Backup and Recovery for Visual-Only and Full Deployments

Backup and Recovery: Overview

This backup and recovery documentation applies to a Linux installation. For Cloud Foundry backup and recovery documentation, see Cloud Foundry Backup and Recovery: Overview.

The Backup and Recovery 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 and Recovery service as part of a regularly scheduled backup process.

IMPORTANT: The Backup and Recovery service does not take the place of operating system or file system backups.

Note: These steps do not apply to programming-only deployments. For programming-only deployments, see Backup and Recovery for Programming-Only Deployments.

Backup and Recovery: Concepts

About the Backup and Recovery Service

The Backup and Recovery service is provided as a way to synchronize the backup and recovery 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 recovery service has the following caveats:
Backup and recovery can be initiated only by SAS Administrators.

The Backup and Recovery service requires that the SAS Infrastructure Data Server can be started.

The Backup service does not include a scheduler. SAS Technical Support provides limited to no support for implementing scheduling of the backup using operating system or third-party tools. Work with your Linux server administrator to find out what tools and/or processes are available in your environment for scheduling jobs.

The Backup and Recovery service is not a tool for disaster recovery. You cannot restore a backup from one deployment to another deployment. You cannot recover a backup to a newly deployed environment on the same machine. These statements apply even if the same host names and IP addresses are used for both deployments.

Note: Cloning can be done using system imaging or ghosting tools or other virtual machine (VM) cloning techniques. The cloned machines must use the same host names and IP addresses as the production machines. The cloned images must be regenerated each time that the SAS Viya configuration is changed. This includes the following:

- adding or updating software
- updating internal passwords
- manually editing configuration files
- changing service configurations

What Is Backed Up and What Is Not Backed Up

What Is Backed Up

The Backup and Recovery service backs up the content and configuration information that is stored in the following components for your SAS Viya 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 Recovery service. If the SAS Infrastructure Data Server is clustered, only the tables on the primary PostgreSQL node are backed up.

- **SAS Configuration Server (Consul)** – The service configuration registry that serves as a central repository for configuration data, service discovery, and health status.

- **SAS Message Broker (RabbitMQ)** – The RabbitMQ configuration. No messages or data from queues is persisted.

- **SAS Cloud Analytic Services (CAS Access Controls) and Caslib Information** – For a Distributed CAS server, only the CAS Controller is backed up.

These sources for a SAS Viya deployment might reside on single machine or on different machines.

What Is Not Backed Up

The Backup and Recovery 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 Recovery service backs up content and configuration information and is not provided as a way to backup and restore a SAS Viya deployment.

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

Backup and Recovery: Guidelines

Best Practices for Performing Backups

- Always use the Backup and Recovery 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 and Recovery service also finds content and configuration data from your SAS Viya deployment and backs them up at the same point in time, which is required for a same point in time recovery of content and configuration data.

- Run the Backup and Recovery 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 SAS Viya configuration including configuration properties.

- Old backups are purged after the retention period and are deleted from the file system. If you do not want backups to be deleted after the retention period, you need to manually archive the backups to a safe location before they are purged. You can then recover these backups from the archive.

Best Practices for Postgres on a Single-Node When the SAS Infrastructure Data Server Is Not Configured for HA

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

- However, if you have not configured the SAS Infrastructure Data Server for HA (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 in addition to using the Backup and Recovery service that you also use the pg_basebackup utility provided by PostgreSQL to create a binary copy of the data to be used as a basis for a point-in-time recovery. It is recommended that you use the pg_basebackup utility after any configuration and or installation changes are made to the SAS Viya environment. The Backup and Recovery service should also be used to perform regular backups.

For more information about pg_basebackup, see Postgres documentation.

