Backup and Restore: Overview

This backup and restore documentation applies to a Linux installation.

The Backup and Restore service, when executed, automatically discovers information about your SAS Viya deployment and backs up critical configuration and user content from your SAS Viya deployment. To protect the integrity of content and configuration information stored in SAS Viya components, SAS recommends that you run the Backup service as part of a regularly scheduled backup process.

**Important:** The Backup service does not take the place of operating system or file system backups.

Backup and restore functions can be initiated only by SAS Administrators.

Backup and Restore: Terms and Concepts

Backup and Restore Terms

Here is a list of terms used in this document for the Backup and Restore service:

**Backup Types**

There are two types of backups that are provided by backup service:

- **default**—This is the default value for the backup type. When the backup type is default, `pg_dump` is used to back up the SAS Infrastructure Data server. `pg_dump` backs up the content in the database but does not include the PostgreSQL metadata such as user information, roles, and permissions.

  The default backup requires that the PostgreSQL metadata is not significantly changed. The default backup type can be fully restored using the SAS restore operation. The restore includes the Postgres data content, as well as the configuration data and other data sources.

- **binary**—When the backup type is binary, the `pg_basebackup` utility is used to back up the SAS Infrastructure Data Server. This takes the backup of all the binaries of the PostgreSQL including metadata such as user information, roles, and permissions. You can also back up other data sources by setting `includeAllSourcesForBinaryBackup` to `true` while initiating the backup.
The PostgreSQL portion of a binary backup must be restored manually. If the `includeAllSourcesForBinaryBackup` is set to `true` and the manual restore of PostgreSQL is completed, a SAS restore of the other portions of the binary backup could restore configuration data and whatever other data sources were included.

**Deployment backup**

A multi-tenant deployment in which only a Provider Administrator can initiate backup for multiple tenants in a single API call for those tenants. If an explicit list of tenants is not provided, the backup for all ONBOARDED tenants is triggered.

**Deployment restore**

A multi-tenant deployment in which only a Provider Administrator can initiate a restore of a Deployment Backup (with at least one successful tenant Backup) for multiple tenants in a single API for those tenants. The restore request accepts the list of tenants to be restored. If this list is not provided, the backup service creates this list with the tenants that are onboarded and are a provider. If all the tenants in the list are present in the backup, then the restore is triggered for each of the tenants on the list. If any of the tenants on the list are not present in the backup, then the restore does not proceed and is marked as failed.

**Intra-tenant administrator**

A SAS Administrator that is responsible for the administration of each tenant’s internal resources. For example, assigning users to custom groups and managing access to SAS Viya content and CAS data are intra-tenant tasks.

**Local Vault**

A local file system path located on the same host as where a backup source resides. It is the location where the backup files for the data source are created and then moved to the shared vault.

**Multi-tenant deployment**

A SAS Viya deployment in which multiple tenants can access the same environment in isolated fashion such that data of tenants are not affected or impacted by other tenant's data or process. A multi-tenant deployment has the provider tenant by default.

**Pre-restore validations**

Validations that are done before performing a restore using a given backup. It includes the following validation checks:

- Does the provided backup exist?
- Is the backup completed?
- Is the backup purged?
- If PostgreSQL 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 Postgres?
- If the restore is using the binary type of backup, is the `includeAllSourcesForBinaryBackup` property set to `true`? If the `includeAllSourcesForBinaryBackup` is set to `false`, the restore fails. To restore the PostgreSQL portion of a binary backup, see Restore an Unresponsive SAS Infrastructure Data Server.
- 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.

**Provider administrator**

A SAS Administrator user who belongs to the ‘provider’ tenant in a multi-tenant deployment and is responsible for administering system-level operations for all the tenants like backup.

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

sas-viya-deploymentBackup-default
service used to schedule a default backup.

Shared Vault
any network location to preserve the backups from all tiers. The backup files are moved from local vault to shared vault. SAS user must have created the shared vault directory. It is referred to as sharedVault in the SAS Environment Manager user interface.

Single-tenant deployment
a SAS Viya installation intended to be used only by a single tenant.

Slug
user-provided name for the backup or restore operation.

State
state of a backup or restore operation. Possible values for this attribute are as follows:
- pending—a backup or restore job has been created but the operation has not yet started.
- running—a backup or restore is in progress.
- completedWithWarning—at least one tenant backup or restore has failed or the CAS controller host is not reachable.
- completed—the backup or restore operation has completed successfully.
- failed—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 it does not have a backup agent, contact your administrator. If it has a backup agent, then restart the backup agent service.

Tenant
one of the customers using a shared SAS Viya deployment.

In a multi-tenant system, a tenant is said to be onboarded when the SAS Viya infrastructure for that tenant is created. This includes the LDAP groups, the LDAP identities, the SAS Infrastructure server databases, the schemas, and the SAS Cloud Analytics Server instance.

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

About the Backup and Restore Service
The Backup and Restore service is provided as a way to synchronize the backup and restoring of content and configuration information stored in the following components of a SAS Viya deployment:
- SAS Infrastructure Data Server
- SAS Configuration Server
- SAS Message Broker
- SAS Cloud Analytic Services (CAS Access Controls, Caslib information)

The Backup and Restore service has the following caveats:
- Backup and restore can be initiated only by SAS Administrators.
- The Backup and Restore service requires that the SAS Infrastructure Data Server is running.
What Is Backed Up

The backup service backs up the following components of your SAS deployment:

- **SAS Infrastructure Data Server (PostgreSQL)** – All of the PostgreSQL tables in the database managed by the SAS Infrastructure Data Server are backed up by the Backup and Restore service. If the SAS Infrastructure Data Server is clustered, only the tables on the primary PostgreSQL node are backed up. PostgreSQL metadata (system catalogs) such as user information, roles, and permissions that are stored in the SAS Infrastructure Data Server are backed up only when a binary backup is used.

  In addition, any scheduled jobs such as automatic report distribution jobs and scheduled backup jobs can be properly restored only when a binary backup is used.

- **SAS Configuration Server (Consul)** – The service configuration registry that serves as a central repository for configuration data, service discovery, and health status. Only the service configuration that is registered with the configuration service and accessible to the tenant initiating the backup is backed up. This implies only a subset of the Consul Key Value store is backed up.

- **SAS Message Broker (RabbitMQ)** – RabbitMQ configuration such as the queue definitions.

- **SAS Cloud Analytic Services (CAS Access Controls)** – CAS configuration containing CAS Access Controls and Caslib Information.

These sources might reside on single machine or on different machines.

What Is Not Backed Up

The backup service does not back up the following:

- The SAS Viya deployment. Files that are included as part of your SAS Viya deployment are not backed up. The Backup and Restore service backs up content and configuration information but is not provided as a way to back up and restore a SAS Viya deployment.

- In a SAS Message Broker backup, messages or data from the queues are not backed up.

- In a clustered CAS environment, the backup action is invoked only on the primary controller.

- Data stored in data sources outside of the SAS Infrastructure Data Server are not backed up.

- Data that is loaded to CAS is not backed up.

- PostgreSQL metadata such as user information, roles, and permissions that are stored in the SAS Infrastructure Data Server are not backed up when the default backup type is used.

- Scheduled jobs such as automatic report distribution jobs and scheduled backup jobs can be properly restored only when a binary backup is used.

- The Backup and Restore service does not take the place of the operating system and file system backups.

- The SAS Message Broker is not backed up when the backup is initiated by an intra-tenant administrator. In a multi-tenant deployment, an intra-tenant administrator cannot take a binary type of backup.

Backup and Restore: Getting Started

A DEFAULT_BACKUP_SCHEDULE is created for you by the deployment process. The DEFAULT_BACKUP_SCHEDULE is set to run every Sunday at 1:00 a.m. There are some additional steps required before you can use the DEFAULT_BACKUP_SCHEDULE.
Confirm that the DEFAULT_BACKUP_SCHEDULE exists in the SAS Environment Manager. To do so, log on to the SAS Environment Manager and click [button]. If the DEFAULT_BACKUP_SCHEDULE does not exist, you must restart the sas-viya-deploymentBackup service and check again.

There are a couple of reasons why the DEFAULT_BACKUP_SCHEDULE might not exist.

a. If a service that is starting fails to register itself with SASLogon, the service tries multiple times to do the client registration until the client registration is done. If this is the case, then the default backup is not created, since it is not able to generate client tokens to access other services such as scheduling or jobExecution. The following error message is displayed:

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

b. While backup service is starting, other services have not yet started. For more information about what services should be running, see How the Restore Process Works on page [14].

In this scenario, the deploymentBackup service retries 25 times to schedule the default backup. If one or more of the services is not running when the 25 times is done, you see the following error message:

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.

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

Complete the steps for Backup Configuration Properties to set the shared vault location. The SAS user must have created the shared vault directory.

3. In the SAS Environment Manager click [button]. In the Jobs list, right-click the DEFAULT_BACKUP_SCHEDULE.

4. Select Run from the pop-up menu to immediately run the backup. If you do not do this, the backup runs on Sunday at 1:00 a.m.

5. In the SAS Environment Manager click [button]. Confirm that the DEFAULT_BACKUP_SCHEDULE is in the list.

SAS Infrastructure Data Server Binary Backup

Overview

The backup service takes the “binary” type for the backup of PostgresSQL using the binary backup and the “default” type for the backup using the default backup. The PostgresSQL backup taken using the binary backup is useful to restore an unresponsive Postgres that occurs for reasons such as the corruption of Postgres system configuration data due to hard drive or memory issues. Without this type of backup, it is not possible to recover on unresponsive PostgreSQL server. The restore mechanism using binary backup is a manual process that is performed by the administrator. See Restore an Unresponsive SAS Infrastructure Data Server for the manual steps required to restore PostgresSQL.
When to Use the Binary Backup and When to Use the Default Backup

Binary Backup
The binary backup uses pg_basebackup, which makes a binary copy of the database cluster files, making sure that the system is put in and out of backup mode automatically. Backups are always taken of the entire database cluster, including the system catalogs, which contain the system configuration that is common for all the databases. The system configuration includes database users, their permissions, databases present in the server, their schemas, as well as other configuration data.

The default backup does not back up this common data, and it cannot restore this system information if it becomes corrupted. Therefore, it is recommended that the user create a new schedule for the binary backup. If there is any change in the system catalog, the binary backup should be run to back up those changes. For more information about system catalog, see https://www.postgresql.org/docs/9.4/static/catalogs.html.

Default Backup
The default backup uses pg_dump, which dumps a single database that is provided as an option to the pg_dump utility. It is not possible to restore individual databases or database objects from the backup taken by the binary backup. If a particular database is corrupted and needs to be restored without affecting other databases, the default backup should be used.

The default backup is essential in the following situations:

- In multi-tenancy, it can back up databases selectively, whereas the binary backs up all of the databases.
- Restoring to an alternate host is not possible with the backup taken by the binary backup. The binary backup overwrites the system catalog from the original environment to the destination environment. Therefore, a default backup is required.

