/playbooks/viya-mmsu/viya-services-status.yml
```

The following services that are running are listed:

- sas-viya-authorization-default
- sas-viya-backup-agent-default
- sas-viya-backupmanager-default
- sas-viya-cachelocator-default
- sas-viya-cacheserver-default

- sas-viya-cas-administration-default
- sas-viya-configuration-default
- sas-viya-consul-default
- sas-viya-credentials-default
- sas-viya-cascontroller-default
- sas-viya-deploymentBackup-default
- sas-viya-environmentmanager-default
- sas-viya-httpproxy-default
- sas-viya-identities-default
- sas-viya-saslogon-default
- sas-viya-notifications-default
- sas-viya-rabbitmq-server-default
- sas-viya-sasdatasvrc-postgres-node0-consul-template-operation\_node
- sas-viya-sasdatasvrc-postgres-node0
- sas-viya-sasdatasvrc-postgres-node0-consul-template-pg\_hba
- sas-viya-sasdatasvrc-postgres-pgpool0-consul-template-operation\_node
- sas-viya-sasdatasvrc-postgres-pgpool0
- sas-viya-sasdatasvrc-postgres-pgpool0-consul-template-pool\_hba
- sas-viya-tenant-default (only in the case of a multi-tenant deployment)
- sas-viya-themecontent-default
- sas-viya-themes-default
- sas-viya-thumbnails-default
- sas-viya-vault-default

---

**Note:** The backup-agent service must be running on all of the data sources that need to be restored. SAS Infrastructure Data Server (PostgreSQL) services for all the nodes should be running. Stop all SAS services except those above and ensure that the processes have been stopped before initiating a restore. Manually stop any SAS processes that are still running except the services listed above.

---

## 7 Perform the following steps depending on your deployment type.

For a multi-tenant deployment:

**IMPORTANT** If your deployment is configured between 22nd August 2022 and 24th September 2023, perform only the Steps 7a - 7g else skip these steps and perform only the Steps 7h - 7j.

- a Restore all the non-provider tenants using the following command:

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

- b Restore the provider tenant using the following command:

```
sas-admin restore start --backup-name=backup_ID --alternate-shared-vault-for-restore=path_of_alterate_sharedVault --tenants=provider
```

- c Add the following properties to the Consul KV store at `/config/application`

- `sas.bootstrap.enabled=false`
- `sas.bootstrap.oauth2.enabled=true`
- `sas.bootstrap.tenant.integration.force=true`
- `sas.bootstrap.tenant.integration.enabled=true`
- `sas.bootstrap.configuration.enabled=true`

The properties can be added using the following commands:

```
. /opt/sas/viya/config/consul.conf
export CONSUL_HTTP_TOKEN=$(sudo cat /opt/sas/viya/config/etc/SASSecurityCertificateFramework/tokens/consul/default/client.token)
```

For every key-value pair, run the following command:

```
/opt/sas/viya/home/bin/sas-bootstrap-config kv write --force config/application/key value
```

Here is an example:

```
/opt/sas/viya/home/bin/sas-bootstrap-config kv write --force config/application/sas.bootstrap.enabled false
```

- d Restart all services.
- e Wait until all tenants are onboarded. View the **Tenants** tab in SAS Environment Manager for the status of the tenants.
- f Remove the properties that you added to the `/config/application` in [Step C on page 50](#) by using the following command.

```
/opt/sas/viya/home/bin/sas-bootstrap-config kv delete config/application/key
```

Here is an example:

```
/opt/sas/viya/home/bin/sas-bootstrap-config kv delete config/application/sas.bootstrap.enabled
```

- g Restart all the services again.
- h Restore the provider tenant using the following command:

**IMPORTANT** If your deployment is configured after 24th September 2023, perform only the Steps 7h - 7j:

```
sas-admin restore start --backup-name=backup_ID --alternate-shared-vault-for-restore=path_of_alterate_sharedVault --tenants=provider
```

- i Restart all services.

- j Restore the remaining tenants using the following command:

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

For a standard (non-multi-tenant) deployment, restore the backup using the following command:

```
sas-admin restore start --backup-name=backup_ID
--alternate-shared-vault-for-restore=path_of_alterdate_sharedVault
```

- 8 Note the *jobID* printed on the console.
- 9 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.

---

**Note:** If you receive a failed status, see the [“Backup and Restore: Troubleshooting”](#) for possible causes and logs.

---

- 10 After the restore is complete, check the pg\_dump restore logs for errors. Certain pg\_restore errors can go undetected. Manual inspection is necessary.

The log files for the restore are found in the following directory:

***sharedVault/backup\_ID/tenant\_ID/postgres/restore/***

The logs are named:

```
restore_ID_SharedServices_pg_dump.dmp_logon_restore.log
restore_ID_SharedServices_pg_dump.dmp_restore.log
```

- 11 Stop all services. Restore SAS Cloud Analytic Services.

For more information, see [“Restore SAS Cloud Analytic Services”](#).

- 12 Start all services and then restore scheduled jobs.

For more information, see [Step 5: To restore jobs, the administrator must perform the following tasks](#).

# Backup and Restore: 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;
```

**Note:** The `accessControl.createBackup` action has parameters. See [“Create backup” in SAS Viya Platform: System Programming Guide](#) for more information.

- 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*

---

## Restore Programming-Only Deployment

- 1 Stop the CAS server.

See *SAS Viya Administration: Using CAS Server Monitor*.

- 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 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.

See *SAS Viya Administration: Using CAS Server Monitor*.

- 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](#).

---

## Backup and Restore: 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: *SAS-configuration-directory*/var/log/backup-agent/default

On Windows: *SAS-configuration-directory*\var\log\backupagent\default

- When restoring a default backup for SAS Infrastructure Data Server, the log files for the restore are dumped to the following directory:

*sharedVault/backup\_ID/tenant\_ID/postgres/restore/*

The logs are named:

*restore\_ID\_SharedServices\_pg\_dump.dmp\_logon\_restore.log*

*restore\_ID\_SharedServices\_pg\_dump.dmp\_restore.log*

---

## 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.

For the May 2019 release, see [“Backup and Restore: Cancel a Backup”](#).

Otherwise, here is how to stop a backup that is in progress:

- 1 On the command line in Linux, enter `sas-admin backup cancel -i=backup_id`. To determine whether the cancel sub-command is supported, enter `sas-admin backup help`. If the cancel sub-command is not supported, you must stop and then restart the Backup service.
- 2 Ensure that the backup has a  state.
- 3 Perform a backup.

For more information, see [“Backup and Restore: Perform a Backup”](#).

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`.  
  
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 [“Backup and Restore: Perform a Restore”](#).

## 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”](#).

## 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”](#).

## 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 deployment should be the same as the source deployment. Use a different backup ID to restore to the target deployment.

## 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 the current release of the SAS Viya platform, 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 and Flows: How To \(Jobs in SAS Environment Manager\)”](#) in *SAS Viya Administration: Jobs and Flows*.

## Cancel operation fails for backup.

A cancel operation failed for source {0}. Here is the error message:

```
The backup operation with the process ID "{1}" could not be canceled for the source "{0}"
```

To resolve this issue, manually terminate the OS process with ID {1}.

## No system data on Available tab on Data page.

During a restore to an alternate deployment, you might receive SAS log messages indicating that a connection to the CAS server was unsuccessful. To resolve this issue, unregister and reregister the client identity used by the batch ETL jobs.

- 1 Using a command line, log on to the SAS Viya platform. For more information, see [“Command-Line Interface: Preliminary Instructions” in SAS Viya Administration: Using the Command-Line Interfaces](#).
- 2 To unregister the client identity, submit:  

```
ops-util deregister -id sas.ops-agentsrv
```
- 3 To reregister the client identity, submit:  

```
ops-util register -id sas.ops-agentsrv -force
```

This obtains a new OAuth token.
- 4 To verify registration, retrieve the current OAuth token for the newly registered client identity.  

```
ops-util token -id sas.ops-agentsrv
```
- 5 (Optional) Perform steps 2 through 4 for the sas.ops-agent client identity (replace `sas.ops-agentsrv` with `sas.ops-agent`).

## Backup in running state a long time after canceling another backup.

Suppose a backup is started and then canceled. Another backup is started. If the later backup is in the running state for a long time, you should restart all instances of the Backup service and the backup-agent service. After the services have been restarted, start the backup again.

## Backup ID for restore is not displayed in SAS Backup Manager or in the sas-admin backup list.

If you are performing restore to alternate deployment using method A, and you do not see the backup ID listed for restore in sas-admin backup list, then restart SAS Backup Service (`sas-viya-deploymentBackup-default`).