For example, on the PostgreSQL server host when you are logged in as the "sas" user, execute:

```bash
export PATH=/opt/sas/viya/home/bin:$PATH
export LD_LIBRARY_PATH=/opt/sas/viya/home/lib:/opt/sas/viya/home/lib64:$LD_LIBRARY_PATH
export BACKUP_DIR=/opt/sas/viya/config/data/sasdatasvr/postgres
cd $BACKUP_DIR
mkdir pgbaseBKPTar
pg_basebackup -D pgbaseBKPTar -P tar -X fetch -h localhost -p 5431 -z -P -v
```

Note: The pgbaseBKPTar directory should already exist before you run this command.

Note: The pg_basebackup command should be run during a maintenance window.

This command backs up the PostgreSQL data directory to the TAR file, which can be archived. This backup is performed on the primary data server.
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 Postgres Database.

**Best Practices for Performing Recoveries**

- Always use the Backup and Recovery Service to perform restores to ensure a same point-in-time recovery of content and configuration data.
- Always choose the most recent successful backup to perform a recovery operation.
- Ensure minimum use of the systems. When performing a recovery, only the following services should be running:

  ```
  sas-viya-consul-default
  sas-viya-rabbitmq-server-default
  sas-viya-cascontroller-default
  sas-viya-sasdatasvrc-postgres-node0-ct-pg_hba
  sas-viya-sasdatasvrc-postgres-node0-ct-postgresql
  sas-viya-sasdatasvrc-postgres-pgpool0-ct-pcm
  sas-viya-sasdatasvrc-postgres-pgpool0-ct-pgpool
  sas-viya-sasdatasvrc-postgres-pgpool0-ct-pool_hba
  sas-viya-sasdatasvrc-postgres-node0
  sas-viya-sasdatasvrc-postgres
  sas-viya-httpproxy-default
  sas-viya-authorization-default
  sas-viya-configuration-default
  sas-viya-identities-default
  sas-viya-saslogon-default
  sas-viya-geodelocator-default
  sas-viya-deploymentBackup-default
  sas-viya-backup-agent-default
  ```
- The backup-agent service must be running on all the data sources that need to be restored.
- After performing a recovery, stop and restart all services.

  - Stop all services
    ```
    sudo /etc/init.d/sas-viya-all-services stop
    ```
  - Restart all services
    ```
    sudo /etc/init.d/sas-viya-all-services start
    ```

**Backup and Recovery Terms**

The following is a list of terms used in this document for the Backup and Recovery service:

**Local vault**

A local file system path located on the same host where a backup source resides. It is the location where the backup files for the data source are created.

**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 purged?
If PostgreSQL is being restored, does the list of databases in the backup match the list of databases currently present in the SAS Infrastructure Data Server?

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

**Shared vault**
any network location to preserve the backups. The backup files are copied from a local vault to a shared vault. The install user of SAS should have access to this location. It is referred to as `vaultLocation` in the SAS Environment Manager user interface.

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

**State**
state of a backup or restore operation. Possible values for this attribute include the following:

- **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** – a backup or restore operation completed but the system was not able to transfer the backup to the specified vault location.
- **completed** – a backup or restore operation has completed successfully.
- **failed** – a backup or restore operation for one or more data sources has failed.

---

**Backup: How the Process Works**

**Note:** This information does not apply to a **programming-only** deployment.

1. You invoke the `/backups/jobs` REST API. The backup service discovers the deployed services that are to be backed up from the SAS Configuration Server and then creates a backup job. Auto discovery ensures that if additional services have been added to the deployment since the last backup, they are included in the backup automatically.

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. After 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 backup name (for example, `2016-08-04T05_29_55_910-0400`) and data source name (for example, `2016-08-04T05_29_55_910-0400\consul\xxxx.dmp`).

4. The backup service then finds the location of the shared vault from the configuration and transfers the locally stored backup files to the shared vault. The backups are stored within the folder named `backupName`.