How to Use the Binary Backup and the Default Backup
For an immediate backup, you can initiate a default backup through the SAS Environment Manager. You can manually schedule a binary backup. For more information see Schedule a Backup.

Other data sources such as the SAS Infrastructure Data Server, the SAS Cloud Analytic Services (CAS Access Controls, Caslib information), and the SAS Message Broker are not backed up by default with the binary backup. They are backed up with the default type of backup. You need to specifically request the backup of other data sources along with Postgres when using the binary backup. This is done by setting the includeAllSourcesForBinaryBackup parameter to true in the backup request body.

If data is corrupted, you first must try to recover using the default backup. To do this, check the history for last successful backup and then recover from that. If Postgres is not responsive, getting the backup history and initiating a regular restore is not possible. Even the pgadmin client cannot connect and access a corrupted database. If this is the case, you must recover Postgres manually using the binary backup. See Restore an Unresponsive SAS Infrastructure Data Server for the manual steps required to restore PostgreSQL. After manually restoring using the binary backup, Postgres is responsive. Then you can perform a regular restore from the latest successful default backup to restore the content and configuration to a point in time as late as possible.

Implementation Details
The backup service’s POST /backups/jobs rest endpoint accepts the backup request payload that contains the parameters backupType and includeAllSourcesForBinaryBackup. These parameters indicate which type of backup (binary or default) is to be used for backing up Postgres.
The backupType parameter in the backup request can have one of the following values:

- **default**—indicates that Postgres is being backed up using the default backup. This is the default value if the parameter is missing in the request body.

- **binary**—indicates that Postgres is being backed up using the binary backup.

  **Note:** The binary backup is made over a regular PostgreSQL connection, and uses the replication protocol. The connection must be made by a superuser or by a user with REPLICATION permissions. pg_hba.conf must explicitly permit the replication connection. For more information about prerequisites of binary backup, see https://www.postgresql.org/docs/9.5/static/app-pgbasebackup.html.

When the backupType is set to **binary**, you can use the includeAllSourcesForBinaryBackup parameter. This parameter, if provided in the backup request, has an option to also back up other sources, while taking a backup of Postgres using binary backup utility.

The includeAllSourcesForBinaryBackup parameter can have one of the following values:

- **false**—indicates only Postgres is backed up. This is the default value for this parameter.

- **true**—indicates that other sources are to be backed up along with the Postgres backup. In the case of a multi-tenant environment, all tenants are included in this backup by default.

The backupType and includeAllSourcesForBinaryBackup parameters are also visible in the details of the backup. This is helpful in identifying if the backup contains the backup taken using the binary backup or the default backup and if other data sources are present in this backup.

**Note:** While restoring a binary backup, Postgres should be restored before all other data sources. Otherwise, restoring the other data sources fails due to an unresponsive Postgres.

### Implications on Current Backup and Multi-tenancy

1. The binary backup is an additional mechanism to back up the Postgres. This is not a replacement to the existing default backup. However, these two backups are mutually exclusive. That is, a backup that contains a Postgres backup using binary backup would not contain a backup using default backup and vice versa.

2. The binary backup does not support backing up individual databases. The binary backup is always a backup of Postgres for the entire deployment. To support the backup and restore of individual tenants, the default backup is used.

3. Two schedules are required for backup. By default, a backup schedule is present for the default type of backup. You must manually schedule the binary type of backup.

   **Note:** In a multi-tenant environment, only a Provide Administrator User can execute an ad hoc binary backup or can create a schedule for binary backup.

   For more information about scheduling a binary backup see Schedule a Binary Backup. The binary backup used to support the restore of Postgres using its binaries, should be scheduled monthly. Both of the schedules can be configured based on the customer’s requirement. However, the binary backup schedule (monthly) can be less frequent compared to the default backup schedule (weekly).

### Backup and Restore: Guidelines

#### Best Practices for Configuring Backups

- Always ensure the values of the `sharedVault` and `retentionPolicy` are set immediately after situations such as a fresh installation, an upgrade, or any modifications to your SAS deployment.
Ensure that the sharedVault is accessible to the install user.

Note: The shared vault location must be different from the local vault location.

Set the retentionPeriod value such that you always have at least the last three to four backups at any point in time. For example, if you are doing daily backups, the retentionPeriod must be 4 days. If you are doing weekly backups, the recommended retentionPeriod is 30 days.

Scheduling is not supported out-of-the-box for binary backups. It is recommended that the administrator schedule a call to the backup REST API to perform scheduled backups. Backups should be scheduled at non-peak hours.

If an upgrade has happened for this SAS Viya setup, log on to the SAS Environment Manager application. Navigate to the backup service configuration screen and make sure that the sharedVault property value is set to the intended location. For a custom property, add the key restore.filter.sas.configuration.config.sas.deploymentbackup and the value "" (without quotation marks). This property should be added under 'supplimentalProperties' section using the Add Property option.

Always initiate a binary backup after a tenant has been onboarded or offboarded.

**Best Practices for Performing Backups**

Always use the Backup and Restore service to perform backups of the content and configuration that is stored in SAS Viya components. This is because the backup service automatically discovers what services are deployed and finds newly deployed services that should be included in the backup. The backup service also finds content and configuration data from your SAS Viya deployment. The backup service backs them up at the same point in time, which is required for a same point-in-time restore of content and configuration data.

Configure the backup service immediately after situations such as a new installation, upgrading software, or after making any modifications to your SAS Viya deployment. See Backup and Restore: Service Configuration for more details.

It is recommended that you schedule a binary backup so that it can be used to recover the SAS Infrastructure Data Server when it becomes unresponsive.

Run the Backup service after making any modifications to your SAS Viya deployments. Examples of modifications include, but are not limited to, deploying SAS Viya, installing software updates, changes to topology, modifications to the SAS Viya configuration, including configuration properties.

Old backups are purged after the retention period. If you do not want any of your backups to be deleted after the retention period, you must manually archive the backups to a safe location before they are purged.

**Best Practices for Postgres on a Single-node When the SAS Infrastructure Data Server Is not Configured for High Availability**

As previously described in the About the Backup and Restore Service on page 3 section of this document, performing a restore with the Backup and Restore service requires that the SAS Infrastructure Data Server is running. In an event where the SAS Infrastructure Data Server does not start due to PostgreSQL corruption or for any other reason, you cannot perform a restore with the Backup and Restore service. SAS Viya deployments, which implement the SAS Infrastructure Data Server for HA, have a standby server (or node). In an event where the primary node is unresponsive, a standby node can be promoted to primary status. If promotion of the standby node to primary node is successful and the SAS Infrastructure Data Server can be started, you can then perform a restore.

If you have not configured the SAS Infrastructure Data Server for High-Availability (which is the default configuration), only a single PostgreSQL data server is configured. When only a single PostgreSQL data server is configured, it is recommended that you use the backup service to take a binary type of backup to create a
binary copy of the data to be used as a basis for a point-in-time restore. It is recommended that you initiate a binary backup after any configuration or installation changes are made to the SAS Viya environment. For information about how to restore the SAS Infrastructure Data Server when the server is unresponsive due to PostgreSQL corruption or for any other reason, see Restore an Unresponsive SAS Infrastructure Data Server.

Best Practices for Performing Restores

- Always use the Deployment Backup and Restore service to perform restores to ensure a same point-in-time restore of content and configuration data.
- Always choose the most recent successful backup to perform a restore operation.
- Ensure minimum use of the systems. When performing a restore, only the following services should be running. For more information about what services are running, see Machines under the “SAS Environment Manager Functions” section.

sas-viya-consul-default
sas-viya-vault-default

sas-viya-sasdatasvrc-postgres-node0-ct-pg_hba
sas-viya-sasdatasvrc-postgres-node0-ct-postgresql
sas-viya-sasdatasvrc-postgres-pgpool0-ct-pcp
sas-viya-sasdatasvrc-postgres-pgpool0-ct-pgpool
sas-viya-sasdatasvrc-postgres-pgpool0-ct-pool_hba
sas-viya-sasdatasvrc-postgres-node0

sas-viya-cascontroller-default
sas-viya-httpproxy-default
sas-viya-rabbitmq-server-default
sas-viya-sasdatasvrc-postgres
sas-viya-authorization-default
sas-viya-cachelocator-default
sas-viya-configuration-default
sas-viya-identities-default
sas-viya-saslogon-default
avsas-viya-cas-management-default
sas-viya-tenant-default (only in the case of a multi-tenant deployment)
sas-viya-deploymentBackup-default
sas-viya-backup-agent-default

Note: The preceding step should be considered only during a restore on a single-tenant deployment or when performing a deployment restore in a multi-tenant environment. Do not stop any service while performing a tenant restore.

- The backup-agent service must be running on all the data sources that need to be restored.
- After performing a restore, stop and restart all services.
  - Stop all services:
    
    ```
    sudo /etc/init.d/sas-viya-all-services stop
    ```
  - Start all services:
    
    ```
    sudo /etc/init.d/sas-viya-all-services start
    ```

Note: Starting and stopping the services is applicable only for a single-tenant restore or a deployment restore in multi-tenant deployment. This is not applicable for a tenant restore.
Backup and Restore: Service Configuration

Backup Configuration Properties

The backup service has its own configuration that is used to perform the backup and restore. The backup configuration includes configuration properties, which come with default values. The sharedVault property does not have a default value.

The following configuration properties can be changed:

- retentionPeriod —The number of days that backups are stored before they are removed from the shared vault. The backups cannot be recovered once they are deleted.
- sharedVault —A shared network location to keep a safe copy of the backup. This directory must exist, and be writeable by the install user (sas) and the user who executes the backup command. In a multi-tenant deployment, the install user must have Read and Write permissions on every machine. It is referred to as the Shared Vault in this document.

Modify the Backup Configuration Using the Environment Manager

The configuration properties retentionPeriod and sharedVault can be modified using SAS Environment Manager.

1. Log on to <protocol>://<host>:<port>/SASEnvironmentManager using administration credentials.
2. Click on the left panel.
3. Select All services from the View drop-down menu.
4. Click Backup service in the left pane.
5. Scroll down until you see sas.deploymentbackup, and click to the right of the service.
6. Change the properties as necessary or keep the defaults. However, you must change the sharedVault property as there is no default value.
7. Click Save.

Configure the Backup

After the software installation is complete, you must perform the following steps:

1. Set the sharedVault location to a network accessible location. This directory must have Read and Write permission to for the install user (sas). See Modify the Backup Configuration Using the Environment Manager to modify the sharedVault property.
2. Determine a schedule for the backup.
3. Backups can be scheduled using the scheduling service. Determine the frequency and type of the backup to be scheduled. See Schedule a Backup to create backup schedules as per your requirement.

Note: The local vault location is /opt/sas/viya/config/backup. The local vault location is located on machines that have SAS Configuration Server, the SAS Cloud Analytic Services (controller node), SAS
Set an appropriate retention period.

Set the `retentionPeriod` value such that you always have at least the last three to four backups at any point in time. For example, if you are doing daily backups, the recommended `retentionPeriod` is 4 days. If you are doing weekly backups, the recommended `retentionPeriod` is 30 days. See Modify the Backup Configuration Using the Environment Manager to set the `retentionPeriod`.