## Scheduled backups are failing or you are unable to initiate an immediate (ad hoc) backup or restore.

If scheduled backups are failing or if you cannot initiate an immediate (ad hoc) backup or restore, check whether the following services are running: SAS Infrastructure Data Server, SAS Message Broker, SAS Configuration Server, SAS Cloud Analytic Services, and any additional SAS

Infrastructure Data Servers. Check whether each node on which these services is running also has a SAS Backup Agent installed and running.

## Restore process hangs in the beginning.

The restore process cleans the data by deleting it at the beginning. If there is a process using a table and it has a lock on it, the restore process waits for the lock to release. Ideally, the process should have released the lock after it processed, but there can be orphaned processes running in the background that never released the lock. As a result, the restore process can wait forever.

To find the process that has a lock, follow these steps:

---

**Note:** By default, in these steps, SASHome is `/opt/sas/viya/home`. If your deployment uses a different SASHome directory, modify the path to match your deployment.

---

1 To get the password of the dbmsowner user (the default user), see [Get Current Passwords](#).

2 Navigate to `/opt/sas/viya/home/postgresql11/bin`.

3 Start the psql utility:

```
./psql -h localhost -d SharedServices -U dbmsowner
```

4 Submit the following query to find the lock:

```
select t.relname,l.locktype,page,virtualtransaction,pid,mode,granted from pg_locks l,
pg_stat_all_tables t where l.relation=t.relid and l.mode='AccessExclusiveLock' order by relation asc;
```

5 From the output, identify the service or process with the lock, stop or kill it, and then rerun the restore process.

6 Enter `\q` to stop the psql utility.

## Large object ### does not exist.

A service can have an indirect lock on a table, which can prevent a successful restoration of a large object in the table. The restore process does not wait to release the lock; it fails and displays the following error:

```
Error: large object ### does not exist
```

In this error message, `###` is the number of the object that cannot be restored. If this error occurs, stop all services, and keep running only the minimum services that are required for the restore process.

If you are running only the minimum services that are required for the restore process and you have a problem restoring a tenant in a multi-tenant environment, then try to restore the tenant individually. For more information about these services, see [“Best Practices for Performing Restores”](#).

## Issue performing backup or restore of more than 20 tenants.

In a multi-tenant system with more than 20 tenants, if the default values for `jobMaximumThreadpoolSize` and `jobQueueCapacity` are not changed, and if an issue occurs in a backup or restore operation, then `jobMaximumThreadpoolSize` and `jobQueueCapacity` should be increased. These two properties are linked and should be increased accordingly. See [“jobMaximumThreadpoolSize”](#) and [“jobQueueCapacity”](#) for default values and more details.

- To increase `jobMaximumThreadpoolSize`, update `config/deploymentBackup/backup.jobMaximumThreadpoolSize` in Consul. The value must be greater than 10.
- To increase `jobQueueCapacity`, update `config/deploymentBackup/backup.jobQueueCapacity` in Consul. The value must be greater than 10.

To use the increased values when creating the thread pool, the Backup service must be restarted. On the command line in Linux, enter:

```
sudo /etc/init.d/sas-viya-deploymentBackup-default restart
```

## Consul restore warning "mediaType": "application/vnd.sas.configuration.config.sas.cache+json;version=4" not found.

When you restore a new SAS Viya 3.5 environment from a backup of an older environment that was continually updated, you might receive the following warning when you restore Consul.

```
Consul restore warning "mediaType": "application/vnd.sas.configuration.config.sas.cache+json;version=4" not found
```

This warning can be ignored because it does not impact the restoration of Consul.

This warning is displayed because the `sas.cache` media type was deprecated in favor of the `sas.cache.config` media type and was removed.

## Problems Restoring PostgreSQL Database

If you are running the backup-agent 2.31.0 and using the October 2024 (24w44) release of SAS Viya 3.5 you might encounter issues on restore.

To work around this problem:

- 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 in the properties. 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 Scroll down until you see **sas.deploymentbackup**, and click  to the right of the service.
- 6 Include the following option: `postgresBackupAdditionalOptions: -F c`
- 7 Restart the backup-related services.

```
sudo systemctl restart sas-viya-deploymentBackup-default
sudo systemctl restart sas-viya-backup-agent-default
```
- 8 Run a new backup.
- 9 Navigate to the [sharedVault path on page 44](#). Inside the backup directory, go to the **postgres** folder. Check the dump file type, using for example: `file SharedServices_pg_dump.dmp`. The dump type should be **PostgreSQL custom database**. If so, this backup is good and can be restored when needed.

This issue was corrected in the December 2024 (24w51) release. These steps are not necessary for that release or later.