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

5. 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, then the entire backup is considered to have failed.
Backup and Recovery: Service Configuration

Backup Configuration Properties
The backup service has its own configuration, which is used to perform the backup and recovery. The backup configuration includes configuration properties, which come with default values. The only property that does not have a default value is vaultLocation, which is the location that you must specify for the Shared Vault.

The following configuration properties can be changed:

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

Best Practices for Configuring Backups

- Always ensure that the values of the vaultLocation and retentionPeriod are set immediately after situations such as a new installation, upgrading software, or after making any modifications to your SAS Viya deployment.

- Ensure that the vaultLocation is accessible to the install user (sas).

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

- Set the retentionPeriod value to ensure 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 retention period must be 4 days. If you are doing weekly backups, the recommended retention period is 30 days.

Configuring the Backup

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

1. **Determine a schedule for the backup.**

   A method to schedule the backup is not provided with the Backup and Recovery service. You need to use your own methods for scheduling the backup. An administrator might have to write a script to get the authentication token and use the token to invoke the backup REST API. Administrators can use tools like cron to schedule these scripts to run periodically at fixed times, dates, or intervals.

2. **Set the vault location to a network accessible location.** See Modify the Backup Configuration Using the SAS Environment Manager to modify the vaultLocation property.

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

3. **Set an appropriate retention period.**

   The retention period should be set to a value to ensure that there are at least three recent successful backups at any point in time. For example: If you schedule a daily backup, then the retention period should be at least 3 days. If you schedule the backup to run weekly, then your retention period should be at least 21 days.

4. **Check the groups for the users who are running Viya services and cas controllers.** The backup service uses a 'sas' user to backup and restore data sources from respective tiers that is 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 recovery.
For example, if you have another user named 'cas' in the 'cas' group, make that 'cas' user also a member of the 'sas' user group. Make the 'sas' user a member of the 'cas' user group.

The following commands are examples of how to make users members of groups:

```
sudo usermod -g sas cas
sudo usermod -g cas sas
```

After running the commands, restart the following two services:

```
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 the 'sas' group.

Make sure that the users running the cas process and sas services have the appropriate memberships.

---

**Modify the Backup Configuration Using the SAS Environment Manager**

The configuration properties `retentionPeriod` and `vaultLocation` can be modified using SAS Environment Manager as follows:

1. Using your administration credentials, log on to `<protocol>://<host>:<port>/SASEnvironmentManager`.
2. Click in the top left corner.
3. Select **Resources ➔ Configuration**.
4. Select **All services** from the drop-down menu.
5. Click **Backup service** in the left pane.
6. Scroll down until you see `sas.deploymentbackup` and click to the right of the service.
7. Change the properties as necessary or keep the defaults. However, you must change the `vaultLocation` property because there is no default value.

---

**Backup and Recovery: How To**

**Overview**

The “How To” topics featured in this section require the running of curl commands. These commands are used to validate backups, view the collection of backups, perform a backup, and other tasks. Here is a list of actions that you can perform for a backup:

**Note:** These commands were validated using curl versions 7.54.0 and 7.19.7.

- Validate Backup Service
  - Validate that the backup service is running.
- Available APIs
  - Get a list of all root-level Rest API endpoints.
- Configuration
  - View the collection of backup configurations.
  - View backup configuration by ID.
  - View a collection of backup-enabled sources by configurationID.
View a backup enabled source by ID.

**Backup**

- Perform a backup.
- View state of the backup job by ID.
- View backup job by ID.
- View backup details.
- View a collection of all of the running or pending backup jobs.
- View backup history.

**Validate That the Backup Service Is Running**

After the deployment is complete, the deploymentBackup service must be configured and running for the successful backup and recovery of the content and configuration. To validate if the backup service is running, run the following curl command:

```
HTTP/1.1 200 OK
Date: Fri, 02 Dec 2016 03:37:09 GMT
Server: Apache-Coyote/1.1
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval';
  img-src 'self' *.sas.com data:; style-src 'self' 'unsafe-inline'; child-src 'self' data: mailto:;
X-Application-Context: deploymentBackup:0
Vary: User-Agent
Content-Type: text/plain; charset=UTF-8
```

For information about how to obtain a token, see [Authenticate the REST APIs](#).

If this call succeeds and returns HTTP status code 200 (OK), then the backup service was successfully deployed.

**Note:** You need to specify a `<port>` if the port is not set to 80. If the port is set to 80, you might or might not need to specify it. In that case, you can just specify a host.

**Get List of All Root-Level Rest API Endpoints**

Before performing a backup and recovery, you need to know about the REST API endpoints that facilitate backup and restore. Executing a curl command to `/deploymentBackup` returns the list of endpoints, which act as an entry into the backup and recovery. The returned endpoints include an API to initiate backup, initiate restore, view backup configuration, view backup history, and view restore history.

The curl command to produce the list of endpoints is as follows:

```
  <protocol>://<host>:<port>/deploymentBackup/Response:
  {
    "version":1,
    "links":{
      "method":"POST",
      "rel":"startBackup",
      "href":":/deploymentBackup/backups/jobs",
```
There is only one POST API to backup all the sources. When the `startBackup` (POST /backups/jobs) is invoked, it discovers Rabbitmq, Postgres, Consul, and CAS data sources and backs them up.

**Note:** You need to specify a `<port>` if the port is not set to 80. If the port is set to 80, you might or might not specify it. In that case, you can just specify a host.

### View the Collection of Backup Configurations

You should review the backup configuration before running a backup or restore. It is recommended to configure the values of `vaultLocation` and `retentionPeriod` immediately after a successful deployment of the backup service. These data source definitions can also be seen in the backup configuration.

The `/deploymentBackup/configurations` in API can be used to view all the available backup configurations. In the current release, only the `default` configuration is supported. To view the collection of backup configurations, run the following curl command:

```bash
```

Here is an example of a response that you might receive:

```json
{
}
"links": [ 
  {
    "method": "GET",
    "rel": "self",
    "href": "/deploymentBackup/configurations",
    "uri": "/deploymentBackup/configurations",
    "type": "application/vnd.sas.collection",
    "itemType": "application/vnd.sas.backup.configuration"
  }
],
"name": "configurations",
"accept": "application/vnd.sas.backup.configuration",
"count": 1,
"items": [ 
  {
    "version": 1,
    "configurationId": "default",
    "retentionPeriod": "P10D",
    "scheduledBackupsAllowed": false,
    "vaultLocation": "/u/username/public/newVault",
    "emailToList": "none@sas.com",
    "sources": [ 
      {
        "version": 1,
        "sourceId": "consul",
        "name": "consul",
        "address": "hostname.mycompany.com",
        "included": true,
        "description": "default description",
        "links": [ 
          {
            "method": "GET",
            "rel": "self",
            "href": "/deploymentBackup/configurations/default/sources/consul",
            "uri": "/deploymentBackup/configurations/default/sources/consul",
            "type": "application/vnd.sas.backup.source.type"
          }
        ]
      },
      {
        "version": 1,
        "sourceId": "rabbitmq",
        "name": "rabbitmq",
        "address": "hostname.mycompany.com",
        "included": true,
        "description": "default description",
        "links": [ 
          {
            "method": "GET",
            "rel": "self",
            "href": "/deploymentBackup/configurations/default/sources/rabbitmq",
            "uri": "/deploymentBackup/configurations/default/sources/rabbitmq",
            "type": "application/vnd.sas.backup.source.type"
          }
        ]
      }
    ]
  }
]
{
  "version": 1,
  "sourceId": "postgres",
  "name": "postgres",
  "address": "hostname.mycompany.com",
  "included": true,
  "description": "default description",
  "links": [
    {
      "method": "GET",
      "rel": "self",
      "href": "/deploymentBackup/configurations/default/sources/postgres",
      "uri": "/deploymentBackup/configurations/default/sources/postgres",
      "type": "application/vnd.sas.backup.source.type"
    }
  ]
},
{
  "version": 1,
  "sourceId": "cas-shared-default",
  "name": "cas-shared-default",
  "address": "hostname.mycompany.com",
  "included": true,
  "description": "default description",
  "links": [
    {
      "method": "GET",
      "rel": "self",
      "href": "/deploymentBackup/configurations/default/sources/cas-shared-default",
      "uri": "/deploymentBackup/configurations/default/sources/cas-shared-default",
      "type": "application/vnd.sas.backup.source.type"
    }
  ]
},
"links": [
  {
    "method": "GET",
    "rel": "self",
    "href": "/deploymentBackup/configurations/default",
    "uri": "/deploymentBackup/configurations/default",
    "type": "application/vnd.sas.backup.configuration"
  },
  {
    "method": "GET",
    "rel": "up",
    "href": "/deploymentBackup/configurations",
    "uri": "/deploymentBackup/configurations",
    "type": "application/vnd.sas.collection",
    "itemType": "application/vnd.sas.backup.configuration"
  },
  {
    "method": "GET",
    "rel": "collection",
    "href": "/deploymentBackup/configurations/default/sources",
    "uri": "/deploymentBackup/configurations/default/sources",
    "type": "application/vnd.sas.backup.source"}
View a Collection of Backup-Enabled Sources by ConfigurationID