Check the groups for the users who are running SAS Viya services and CAS controllers. The backup service uses a ‘sas’ user to backup and restore data sources from the respective tiers that are included in the backup. For CAS backup, if you are using a different user who is not part of the ‘sas’ group, then you need to change some settings before running backup and restore. For more information, see Backup CAS Access Controls and Caslib Information.

For example, if you have another user named ‘cas’ in the ‘cas’ group, make that ‘cas’ user a member of the ‘sas’ user group. Also make the ‘sas’ user a member of ‘cas’ user group. The following commands are examples of how to make users members of groups:

```bash
sudo usermod -a -G sas cas
sudo usermod -a -G cas sas
```

After running the commands, restart the following two services:

```bash
sudo /etc/init.d/sas-viya-backup-agent-default restart
sudo /etc/init.d/sas-viya-cascontroller-default restart
```

Note: During SAS Viya installation, the ‘sas’ user is created along with ‘sas’ group.

Make sure that the users running the cas process and sas services have the appropriate memberships. For more information see Backup Configuration Information.

---

### Backup: How the Process Works

#### Single-Tenant Deployment

1. You invoke the `/backups/jobs` REST API with request of type `application/vnd.sas.backup.request+json`. A job is created in the global history file (backuphistory.json). The REST API then discovers the data sources that are to be backed up and creates a backup job with tasks for each of the data sources discovered. The sources are discovered using Consul Service Catalog and CAS Management Service.

2. A backup job is created. This object has a field ‘ID’, which is a unique identifier for the job and can be used to track the status of the backup using the rest endpoints. The service should be polled until the job status is either completed, failed, or completedWithWarning. The backup operation runs in the background.

3. Once the backup is complete, the backup files are stored locally on host where the data source resides. The data is stored inside a folder with a timestamp-based backupName (for example, 2016-08-04T05_29_55_910-0400), tenant ID (‘default’ in the case of a single-tenant deployment), and data source name (for example, 2016-08-04T05_29_55_910-0400\default\consul\xxxx.dmp).

4. After the backup operation is complete, the status of the backup operation is updated to the history file (backuphistory_default.json).

5. The backup service then finds the location of the shared vault from the configuration and transfers the locally stored backup files, including the history file, to the shared vault. The backups are stored within the folder
named using the backupID. See How Backups are Stored for more details about the sharedVault directory structure.

Note: The shared vault location must be different from local vault location and should always be accessible to the install user of SAS Viya services.

6 After all of the files are transferred from the local vault to the shared vault, the transfer is complete. If backup of any of the data sources fails or the transfer of files fails, the entire backup is considered to have failed.

7 Once the transfer is complete, the status of the backup job is updated in the backuphistory.json file, and the backup data from the local vault is deleted.

Multi-Tenant Deployment

1 You invoke the /backups/jobs REST API with request of type application/vnd.sas.backup.deployment.request+json. (Optional) You can specify the list of tenants to be backed up. If the tenant list is provided in the backup request, then the backup service validates if each of the tenants received in the request are onboarded. However, if the tenant list is not provided in the backup request, the backup services retrieves all of the onboarded tenants in the system. Once the list of tenants are determined, the backup service creates a job in the global history file (backuphistory.json) and invokes the /backups/jobs REST API with request application/vnd.sas.backup.request for each tenant in the determined list with a common backupID.

Note: A binary type of backup includes all of the onboarded tenants by default. The list of tenants to be backed up is not accepted by the backup service in a binary type of backup.

2 For each tenant, the backup service discovers the data sources that are to be backed up. The backup service creates a backup job with tasks for each of the data sources discovered. The sources are discovered using Consul Service Catalog and CAS Management Service.

3 A backup job is created. This object has the backupID, which was generated during the deployment backup operation. The backupID can be used to track the status of the backup using the rest endpoints. The service should be polled until the job status is either completed, failed, or completedWithWarning. The backup operation runs in the background.

4 Once the backup is complete, the backup files are stored locally on the host where the data source resides. The data is stored inside a folder with a timestamp-based backupName (for example, 2016-08-04T05_29_55_910-0400) and data source name (for example, 2016-08-04T05_29_55_910-0400/acme/consul/xxxx.dmp).

5 After the backup operation is complete, the status of the backup operation is updated to the tenant history file (backuphistory_<tenantId>.json).

6 The backup service then finds the location of the shared vault from the configuration and transfers the locally stored backup files, including the tenant history file, to the shared vault. The backups are stored within the folder named using the backupID. See How Backups are Stored for more details about the sharedVault directory structure.

Note: The shared vault location must be different from local vault location and should always be accessible to the install user of SAS Viya services.

7 After all of the files are transferred from the local vault to the shared vault, the transfer is complete. If backup of any of the data sources fails or the transfer of files fails, the entire backup is considered to have failed.

8 Once the backup operation is complete, an event is triggered. The backup service listens to this event and updates the status of the backup operation for that tenant in the global history file (backuphistory.json).

9 When the backup operation completion event is received for all the tenants, the deployment job status is updated. If the backup of all tenants is successful, the deployment backup job is marked complete. If at least
one tenant backup fails, the deployment backup job is marked completedWithWarning. If all the tenant backups fail, the deployment backup job is marked as failed.

**Backups: How They Are Stored**

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

In the diagram above, the path `/u/sinabc/shareVault/All_backups` is the path to the shared vault. This directory contains the folders for the backups taken. The 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 single-tenant environment, there is only one folder named `__default__`. In a multi-tenant environment, a folder named `tenantId` is available. Within each tenant folder, there are folders for each of the data sources to which the tenant has access. Within each data source folder, you can find the backup files for that data source.

Within the shared vault, there are also folders named `History` and `HistoryArchive`. The History folder stores the history files, which includes the global history file (backuphistory.json) and tenant history files (backuphistory_<tenantId>.json). The History archive folder contains the backup of the History folder taken after each successful backup or restore operation.

**Backup and Restore: Purging**

The Backup service retains backups for a period of time that is set by an administrator. The default value for `retentionPeriod` is 30 days. The `retentionPeriod` can be modified through the Backup Configuration using SAS Environment Manager.

The Backup service retains the last successful backup of each type regardless of `retentionPeriod`. If a binary and default type backup is taken for particular deployment, then the last successful backup for type ‘default ’ and the last successful backup for type ‘binary’ is retained. In a multi-tenant deployment, if a backup was explicitly taken by a tenant after a successful deployment backup (default or binary), those backups are also retained.

Old backups are purged after the retention period and are deleted from the file system. Previous backups for onboarded tenants are purged in the next purge cycle if the backup has passed the retention period. You should
not manually delete the data from the shared vault for an offboarded tenant. The restore from this backup would fail because the backup data is not present. In the case of a multi-tenant environment, purging of the backups happens only for tenants with the state “ONBOARDED”.

Note: Purging is not performed by the Backup Service for backups of offboarded tenants.

---

### Restore: Perform a Restore

#### Overview

The restore operation automatically restores content and configuration information to the SAS Configuration Server, the SAS Message Broker, and the SAS Infrastructure Data Server. However, you cannot use the backup service to automatically restore the CAS configuration and to restore the SAS Infrastructure Data server if it is unresponsive. For instructions about manually restoring CAS configurations, see [Restore CAS Server Access Controls and Caslib Information](#). For instructions about how to restore an unresponsive SAS Infrastructure Data server, see [Restore an Unresponsive SAS Infrastructure Data Server](#) on page 17.

The Backup and Restore service has the following caveats:

- **Cannot be used to restore a CAS configuration.** You must do this manually. See [Restore CAS Server Access Controls and Caslib Information](#).
- **Cannot resolve a problem where the SAS Infrastructure Data server cannot start by redeploying PostgreSQL and then attempting to restore from a backup to that new deployment.**
- **Cannot perform a restore if the SAS Infrastructure Data Server does not start due to PostgreSQL corruption or for any other reason.**
  - If the SAS Infrastructure Data Server does not start and you have configured the SAS Infrastructure Data Server for HA, you must first promote a standby server to primary status before performing a restore with the Backup and Restore service. For more information, see [Restore an Unresponsive SAS Infrastructure Data Server](#).
  - If you have not configured the SAS Infrastructure Data Server for HA, SAS recommends that you perform the steps provided in the section [Best Practices for Postgres on a Single-node When the SAS Infrastructure Data Server is Not Configured for HA](#). Then use the binary backup in addition to the Backup and Recovery service.

#### Prerequisites

To perform a restore, the SAS Infrastructure Data Server must be running and responding to the requests. If you have not configured the SAS Infrastructure Data Server for HA and the server becomes unresponsive and cannot be started because of corruption or for any other reason, you must first use the binary backup utility to restore. For more information, see [Best Practices for Postgres on a Single-node When the SAS Infrastructure Data Server is Not Configured for HA](#).

#### How the Restore Process Works

**Tenant in a Multi-Tenant Deployment and Single-Tenant Deployment**

For a tenant in a multi-tenant deployment or restoring a single-tenant deployment, follow these steps:

Note: Only in the case of a single-tenant deployment when restoring using the binary backup, ensure that you restore the SAS Infrastructure Data server manually. For more information, see [Restore an Unresponsive SAS...](#)
Intrastructure Data Server. If no other data sources are included in the binary backup, start the restore using backup service after manual restore of SAS Infrastructure Data server to restore those data sources.

1 Before starting the restore, you need to check whether the shared vault location is pointing to the location where the backup resides.

2 During the restore, the following services must be running:

   sas-viya-consul-default
   sas-viya-vault-default
   sas-viya-sasdatasvrc-postgres-node0-ct-pg_hba
   sas-viya-sasdatasvrc-postgres-node0-ct-postgresql
   sas-viya-sasdatasvrc-postgres-pgpool0-ct-pcp
   sas-viya-sasdatasvrc-postgres-pgpool0-ct-pgpool
   sas-viya-sasdatasvrc-postgres-pgpool0-ct-pool_hba
   sas-viya-sasdatasvrc-postgres-node0
   sas-viya-cascontroller-default
   sas-viya-httpproxy-default
   sas-viya-rabbitmq-server-default
   sas-viya-sasdatasvrc-postgres
   sas-viya-authorization-default
   sas-viya-cachelocator-default
   sas-viya-configuration-default
   sas-viya-identities-default
   sas-viya-saslogon-default
   sas-viya-cas-management-default
   sas-viya-tenant-default (only in the case of a multi-tenant deployment)
   sas-viya-deploymentBackup-default
   sas-viya-backup-agent-default

   Note: The backup-agent service must be running on all the data sources that need to be restored.

   Stop all SAS services except those mentioned above, and ensure that the processes have been stopped before initiating a restore. Manually stop any SAS processes that are still running. For more information, see “General Servers and Services: Operate” in SAS Viya Administration: General Servers and Services.

3 While initiating the restore, invoke the /restores/jobs endpoint along with the name of the backup (value in the backupName field) in the restore request of type ‘application/vnd.sas.restore.request’. The backup service receives the request and creates a job in the global history file.

4 When a restore is initiated, the backup service performs the pre-restore validations. For more information about the pre-restore validations, see Backup and Restore Terms in the “Backup and Restore: Terms and Concepts” section.

   If all the checks pass the test, the restore is initiated.

5 The backup service sends a message to each of the data sources to download the backup files from the shared vault to local vault for the restore.

6 Once files are downloaded to the local vault, the restore is started.

7 Once the restore is completed, all of the data sources send the message of completion back to backup service.

8 The backup service then updates the status of the restore job depending on the status of the restore of data sources.

9 Once the restore has successfully completed, stop all SAS services and ensure that the processes have been stopped. Manually stop any SAS processes that are still running.
For more information, see “General Servers and Services: Operate” in SAS Viya Administration: General Servers and Services.

10 Restore the CAS server manually. For more information, see Restore CAS Server Access Controls and Caslib Information.

11 Restart all services.

   For more information, see “General Servers and Services: Operate” in SAS Viya Administration: General Servers and Services.

Note: When restoring a tenant in a multi-tenant deployment, the steps are the same. However, the SAS services mentioned in step two should not be stopped and no service is required to be restarted once the restore is completed. When a tenant is being restored, only the configuration for that tenant is restored and Postgres is restored only if the backup type is default. The CAS server should be restored manually only for the tenant being restored.

Multi-Tenant Deployment by Provider Administrator

In the case of a multi-tenant deployment by a Provider administrator where all tenants or selected tenants are backed up:

Note: When restoring using the binary backup, ensure that you restore the SAS Infrastructure Data server manually. For more information see Restore Unresponsive SAS Infrastructure Data Server. If there are other data sources included in the binary backup, start the restore using the backup service after manual restore of SAS Infrastructure Data server to restore those data sources.

1 Before starting the restore, ensure that the shared vault location is pointing to the location where the backup resides.

2 During the restore, the following services must be running:

   sas-viya-consul-default
   sas-viya-vault-default
   sas-viya-sasdatasvrc-postgres-node0-ct-pg_hba
   sas-viya-sasdatasvrc-postgres-node0-ct-postgresql
   sas-viya-sasdatasvrc-postgres-pgpool0-ct-pcp
   sas-viya-sasdatasvrc-postgres-pgpool0-ct-pgpool
   sas-viya-sasdatasvrc-postgres-pgpool0-ct-pool_hba
   sas-viya-sasdatasvrc-postgres-node0
   sas-viya-cascontroller-default
   sas-viya-cascontroller-vault-default
   sas-viya-httproxy-default
   sas-viya-rabbitmq-server-default
   sas-viya-sasdatasvrc-postgres
   sas-viya-authorization-default
   sas-viya-cachelocator-default
   sas-viya-configuration-default
   sas-viya-identities-default
   sas-viya-saslogon-default
   sas-viya-cas-management-default
   sas-viya-tenant-default
   sas-viya-deploymentBackup-default
   sas-viya-backup-agent-default

   Note: The backup-agent service must be running on all the data sources that need to be restored.

   Stop all SAS services except those mentioned above, and ensure that the processes have been stopped before initiating a restore. Manually stop any SAS processes that are still running. For more information, see “General Servers and Services: Operate” in SAS Viya Administration: General Servers and Services.
Invoke `/restores/jobs` with the backupName to be used for the restore in the request of type 'application/vnd.sas.restore.deployment.request+json'.

(Optional) Specify the list of tenants to be restored, and those tenants should be part of specified backup.

The restore request accepts the list of tenants to be restored. If this list is not provided, the backup service creates this list with the tenants that are onboarded along with the Provided Administrator. If any of the tenants on the list are not present in the specified backup, then the restore operation does not proceed and is marked as failed. However, if all the tenants on the list are present in the specified backup, then the restore job is created in the global history file. The `/restores/jobs` API is invoked for each requested tenant with the request 'application/vnd.sas.restore.request+json'.

The backup service receives the restore request and pre-restore validations and checks to see whether the provided backupName is valid. For more information about the pre-restore validations, see `Backup and Restore Terms` in the “Backup and Restore: Terms and Concepts” section.

If the backupName is valid, the backup service retrieves the data sources from the backup and initiates the restore tasks for each of the data sources and sends it to the backup agent.

The backup agent performs the restore and sends the appropriate result back to the backup service.

The backup service consolidates the results of the restore for all the data sources and marks the restore job for that tenant appropriately. The backup service sends an event about the restore status for this tenant.

When the service receives the responses for each of the tenants, it marks the status of the restore job in the global history file. If all tenants send a success event, the job is marked completed. If any tenant restore is unsuccessful, the job is marked as failed.

Once the restore has completed successfully, stop all SAS services and ensure that the processes have been stopped. Manually stop any SAS processes that are still running.

For more information, see “General Servers and Services: Operate” in SAS Viya Administration: General Servers and Services.

Manually restore the CAS server for each tenant. For more information, see `Restore CAS Server Access Controls and Caslib Information`.

Restart all services.

For more information, see “General Servers and Services: Operate” in SAS Viya Administration: General Servers and Services.

---

**Restore an Unresponsive SAS Infrastructure Data Server**

If you have not configured the data server for HA, and the data server does not start because of PostgreSQL corruption or for any other reason, perform the following steps:

1. Stop all services including the database service.
   ```
   sudo /etc/init.d/sas-viya-all-services stop
   ```

2. Archive or rename the existing node0 directory.
   ```
   cd /opt/sas/viya/config/data/sasdatasvrc/postgres
   mv node0 node0_original
   ```

3. Create a node0 directory with permissions and ownership similar to the old node0 directory.
   ```
   mkdir node0
   chmod 700 node0
   cd node0
   ```
Extract the contents of the base.tar.gz file into the node0 directory.

- In a multi-tenant environment:
  ```bash
tar -xvf ../sharedVault/<backup-Id>/provider/postgres/base.tar.gz
  ```

- In a single-tenant environment:
  ```bash
tar -xvf ../sharedVault/<backup-Id>/__default__/postgres/base.tar.gz
  ```

Once the files are extracted, delete the base.tar.gz file from the node0 directory.

Ensure that the `hot_standby` property is set to `off` in the postgresql.conf file. The postgresql.conf file can be found in the `/opt/sas/viya/config/data/sasdatasvrc/postgres/node0` directory.

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

Remove the recovery.conf and recovery.done files located at `/opt/sas/viya/config/data/sasdatasvrc/postgres/node0`.

Start the Consul service and then start the database service.

```
sudo /etc/init.d/sas-viya-vault-default start
sudo /etc/init.d/sas-viya-sasdatasvrc-postgres start
```

Make sure that the database service started successfully without any issues.

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

Verify that the primary data server has started without any issues and has a status of “up”. Here is an example:

```
sudo /etc/init.d/sas-viya-sasdatasvrc-postgres status
Checking status of sas-viya-sasdatasvrc-postgres...
PGPool is running with PID=4733
```

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

(1 row)

Set the `hot_standby` property in the psql.conf file back to `on`.

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

Restart all services.
Backup and Restore for Programming-Only Deployments

How To

Back up CAS Access Controls and Caslib Information

**CAUTION!** It is strongly recommended that you back up each CAS server’s stored access control and caslib information after adding global-scope caslibs or setting access controls. Backups are particularly important after you modify access controls or add, delete, or modify global caslibs.

You can perform a backup programmatically by using the createBackup and completeBackup actions.

**Note:** You need to be an administrator to perform a backup.

1. To perform the backup, run the following code in SAS Studio replacing the `path` location to your location:

   ```sas
   cas casauto host="cloud.example.com" port=5570;
   
   proc cas;
   accessControl.assumeRole / adminRole="SuperUser";
   accessControl.createBackup / path="/my/backup/location";
   accessControl.completeBackup;
   accessControl.dropRole / adminRole="SuperUser";
   quit;
   
   2. Copy the backup location directory to a location where it can be saved. The cas user needs Write access to the location provided. If the location does not exist and the cas user has Write access, 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 named for the fully qualified DNS name of the machine that runs the main controller. The cas user must have Read and Write access to both the `permstore` and `backup` directories. For more information about permstore, see Configuration File Options Reference in the “SAS Cloud Analytic Services: Reference” section of the SAS Viya Administration: SAS Cloud Analytic Services.

Back up Configuration Information

Here are the located hosts that have been listed in the [sas-casserver-primary] host group in the inventory file:

```
machine:

/opt/sas/viya/config/etc/cas/default/casconfig.lua
/opt/sas/viya/config/etc/cas/default/cas.hosts
```

Here are the located hosts that have been listed in the [programming] host group in the inventory file:

```
_machine:

/opt/sas/viya/config/etc/sasstudio/default/init_usermods.properties
/opt/sas/viya/config/etc/sasstudio/default/appserver_usermods.sh
/opt/sas/viya/config/etc/spawner/default/spawner_usermods.sh
/opt/sas/viya/config/etc/workspaceserver/default/autoexec_usermods.sas
/opt/sas/viya/config/etc/workspaceserver/default/sasv9_usermods.cfg
/opt/sas/viya/config/etc/workspaceserver/default/workspaceserver_usermods.sh
```
If your site has created global folder shortcuts for SAS Studio, you should back up the directory that contains the shortcuts. By default, the shortcuts are stored in the following directory:

/opt/sas/viya/home/SASFoundation/GlobalStudioSettings

Note: Your site might have configured a different directory for the shortcuts. For details, see Configuring Global Folder Shortcuts in the Configuration Properties: How to Configure SAS Studio topic in the SAS Viya Administration: Configuration Properties.

### Restore CAS Server Access Controls and Caslib Information


2. The permstore directory and its contents at /opt/sas/viya/config/etc/cas/default should be replaced with the permstore directory that is located in the sharedVault that you specified when configuring your backup. The permstore directory is under the <backupId>/cas-shared-default folder. The cas user needs Read and Write access to the permstore directory.

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


### Restore the Most Recent Permstore in the Event of a Failover

If no global-scope caslibs were added or changes to access controls were made after the failover, then you can restore from a backup as described in Restore CAS Server Access Controls and Caslib Information

If changes were made or you are unsure, then perform the following steps to restore the latest permstore from the backup controller.

**CAUTION!** The backup controller removes its permission store at start-up in order to begin in a synchronized state with the primary controller. It is vital that you preserve the permstore from the backup controller before restarting the server in order to have access to the most up-to-date permission store.


2. Find the location of the primary controller's permission store. The default location is: /opt/sas/viya/config/etc/cas/default/permstore/<fully-qualified-domain-name>.

3. Remove the contents of the directory.

4. On the backup controller host, find the location of the backup controller's permission store. The default location is: /opt/sas/viya/config/etc/cas/default/permstore/<fully-qualified-domain-name>.

5. On the backup controller host, make a copy of the permstore. Make sure that you preserve the file ownership and permissions. One way to do this is with the tar command.

   ```bash
   sudo tar cf /root/backup_controller_permstore.tar
   ```

6. Copy the archive to the host for the primary controller.

7. On the primary controller host, change directory to the location of the now empty permstore.

   ```bash
   sudo tar xf /path/to/backup_controller_permstore.tar
   ```
8 Start the server.

- If the primary controller host is stopped, then boot the machine. When the machine starts, the server is automatically started.
- If the primary controller host is running, then start the server with the following command:
  
  `sudo /etc/init.d/sas-viya-cascontroller-default start`

For more information about stopping and starting CAS see Operate in the SAS Cloud Analytics Services: How To (Scripts) topic.

---

### Backup and Restore: Backup Manager

#### What Is the Backup Manager

The Backup Manager is a graphical interface in which you can manage the backup and restore processes for your systems. The SAS Backup Manager is available as a plug-in within the SAS Environment Manager. You can use the SAS Backup Manager for the following tasks:

- viewing the backup and restore history
- viewing details about backup and restore
- viewing the backup configuration
- running an immediate (ad hoc) backup
- restoring a backup

To view the SAS Backup Manager from the Environment Manager:

1. Log on to the SAS Environment Manager.
2. In the left menu panel, click [ ]

#### First Look at the Backup Manager

The Backup Manager provides a way to back up and restore your system using a graphical interface. The features of the SAS Backup Manager window are as follows:
1. The toolbar enables you to view backup or restore details, perform an ad hoc backup or restore, and view the backup configuration.

2. The backup and restore history view displays all of the completed backups or restores. Highlighting a row displays details about that backup or restore.

3. The backup and restore details view enables you to view operational and data source details about the backup or restore in the Operation Details pane.

### View Backup and Restore History

To view a list of backups or restores that are complete, are currently running, or are waiting to run:

- From the View drop-down list on the toolbar, select Backup details or Restore details.

The list includes all backups or restores recorded in the backup history. This includes backups that have been purged due to the retention policy. It also includes backups or restores currently running or that are waiting to run. By default, they are listed in descending order by Start Time. The following information is listed in each table:

- **Backup Name or Restore ID**
  - the unique identifier of the backup or restore, based on the date and time that the backup or restore started (for example, 2017-10-28T05_33_47_326-0400).

- **User ID**
  - the user ID of the user that ran the backup or restore or the identity name of the service that initiated the backup or restore.

- **Type**
  - the type of backup – Binary or Default.

- **Size**
  - the total size of the files that were backed up (not available for a provider in a multi-tenant environment).
  - This column is not displayed when you select Restore details.

- **Start Time**
  - the date and time that the backup or restore started running.

- **End Time**
  - the date and time that the backup or restore stopped running.
Status contains one of the following icons, indicating the status of the backup or restore operation:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🚮</td>
<td>The backup or restore has not yet started.</td>
</tr>
<tr>
<td>🍀</td>
<td>The backup or restore is currently running (in progress).</td>
</tr>
<tr>
<td>✔</td>
<td>The backup or restore completed without errors or warnings.</td>
</tr>
<tr>
<td>🚩</td>
<td>The backup or restore completed with warnings.</td>
</tr>
<tr>
<td>❌</td>
<td>The backup or restore completed with errors.</td>
</tr>
<tr>
<td>✗</td>
<td>The backup was purged.</td>
</tr>
<tr>
<td>⚫</td>
<td>The status of the backup or restore cannot be determined.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Backup Name</th>
<th>User ID</th>
<th>Type</th>
<th>Size</th>
<th>Start Time</th>
<th>End Time</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-11-15T08_07_03_322-0500</td>
<td>seaboot</td>
<td>Default</td>
<td>204.0 MB</td>
<td>Nov 15, 2017, 8:07:03 AM</td>
<td>Nov 15, 2017, 8:08:07 AM</td>
<td>✔</td>
</tr>
</tbody>
</table>

**TIP** You can refresh your browser to see the latest status.

To use CLI commands to view the backup and restore history, see Backup and Restore: Command Line Interface on page 29

**View Backup or Restore Details in a Single-tenant Setup or Tenant in a Multi-tenant Setup**

**View Backup or Restore Operation Details**

To view details for a particular backup or restore operation, click in the right pane. A panel slides out that displays all of the details for that operation. The following details are displayed:

- Backup Name or Restore ID.
- Status of the backup or restore job.
- Total size of the files that were backed up. This information does not appear for restores.
- Any comments that were specified when the backup or restore was run.
- User ID of the user that ran the backup or restore or the identity name of the service that initiated the backup or restore.
- Start and end date and time for the backup or restore.

**Operation Details**

Backup name: 2017-11-01T02_49_41_450-0400  
Status: completed  
Size: 204.0 MB  
Comments: NewBkpDefault  
User ID: sasv  
Start time: 1 Nov 2017, 12:19:42  
End time: 1 Nov 2017, 12:20:44

**View Backup or Restore Data Sources**

**View the List of Data Sources**

The data sources for the currently selected backup or restore are listed in the right pane. To view the list of data sources, click . If you are viewing details for a restore, only the data sources that were restored are listed.

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

For more information about the data sources, see About the Backup and Restore Service .
**View Details about a Data Source**

To view details about a particular backup or restore data source, click ▶ to the left of the source name. The following details are displayed:

- the status of the data source’s backup or restore.
- the total size of the backup files for this data source. This information does not appear for restores.

To collapse the data source so that the details are not displayed, click ▼ to the left of the data source name.

![Datasources](image)

**View Backup or Restore Details for a Provider in a Multi-tenant Setup**

To view details for a particular backup or restore operation, select the operation by double-clicking any of its columns or right-clicking and selecting **Tenants** from the pop-up menu. A listing of the tenants that were backed up or restored is displayed. The following details appear for each tenant:

- the tenant name.
- the start and end date and time for the backup or restore for the tenant.
- the status of the backup or restore for the tenant.
View the Backup Configuration

To view the current backup configuration, click **Backup Configuration**. The Backup Configuration dialog box displays the following information:

- **Retention period**—number of days that backups are stored before they are removed from the shared vault.
- **Shared vault**—location where all backups are stored. SAS user must have created the shared vault directory.

For more information see **Configuring the Backup**

Run an Unscheduled Backup

To start an immediate backup:

1. Log on to the SAS Environment Manager.
2. In the left menu panel, click **Backup**.
3. Click **Backup** in the upper right corner of the Backup and Restore window.
4. In the Backup dialog box, enter the following:
   - **Comments**—optional free-form comment describing the backup. The comment is recorded in backup history and is displayed in the backup’s **Operation Details**.
   - **Backup type**—select a backup type. There are two types of backups:
     - Default
     - Binary
     For more information about the backup types, see **Backup and Restore Terms**.
     The **Default** type is selected by default.
For the **Binary** type, select the **Include all sources** check box, if other sources also need to be backed up.

**Backup**

- Comments:

- Backup type:
  - Binary
    - Include all sources
  - Default

- **Tenants**—If the user is a provider in a multi-tenant setup, the user can select the tenants to be backed up from the onboarded tenant list.

**Backup**

- Comments:

- Backup type:
  - Binary
    - Include all sources
  - Default

- **Tenants**

  - provider
  - acme
  - cyberyne

**Note:** A binary backup includes all of the onboarded tenants by default.

If the user is an intra-tenant administrator in a multi-tenant environment or an administrator in a single-tenant environment, the tenant list is not displayed.

For an intra-tenant administrator, the backup type is not displayed since the intra-tenant administrator is allowed to perform only a default backup.

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

A new row is added in the table with the status running.
The page refreshes until the backup process is complete. After the process is complete, a message is displayed letting you know whether the backup was completed, completed with warnings, or failed.

Note: To see the status of the backup on the main page, refresh your browser.

**Restore a Backup**

1. Select **Backup details** from the **Views** drop-down list.
2. Select the backup to be restored.
   - If the backup type is **Binary**, ensure that you restore the **SAS Infrastructure Data Server** before initiating the restore using the user interface
     - In the case of a multi-tenant environment where the Provider Administrator is initiating the restore operation, the status of the backup must either be Completed (✓) or Completed with Warnings (✗). If the backup has a status of ‘Completed with Warnings’, the Provider Administrator needs to select those tenants only with a status of Completed from specified backup and initiate restore operation.
     - In the case of a multi-tenant environment, if the intra-tenant Administrator is initiating a restore operation, the status of the backup must be Completed.
     - In the case of a single-tenant environment, the backup status must be Completed before a restore operation can be initiated.
   - If a Binary backup had other sources included, only those sources can be restored using the user interface. The SAS Cloud Analytic Services must be manually restored. For more information, see **Restore CAS Server Access Controls and Caslib Information** on page 20.
3. The **Restore** dialog box displays the selected Backup name.
4. The following details can be entered in the **Restore** dialog box:
   - **Comments**—optional free-form comment describing the backup. The comment is recorded in restore history and is 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.

**Restore**

Backup ID:
2017-11-15T08_07_03_322-0500
Comments:

☐ Force restore if some databases don’t match

- **Tenants**—if the user is a provider in a multi-tenant setup, the user can select the tenants to be restored from the tenant list. The tenant list displays the onboarded tenants present in the specified backup whose backups are "completed" or "completedWithWarnings".
5 Click **Restore** to start the restore process. The UI displays a message **Restore In Progress**.

It is recommended not to use the UI while a restore is in progress. As the datasources are being refreshed, the UI might not display all results.

6 After the process is complete, a message is displayed letting you know whether the restore was completed, completed with warnings, or failed.

   For any failed backup or restore operation, the Provider Administrator can check the logs at `/opt/sas/viya/config/var/log/deploymentBackup/default` and `/opt/sas/viya/config/var/log/backup-agent/default`. If a failure occurs in any operation initiated by an intra-tenant Administrator, the administrator should contact the Provider Administrator to get a reason for the failure.

7 To view the restore, select **Restore details** in the **Views** drop-down list. The latest restore operation is now the first row in the table.

---

**Backup and Restore: Command-Line Interface**

**Overview**

The Backup microservice has two command-line interface (CLI) utilities that are available in SAS Viya. These CLIs are developed using the SAS Viya CLI framework and can be used as independent utilities or as plug-ins to the sas-admin CLI. For details about the CLI framework, see the SAS CLI Framework documentation. For more information about CLI, see **Overview of the Command-Line Interface**

**Note:** The CLI does not support tenant-specific backup or restore operations.

The following sections show how to use these CLIs to perform backup and restore operations.

**SAS Admin CLI**

The CLI commands are located at `/opt/sas/viya/home/bin`. Navigate to that directory and initialize the profile and authenticate against the host.
Create a profile: Specify the URL of the host where the backup service is hosted. Also, specify an output type.

Command: sas-admin --profile "hostname.mycompany.com" profile init
Enter configuration options:

Service Endpoint> http://hostname.mycompany.com

Output type (text|json|fulljson)> text

Enable ANSI colored output (y/n)>> y
Saved 'hostname.mycompany.com' profile to

Authenticate: Specify user name and password.

Command: sas-admin --profile "hostname.mycompany.com" auth login
Enter credentials for http://hostname.mycompany.com:
Userid>> sasboot
Password>>
Login succeeded. Token saved

On a multi-tenant setup, the provider credentials should be provided for deployment level environment operations.

On a multi-tenant setup, tenant credentials should be provided for a tenant level environment operation.

On a single-tenant system, the administrator credentials should be provided.

Once the profile is created and the user is authenticated, that user can use other commands.

Set a default profile: sets "hostname.mycompany.com" as default profile.

Command export SAS_CLI_PROFILE="hostname.mycompany.com"

SAS Backup CLI

Overview

There are three backup CLI commands specific to the backup service:

- start
- list
- show

There are many other commands, which come with the CLI framework, and those can also be used as required. For example, the -help command can be used with any plug-in or command to get related help.

Command: -help

Example:

sas-admin backup -help

Output:

NAME:
sas-backup - SAS Backup Command Line Interface

USAGE:
sas-admin backup command [command options] [arguments...]
VERSION:
1.2.3

COMMANDS:
authenticate, auth, authn    Handle authentication process
help, h                      Show a list of commands or help for one command
list                         Lists backups
show                         Shows backup details
start                        Start backup

Backup CLI Commands

Start Backup Help

Show backup CLI start command help:

start

Example:
sas-admin backup start -help

Output:

NAME:
sas-admin backup start

USAGE:
sas-admin backup start [command options] [arguments...]

OPTIONS:
--backup-type, -t "default"  Specifies the type of backup to be taken.
The default value is: "default". The valid values for the
"backup-type" option are as follows: "default", "binary"

--comments, -c "default comment"  Specifies free text comments that are associated with this
backup operation. The default value is: "default comment"

--configuration-id, -n "default"  Specifies the ID of a backup configuration to be used for
a backup operation. Only the default configuration
is supported. The default value is: "default"

--include-all-sources-for-binary-backup, -i  Specifies whether to include other sources in the backup when
the "backup-type" option is specified as "binary". If the
"true" value is specified, then all sources are included.
The default value is: "false"

--slug, -s "default slug"  Specifies the name that is given to a backup operation.
The default value is as follows: "default slug"

--version, -v "1"  Specifies the version of the media type.
The default value is 1.

Start Backup

Command:

start

Example:
sas-admin backup start --comments="default comments" --configuration-id="default"
                         --slug="default slug" --version=1

Output for a multi-tenant system:

Start Deployment backup
Output for a single-tenant system or when the backup is initiated by an intra-tenant administrator on a multi-tenant system:

```
sas-backup-cli start
```

To start a default backup with comment:

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

OR

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

To start a binary backup to include only the Postgres data source, with a comment:

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

OR

```
sas-admin backup start --backup-type=binary -c="sample --includeAllSourcesForBinaryBackup=false
```

To start a binary backup to include all other sources in addition to the Postgres data source, with a comment:

```
sas-admin backup start --backup-type=binary
--includeAllSourcesForBinaryBackup=true -c="sample comment"
```

On a multi-tenant system when the provider is logged in, this command takes a backup of all on boarded tenants.

On a multi-tenant system when the intra-tenant administrator is logged in, this command takes a backup of that tenant.

On a single-tenant system, this command takes a backup of that system.

Get Backup List Help

Command:

```
list --help
```

Output:

```
NAME:
sas-admin backup list - Lists backups.

USAGE:
```
sas-admin backup list [command options] [arguments...]

OPTIONS:
--limit, -l "10"  Specifies the maximum number of backup jobs to return. The default value is 10.
--start, -s "0"    Specifies the 0-based offset of the first backup to return. The default value is 0 for the first one.

Show Backup List

Example:
sas-admin backup list

Output for a multi-tenant system. This is a sample and not all output columns are represented.

<table>
<thead>
<tr>
<th>BackupId</th>
<th>Version</th>
<th>BackupType</th>
<th>State</th>
<th>Owner</th>
<th>StartTimeStamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-10-28T05_56_24_380-0400</td>
<td>1</td>
<td>default</td>
<td>running</td>
<td>sasboot</td>
<td>2017-10-28T09:56:24.385Z</td>
</tr>
<tr>
<td>2017-10-28T05_47_56_781-0400</td>
<td>1</td>
<td>default</td>
<td>completedWithWarning</td>
<td>sasboot</td>
<td>2017-10-24T09:31:259Z</td>
</tr>
<tr>
<td>2017-10-24T04_50_51_569-0400</td>
<td>1</td>
<td>default</td>
<td>failed</td>
<td>sasboot</td>
<td>2017-10-24T08:51:575Z</td>
</tr>
<tr>
<td>2017-10-23T06_37_01_017-0400</td>
<td>1</td>
<td>binary</td>
<td>completed</td>
<td>sasboot</td>
<td>2017-10-23T10:37:01:020Z</td>
</tr>
<tr>
<td>2017-10-23T06_30_23_033-0400</td>
<td>1</td>
<td>default</td>
<td>completed</td>
<td>sasboot</td>
<td>2017-10-23T10:30:23:037Z</td>
</tr>
<tr>
<td>2017-10-23T06_09_39_355-0400</td>
<td>1</td>
<td>default</td>
<td>completed</td>
<td>sasboot</td>
<td>2017-10-23T10:09:39:361Z</td>
</tr>
<tr>
<td>2017-10-23T03_40_16_240-0400</td>
<td>1</td>
<td>default</td>
<td>completed</td>
<td>sasboot</td>
<td>2017-10-23T07:40:16:249Z</td>
</tr>
<tr>
<td>2017-10-23T00_53_09_691-0400</td>
<td>1</td>
<td>default</td>
<td>completedWithWarning</td>
<td>sasboot</td>
<td>2017-10-23T04:53:09:697Z</td>
</tr>
<tr>
<td>2017-10-17T09_13_04_082-0400</td>
<td>1</td>
<td>default</td>
<td>completed</td>
<td>sasboot</td>
<td>2017-10-17T13:13:04:087Z</td>
</tr>
</tbody>
</table>

For a single-tenant setup or when initiated by an intra-tenant administrator on a multi-tenant setup. This is a sample and not all output columns are represented.

<table>
<thead>
<tr>
<th>Version</th>
<th>BackupId</th>
<th>BackupType</th>
<th>IncludeAllSourcesForBinaryBackup</th>
<th>Slug</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2017-10-28T11_06_51_561-0400</td>
<td>default</td>
<td>false</td>
<td>default slug</td>
<td>default comment</td>
</tr>
<tr>
<td>1</td>
<td>2017-10-28T09_04_37_140-0400</td>
<td>default</td>
<td>false</td>
<td>new-slug</td>
<td>new backup</td>
</tr>
<tr>
<td>1</td>
<td>2017-10-27T14_38_26_579-0400</td>
<td>default</td>
<td>false</td>
<td>default slug</td>
<td>default comment</td>
</tr>
<tr>
<td>1</td>
<td>2017-10-27T14_29_00_225-0400</td>
<td>default</td>
<td>false</td>
<td>default slug</td>
<td>default comment</td>
</tr>
<tr>
<td>1</td>
<td>2017-10-27T13_44_03_524-0400</td>
<td>default</td>
<td>false</td>
<td>default slug</td>
<td>default comment</td>
</tr>
<tr>
<td>1</td>
<td>2017-10-27T13_42_21_700-0400</td>
<td>default</td>
<td>false</td>
<td>default slug</td>
<td>default comment</td>
</tr>
<tr>
<td>1</td>
<td>2017-10-27T13_36_15_236-0400</td>
<td>default</td>
<td>false</td>
<td>default slug</td>
<td>default comment</td>
</tr>
<tr>
<td>1</td>
<td>2017-10-26T02_14_03_814-0400</td>
<td>default</td>
<td>false</td>
<td>default slug</td>
<td>default comment</td>
</tr>
<tr>
<td>1</td>
<td>2017-10-25T07_45_52_386-0400</td>
<td>default</td>
<td>false</td>
<td>default slug</td>
<td>default comment</td>
</tr>
</tbody>
</table>

Show all backups sorted in time order, newest to oldest.

On a multi-tenant system, the provider administrator sees all deployment backups. The intra-tenant administrator sees all available tenant backups for that tenant.

On a single-tenant system, the administrator sees all available backups on that system.

Example: See the most recent 10 records from the backup history:

sas-admin backup list (Uses defaults)

OR

sas-admin backup list -s=0 -l=10

OR

sas-admin backup list --start=0 -- limit=10

Show Backup Details Help

Command:

show -help
Example:

sas-admin backup show -help

Output:

NAME:

sas-admin backup show - Shows backup details.

USAGE:

sas-admin backup show [command options] [arguments...]

OPTIONS:

--id, -i     Specifies the unique ID of the backup operation for which details have been requested.

Show Backup Details

Example:

sas-admin backup show -i=2017-10-28T05_56_24_380-0400

Output for a multi-tenant system. This is a sample and not all output columns are represented.

<table>
<thead>
<tr>
<th>Version</th>
<th>BackupId</th>
<th>BackupType</th>
<th>IncludeAllSourcesForBinaryBackup</th>
<th>Slug</th>
<th>Name</th>
<th>State</th>
<th>Owner</th>
<th>StartTimeStamp</th>
<th>EndTimeStamp</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>default</td>
<td>false</td>
<td></td>
<td></td>
<td>running</td>
<td>sasboot</td>
<td>2017-10-28T09:56:24.385Z</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tenant Backups:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BackupId</td>
<td>Tenant</td>
<td>StartTimeStamp</td>
<td>EndTimeStamp</td>
<td>State</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>--------</td>
<td>----------------</td>
<td>--------------</td>
<td>-------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Output for a single-tenant system or when initiated by an intra-tenant administrator on a multi-tenant system. This is a sample and not all output columns are represented.

show --id=2017-10-28T11_06_51_561-0400

<table>
<thead>
<tr>
<th>Version</th>
<th>BackupId</th>
<th>BackupType</th>
<th>IncludeAllSourcesForBinaryBackup</th>
<th>Slug</th>
<th>Name</th>
<th>State</th>
<th>Size</th>
<th>Owner</th>
<th>StartTimeStamp</th>
<th>EndTimeStamp</th>
<th>Purged</th>
<th>Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>default</td>
<td>false</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>sasin</td>
<td>2017-10-28T11:06:51:561-0400</td>
<td></td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Sources:</td>
<td>SourceId</td>
<td>Name</td>
<td>Address</td>
<td>State</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td>------</td>
<td>--------</td>
<td>-------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>34</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
On a multi-tenant system, the provider sees the administration details of the specified deployment backup. The intra-tenant administrator sees details of the specified tenant backup.

On a single-tenant system, the administrator sees the details of the specified backup on that system.

**SAS Restore CLI**

**Restore CLI Help**

Example:

```bash
sas-admin restore -help
```

**Start Restore Operation Help**

Command:

```bash
start -help
```

Example:

```bash
sas-admin restore start -help
```

Output:

**NAME:**

`sas-admin restore start - Starts a restore operation.

**USAGE:**

`sas-admin restore start [command options] [arguments...]

**OPTIONS:**

`--backup-name, -b` Specifies the unique ID of the backup for which the restore operation is to be executed.

`--comments, -c "comments"` Specifies free text comments that are associated with this restore operation. The default value is as follows: "default comment"

`--force, -f` Specifies whether to perform the restore operation even if the validation checks fail. The default value is false.

`--slug, -s "slug"` Specifies the name that is given to a restore operation. The default value is: "default slug"

`--version, -v "1"` Specifies the version of the media type. The default value is 1.

**Start Restore Operation**

Command:

```bash
start
```

Example:

```bash
sas-admin restore start --backup-name="2017-10-28T07_16_40_223-0400" --comments="" --force=false --slug=" " --version=1
```

Output for a multi-tenant system:

<table>
<thead>
<tr>
<th>Version</th>
<th>JobId</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2017-10-28T07_23_44_594-0400</td>
</tr>
</tbody>
</table>
Output for a single-tenant system or when initiated by an intra-tenant administrator on multi-tenant system:

```
Version 1
JobId 2017-10-28T11_33_24_330-0400
Slug slug
Comments comments
BackupName 2017-10-28T11_06_51_561-0400
BackupType default
IncludeAllSourcesForBinaryBackup false
State running
Owner sasin
EndTimeStamp
```
Show Restore Operations List

Command:

list

Example:

```bash
sas-admin restore list
```

Output in a multi-tenant system. This is a sample and not all output columns are represented.

<table>
<thead>
<tr>
<th>Version</th>
<th>RestoreId</th>
<th>BackupName</th>
<th>BackupType</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2017-10-28T07_23_44_594-0400</td>
<td>2017-10-28T07_16_40_223-0400</td>
<td>default</td>
<td>completed</td>
</tr>
<tr>
<td>1</td>
<td>2017-10-23T11_24_44_602-0400</td>
<td>2017-10-23T06_09_39_355-0400</td>
<td>default</td>
<td>completed</td>
</tr>
<tr>
<td>1</td>
<td>2017-10-23T06_42_51_525-0400</td>
<td>2017-10-23T06_37_01_017-0400</td>
<td>binary</td>
<td>completed</td>
</tr>
<tr>
<td>1</td>
<td>2017-10-23T06_33_11_357-0400</td>
<td>2017-10-23T06_30_23_033-0400</td>
<td>default</td>
<td>completed</td>
</tr>
<tr>
<td>1</td>
<td>2017-10-17T09_17_41_209-0400</td>
<td>2017-10-17T09_13_04_082-0400</td>
<td>default</td>
<td>completed</td>
</tr>
</tbody>
</table>

Output in a single-tenant system or when the backup is initiated by an intra-tenant administrator on multi-tenant system. This is a sample and not all output columns are represented.

<table>
<thead>
<tr>
<th>Version</th>
<th>RestoreId</th>
<th>BackupName</th>
<th>BackupType</th>
<th>Slug</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2017-10-28T11_33_24_330-0400</td>
<td>2017-10-28T11_06_51_561-0400</td>
<td>default</td>
<td>slug</td>
</tr>
<tr>
<td>1</td>
<td>2017-10-28T10_14_09_371-0400</td>
<td>2017-10-28T09_04_37_140-0400</td>
<td>default</td>
<td>new-restore-slug</td>
</tr>
<tr>
<td>1</td>
<td>2017-10-27T03_21_26_623-0400</td>
<td>2017-10-26T02_14_03_814-0400</td>
<td>default</td>
<td>new-restore-slug</td>
</tr>
<tr>
<td>1</td>
<td>2017-10-26T02_19_59_068-0400</td>
<td>2017-10-25T07_45_52_386-0400</td>
<td>default</td>
<td>new-restore-slug</td>
</tr>
<tr>
<td>1</td>
<td>2017-10-26T02_15_38_600-0400</td>
<td>2017-10-26T02_14_03_814-0400</td>
<td>default</td>
<td>new-restore-slug</td>
</tr>
<tr>
<td>1</td>
<td>2017-10-25T07_43_34_590-0400</td>
<td>2017-10-25T07_39_27_192-0400</td>
<td>default</td>
<td>new-restore-slug</td>
</tr>
<tr>
<td>1</td>
<td>2017-10-25T05_35_16_499-0400</td>
<td>2017-10-25T05_28_24_244-0400</td>
<td>default</td>
<td>new-restore-slug</td>
</tr>
<tr>
<td>1</td>
<td>2017-10-25T03_01_25_128-0400</td>
<td>2017-10-25T02_51_31_855-0400</td>
<td>binary</td>
<td>restore</td>
</tr>
<tr>
<td>1</td>
<td>2017-10-24T06_42_56_211-0400</td>
<td>2017-10-16T03_33_38_720-0400</td>
<td>default</td>
<td>slug</td>
</tr>
<tr>
<td>1</td>
<td>2017-10-18T06_05_20_455-0400</td>
<td>2017-10-18T06_03_35_463-0400</td>
<td>binary</td>
<td>new-restore-slug</td>
</tr>
</tbody>
</table>

This list shows all the restores that are available to the logged in user, sorted in time order, newest to oldest.

On a multi-tenant system, the provider administrator sees all deployment restores. The intra-tenant administrator sees all available tenant restores for that tenant.

On a single-tenant system, the administrator sees all available restores on that system.

Show the most recent 10 restores from the restore history:

```bash
sas-admin restore list
```

OR

```bash
sas-admin restore list -s=0 -l=10
```

OR

```bash
sas-admin restore list --start=0 --limit=10
```

Show Restore Job Details Help

Command:

```bash
show --help
```

Example:

```bash
sas-admin restore --help
```

Output:

NAME:
sas-admin restore show - Shows the details of a restore operation.

USAGE:
   sas-admin restore show [command options] [arguments...]

OPTIONS:
   --id, -i       Specifies the unique ID of the restore operation for which details have been requested.

Show Restore Job Details

Command:
   show

Example:
   sas-admin restore show --id=2017-10-28T07_23_44_594-0400

Output for a multi-tenant system:

<table>
<thead>
<tr>
<th>Version</th>
<th>RestoreId</th>
<th>BackupName</th>
<th>BackupType</th>
<th>Slug</th>
<th>Comments</th>
<th>State</th>
<th>Owner</th>
<th>OwnerTenantId</th>
<th>IncludeAllSourcesForBinaryBackup</th>
<th>StartTimeStamp</th>
<th>EndTimeStamp</th>
</tr>
</thead>
</table>

Output for tenant restores. This is a sample and not all output columns are represented.

<table>
<thead>
<tr>
<th>RestoreId</th>
<th>Tenant</th>
<th>StartTimeStamp</th>
<th>EndTimeStamp</th>
<th>State</th>
</tr>
</thead>
</table>

Output for a single-tenant system or when initiated by an intra-tenant administrator on a multi-tenant system.

This is a sample and not all output columns are represented.

<table>
<thead>
<tr>
<th>Version</th>
<th>RestoreId</th>
<th>BackupName</th>
<th>BackupType</th>
<th>Slug</th>
<th>Comments</th>
<th>State</th>
<th>Owner</th>
<th>StartTimeStamp</th>
<th>EndTimeStamp</th>
</tr>
</thead>
</table>

Sources:

<table>
<thead>
<tr>
<th>Version</th>
<th>SourceId</th>
<th>Name</th>
<th>Address</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>rabbitmq</td>
<td>SAS Message Broker</td>
<td>rdcesx14016.race.sas.com</td>
<td>completed</td>
</tr>
<tr>
<td>1</td>
<td>postgres</td>
<td>SAS Infrastructure Data Server</td>
<td>rdcesx14016.race.sas.com</td>
<td>completed</td>
</tr>
</tbody>
</table>
Backup and Restore: Schedule a Backup

Default Scheduling in Backup
The default schedule backup for a default backup is to run every Sunday at 1:00 a.m.. You can see the following log message in the Backup Service log: Default schedule created for BackupService to run backup job every Sunday 1AM.

For scheduling, the following services need to be started for the backup schedule to work:
- sas-viya-identities-default
- sas-viya-scheduler-default
- sas-viya-jobdefinitions-default
- sas-viya-jobexecution-default
- sas-viya-restexecutionprovider-default

If one of the services is not running during Backup Service bootstrap, then the Backup Service retries every 5 minutes for 25 tries to schedule default 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. Check and ensure that all the required services are started, and then restart the Backup Service (sas-viya-deploymentBackup-default). This schedules the default backup.

Once the backup schedule has been created, it is displayed in the SAS Environment Manager.

You can add one or more triggers to the schedule. To add a trigger to the schedule:

1. Click in the left pane to display the Scheduling window.

2. Select the name of the schedule that you created. In the figure above, the schedule is named DEFAULT_BACKUP_SCHEDULE. Click . The Edit Schedule dialog box is displayed.
Edit Schedule

Name: **DEFAULT_BACKUP_SCHEDULER_JOB**

Run as:  ⓢ  

sas.scheduler

Trigger type:  

Time Event

Available triggers

<table>
<thead>
<tr>
<th></th>
<th>Name</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>⓶</td>
<td>Default_Backup_Schedule_Trigger</td>
<td>🔄</td>
</tr>
</tbody>
</table>

3  Click  ‍‍‍‍‍ to add a trigger to the schedule. The New Trigger window is displayed.

New Trigger

Name:  

Frequency:  Daily  | Interval:  ▾  1  days

Time:  10:53

Time zone:  ⓢ  America/New_York

Start date:  Nov 16, 2017

End:  Never

4  Update the fields as appropriate. You must complete the **Name** and **Time** fields.

5  Click **Save** to save the new trigger.

   If you want to return to the default settings, click **Reset**.
6 Click **Save** to save the new job schedule.

**Schedule a Binary Backup**

In SAS Viya, a default backup is scheduled through the Backup Service bootstrap. If you want to schedule a binary backup, then manual steps need to be executed. When using curl commands, the user needs to get the Authorization token for the administrator user.

For information about how to obtain a token, see [Obtain an Access Token Using Password Credentials](#).

To create a schedule for a binary backup:

1 You need a jobDefinition ID. This jobDefinition ID is already created when default backup is scheduled.
2 Using the jobDefinition ID, you need to create a jobExecution Request.
3 The jobExecution response to the jobExecution request gives a link to submit the job to be scheduled.
4 Once the job is submitted, it is visible through SAS Environment Manager and you can schedule your job.

The following steps provide the details to schedule a binary backup:

1 Execute the jobDefinitions REST API to get the jobDefinition ID. This ID was created while scheduling Default backup. The jobDefinition can be used to create schedule for binary backup. To get the jobDefinition ID for an existing jobDefinition, run the following curl command:

   ```bash
   curl --verbose --header "Accept: application/json" --header "Authorization: bearer <token>" --request "GET" 
   "<protocol>://<host>:<port>/jobDefinitions/
   definitions?limit=20&filter=in(name,"DEFAULT_BACKUP_SCHEDULE")"
   ``

   This will return a jobDefinition object defined for default backup schedule. From the response select the "id" parameter.