Each configuration has a set of data sources for the backup. To view these sources for a particular configuration, you can use the `/deploymentBackup/configurations/<configurationId>/sources` service. Only the "default" configuration is supported for this release.

To view the collection of enabled sources by configurationID, run the following curl command:

```
<protocol>://<host>:<port>/deploymentBackup/configurations/<configuration-id>/sources
```

Here is an example of a response that you might receive:

```
Response:
{
  "links": [
    {
      "method": "GET",
      "rel": "collection",
      "href": "/deploymentBackup/backups",
      "uri": "/deploymentBackup/backups",
      "type": "application/vnd.sas.collection",
      "itemType": "application/vnd.sas.backup.source.type"
    },
    {
      "method": "GET",
      "rel": "self",
      "href": "/deploymentBackup/backups?start=0&limit=10",
      "uri": "/deploymentBackup/backups?start=0&limit=10",
      "type": "application/vnd.sas.collection",
      "itemType": "application/vnd.sas.backup.source.type"
    }
  ],
  "name": "sources",
  "accept": "application/vnd.sas.backup.source.type",
  "start": 0,
  "count": 4,
  "items": [
    {
      "version": 1,
      "sourceId": "consul",
      "name": "consul",
```
"address": "hostname.mycompany.com",
"included": true,
"description": "default description",
"links": [ 
  
  
  "version": 1,
  "sourceId": "rabbitmq",
  "name": "rabbitmq",
  "address": "hostname.mycompany.com",
  "included": true,
  "description": "default description",
  "links": [ 
    
    ]
  
  "version": 1,
  "sourceId": "postgres",
  "name": "postgres",
  "address": "hostname.mycompany.com",
  "included": true,
  "description": "default description",
  "links": [ 
    
    ]
  
  "version": 1,
  "sourceId": "cas-shared-default",
  "name": "cas-shared-default",
  "address": "hostname.mycompany.com",
  "included": true,
  "description": "default description",
  "links": [ 
    
    ]
]
View Backup Configuration by ConfigurationID

You can also look up a configuration by the configuration ID. The API endpoint /deploymentBackup/configurations/<configurationId> can be used to look up a configuration with a specified ID instead of using the <configurationId> parameter. Therefore, the API endpoint /deploymentBackup/configurations/default can be used to retrieve configuration with the default ID. The backup service automatically discovers the sources that are enabled for the backup in this configuration. To get the configuration by ID, run the following curl command:

```
```