   Sample Response:

   ```json
   "items": [ 
   {"creationTimeStamp": "2017-10-28T13:40:55.566Z",
   "modifiedTimeStamp": "2017-10-28T13:40:55.566Z",
   "createdBy": "sas.deploymentBackup",
   "modifiedBy": "sas.deploymentBackup",
   "version": 1,
   "id": "7c0f326b-280f-42ef-a404-39c9c775f325" }
   ]
   ```
Create a job request once the jobDefinition ID is known. The following parameters need to be populated to create a jobRequest object.

- **name**—Name of the job request to be created. This name is used as the label in the SAS Environment Manager.
- **description**—One-line description of jobRequest to be created.
- **jobDefinitionURI**—This is the jobDefinition ID that was obtained when the curl command was run.
- **contentType**—This is the content type of the DeploymentBackup Request.
  
  If multi-tenant: `contentType = "application/vnd.sas.backup.deployment.request+json"`
  
  If single-tenant: `contentType = "application/vnd.sas.backup.request+json"`

If you are running a single-tenant environment, the following is a sample curl command for creating a jobRequest for the job execution service:

```bash
curl --verbose --header "Accept: application/vnd.sas.job.execution.job.request+json"
   --header "Authorization: bearer <token> "
   --header "Content-Type: application/vnd.sas.job.execution.job.request+json" --data '{
   "name": "BINARY_BACKUP_SCHEDULE1",
   "description": "This jobRequest is to execute binary backup.",
   "jobDefinitionUri": "/jobDefinitions/definitions/7c0f326b-280f-42ef-a404-39c9c775f325",
   "arguments": {
      "contentType": "application/vnd.sas.backup.request+json",
      "backupType": "binary"
   }
}' --request "POST" "<protocol>://<host>:<port>/jobExecution/jobRequests"
```

If you are running a multi-tenant environment, the following is a sample curl command for creating a jobRequest for the job execution service:

```bash
curl --verbose --header "Accept: application/vnd.sas.job.execution.job.request+json"
   --header "Authorization: bearer <token> "
   --header "Content-Type: application/vnd.sas.job.execution.job.request+json" --data '{
   "name": "BINARY_BACKUP_SCHEDULE1",
   "description": "This jobRequest is to execute binary backup.",
   "jobDefinitionUri": "/jobDefinitions/definitions/7c0f326b-280f-42ef-a404-39c9c775f325",
   "arguments": {
      "contentType": "application/vnd.sas.backup.deployment.request+json",
      "backupType": "binary"
   }
}' --request "POST" "<protocol>://<host>:<port>/jobExecution/jobRequests"
```

**Note:** If you are creating a schedule for a binary backup, the `includeAllSourcesForBinaryBackup` property is not provided in the job request. In this case, only the Postgres data source is backed up. To back up other sources along with the Postgres binary backup, you need to run ad hoc backup.

Once the jobRequest is created, there is a link with "rel" as "submitJob" in the response. This link is used to submit the job. The following code is a sample response from the jobRequest command:

```json
{
   "creationTimeStamp": "2017-10-30T10:43:11.203Z",
   "modifiedTimeStamp": "2017-10-30T10:43:11.203Z",
   "createdBy": "sasin",
}
The "rel" and the corresponding link are highlighted in the code above.

4 To submit the job, execute the following curl command:

```bash
```

The job is created for the given jobRequest and the job is displayed in the SAS Environment Manager.

5 Once the job is created, you can schedule the job by adding a schedule trigger in the SAS Environment Manager.

a Select the job name in the SAS Environment Manager and click 📅 . The Edit Schedule dialog box is displayed.
In the **Run as** field, select the user from the Selected Identities window who should run the job. This user should be the administrator user.

Click **+** to add a trigger to the schedule. The New Trigger window is displayed.

**New Trigger**

- **Name:**
- **Frequency:** Daily
- **Interval:** 1 days
- **Time:** 10:53
- **Time zone:** America/New_York
- **Start date:** Nov 16, 2017
- **End:** Never

Update the fields as appropriate. You must complete the **Name** and **Time** fields.

Click **Save** to save the new trigger.

If you want to return to the default settings, click **Reset**.

Click **Save** to save the new job schedule.
Backup and Restore: Restoring to an Alternate Host

Overview
The following terminology is used in this section of the document:

Source machine
Machine where the backups were taken and these backups need to be restored on another machine.

Target machine
Alternate host having the same SAS Viya software installed on it as the source machine. The recovery operation should be executed on this alternate host from the backup taken on the source machine.

Source shared vault
Shared vault location for the source machine.

Target shared vault
Shared vault location for the target machine.

You cannot restore a binary backup to an alternate host. On a multi-tenant environment, a provider administrator can restore a default backup to an alternate host. On a single-tenant (standard) environment, an administrator can restore a default backup to an alternate host. The information in this section can be used as a part of the disaster recovery strategy at a customer site.

Assumptions
The following assumptions are made for restoring to an alternate host:

- The content present on the source machine sharedVault should be copied to some other network location. This is referred to as the target shared vault.
- The SAS Viya configuration (such as the version of SAS Viya and the hot fixes applied on it, if any) on the source machine and target machine are the same.
- All the services started successfully on the target machine.

Perform a Restore to an Alternate Host

1 Copy the contents of the source shared vault to some location. This is also used as the target shared vault.
2 Make sure the target shared vault location has the same access rights as the source shared vault.
3 Go to the SAS Environment Manager on the target machine and navigate to the backup service configuration. Change the sharedVault property value to the location for the target shared vault.
   
   **Note:** The content needs to be available under the target shared vault location before doing this. If you change the shared vault location and then copy the content, you risk losing data on the target machine.
4 As soon as the shared vault is changed, if there is any request issued for the backup or restore endpoints or if the service is restarted, then the system evaluates whether it needs to synchronize the local history with the Postgres tables. This is done by checking that the last successful backup from the global history is available in the Postgres table. If it is not available, the local history files are synchronized with the Postgres tables.
Go to the target machine command prompt, or the machine where the CLI utilities are installed. For more details about the CLI utilities, see Backup and Restore: Command Line Interface.

Use the sas-admin backup list command to see the backup history list. You should be able to see all the backups that are available on the source machine listing output.

Select a backup ID from the list to use in the restore operation.

Using the command line interface, enter the following command:

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

Make a note of the JobId printed on the console.

To see the details of restore operation, enter the following command:

```
sas-admin restore show --id=JobId
```

While the restore is running and Postgres is being restored, all of the services might not respond. The CLI command might not give the expected response and give a 403 error. You need to keep running the `sas-admin restore show --id=JobId` until you see the proper output and the status is either completed or failed.

If the restore job details show the status as completed, the restore is successful.

Restart all of the services.

After you restart all of the services, you need to restore CAS. To restore CAS, see Restore CAS Server Access Controls and Caslib Information on page 20.

After all of the steps are completed, the task of restoring to an alternate host is completed.

If a restore job’s status is failed, look in the logs to see what has failed and then take the necessary actions.

You can also use the Backup Manager on page 21 or the Backup and Restore: Command Line Interface on page 29 to perform the restore steps.

---

**Backup and Restore: Troubleshooting**

**Backup and Restore: Logs**

The backup and restore facility generates the following logs that can be used in troubleshooting:

- On the host where the backup service deployed, service logs are created under the path `/var/log/sas/viya/deploymentBackup/default/xxxxx.log`. The name of the log files is based on the time at which the backup service was started.

- On each of the data sources, backup logs are created under the path `/var/log/sas/viya/backup-agent/default/xxxxx.log`. The name of the log files is based on the time at which the backup agent service was started.

- If a restore of the SAS Infrastructure Data Server fails, the log files for this restore operation backup log files are dumped to `/opt/sas/viya/config/backup/<backup_id>/<tenant_id>/postgres` on the host where a data source resides. This is the location of the local vault.
Backup and Restore: Error and Warning Messages

A Backup or Restore Is Already in Progress
This message indicates that there is already a backup or restore operation in progress. You cannot initiate multiple backup and restore operations at the same time.

Database List in the Backup and Postgres Database Do Not Match
Databases in backup: <source list in backup> and Databases in Postgres: <source list in database> do not match. Set force option in restore request to true to force restore:

This indicates that the databases present in Postgres at the time of the backup and the databases currently in Postgres do not match. The service would not restore a database missing in the current system in this case.

**TIP** If this is acceptable and a user still wants to restore the remaining databases, then you need to set ‘force’ field sent in body of restore request to ‘true’ to force restore. When force restore is set to true, the restore operation restores only the databases that are currently in Postgres and which are also available in backup.

```
-H 'Content-Type: application/vnd.sas.restore.request+json' -d '{ "slug": "<slug name>",
*comments": "<comments>", "backupName": "<name>", "force": true
}
' '<protocol>://<host>:<port>/deploymentBackup/restores/jobs'
```

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 **default** is the value supported for configurationId. Modify the backup request body to set the configurationId to **default** and try again.

Error Code 403 While Retrieving Information Related to Restore Operation
While a Postgres restore is running, it might take a while for all services to respond. In this case, the user might see **403 Forbidden** error.

Request Contains Invalid Values for the Start or Limit Parameters
The request contains invalid values for the start ({0}) or limit ({1}) parameters. The values received for the start parameter and the limit parameter are invalid. Use positive integers as values for the start and limit parameters. Resubmit the request with valid values.

Specified Backup Does Not Have a Directory in the Vault or the History File
The specified backup is not found in the shared vault or the history file. Try using another backup to initiate the restore.

Invalid Shared Vault Location
The shared vault location is invalid. Set the valid shared vault location from the SAS Environment Manager. See **Modify the Backup Configuration Using the Environment Manager on page 10**.
List Can Only Contain Onboarded Tenants

The list of tenants should contain only tenants with a state of "onboarded". The following tenants are either not onboarded or are not valid: {0}.

Only onboarded tenants can be provided in the tenant list. Remove the tenants listed in the error from the tenant list.

backupType Value of Binary Contains a List of Tenants

The list of tenants should not be provided for backupType value of 'binary'. The Deployment Backup of backupType value 'binary' can be triggered only by a Provider Administrator user in multi-tenant deployment.

A binary backup cannot be taken for a subset of tenants in a multi-tenant environment. Remove the list of tenants from the request body if a binary backup is to be taken. You can also change the backup type to default for taking the backup for the tenants provided in the tenant list.

Also, use the Provider Administrator credentials to initiate the backup in a multi-tenant environment.

Multi-Tenant Deployment Can Be Triggered Only by a Provider Administrator

Use Provider Administrator credentials to initiate the deployment backup.

Shared Vault Is Not Accessible

The shared vault "{0}" is not accessible. Ensure that the shared vault is accessible before starting the job.

Check to see whether the shared vault location is accessible to the 'sas' user in 'sas' group.

Specified Backup ID Is Incompatible with the Target System

The specified backup ID is incompatible with the target system. Use a different backup ID to restore to the target environment.

The database mode of the environment from which the backup was taken is different from the target system. Ensure you are using the appropriate backup from the appropriate environment.