Here is an example of a response that you might receive:

```
Response for configurationId = default
{
  "version": 1,
  "configurationId": "default",
  "retentionPeriod": "P10D",
  "scheduledBackupsAllowed": false,
  "vaultLocation": "/u/username/public/newVault",
  "emailToList": "none@sas.com",
  "sources": [
    {
      "version": 1,
      "sourceId": "consul",
      "name": "consul",
      "address": "hostname.mycompany.com",
      "included": true,
      "description": "default description",
      "links": [
        {
          "method": "GET",
          "rel": "self",
          "href": "/deploymentBackup/configurations/default/sources/consul",
          "uri": "/deploymentBackup/configurations/default/sources/consul",
          "type": "application/vnd.sas.backup.source.type"
        }
      ]
    },
    {
      "version": 1,
      "sourceId": "rabbitmq",
      "name": "rabbitmq",
      "address": "hostname.mycompany.com",
      "included": true,
      "description": "default description",
      "links": [
        {
          "method": "GET",
          "rel": "self",
          "href": "/deploymentBackup/configurations/default/sources/rabbitmq",
          "uri": "/deploymentBackup/configurations/default/sources/rabbitmq",
          "type": "application/vnd.sas.backup.source.type"
        }
      ]
    }
  ]
}
```
"included": true,
"description": "default description",
"links": [
  {
    "method": "GET",
    "rel": "self",
    "href": "/deploymentBackup/configurations/default/sources/rabbitmq",
    "uri": "/deploymentBackup/configurations/default/sources/rabbitmq",
    "type": "application/vnd.sas.backup.source.type"
  }
],
"version": 1,
"sourceId": "postgres",
"name": "postgres",
"address": "hostname.mycompany.com",
"included": true,
"description": "default description",
"links": [
  {
    "method": "GET",
    "rel": "self",
    "href": "/deploymentBackup/configurations/default/sources/postgres",
    "uri": "/deploymentBackup/configurations/default/sources/postgres",
    "type": "application/vnd.sas.backup.source.type"
  }
],
"version": 1,
"sourceId": "cas-shared-default",
"name": "cas-shared-default",
"address": "hostname.mycompany.com",
"included": true,
"description": "default description",
"links": [
  {
    "method": "GET",
    "rel": "self",
    "href": "/deploymentBackup/configurations/default/sources/cas-shared-default",
    "uri": "/deploymentBackup/configurations/default/sources/cas-shared-default",
    "type": "application/vnd.sas.backup.source.type"
  }
],
"links": [
  {
    "method": "GET",
    "rel": "self",
    "href": "/deploymentBackup/configurations/default",
    "uri": "/deploymentBackup/configurations/default",
    "type": "application/vnd.sas.backup.configuration"
  }
]
View a Backup Enabled Source by SourceID

From the list of data sources enabled for a backup in a configuration, you can view the definition for a specific data source by using the datasourceId. The GET /deploymentBackup/configurations/<configurationId>/sources/<sourceId> API endpoint can be used to fetch a data source definition within a configuration. Here, the configuration is identified using the configurationId, and the source is identified using the sourceId. The sourceId can have the values Postgres, rabbitmq, consul, and cas. The only value that the configurationId can have is default. Use the following curl command to view a backup enabled source by ID:

```
```

Here is an example of a response that you might receive:

```
Response:
{
  "version": 1,
  "sourceId": "postgres",
  "name": "postgres",
  "address": "hostname.mycompany.com",
  "included": true,
  "description": "default description",
  "links": [
    {
      "method": "GET",
      "rel": "self",
      "href": "/deploymentBackup/configurations/default/sources/postgres",
      "uri": "/deploymentBackup/configurations/default/sources/postgres",
      "type": "application/vnd.sas.backup.source.type"
    },
    {
      "method": "GET",
      "rel": "configuration",
      "href": "/deploymentBackup/configurations/default/sources/postgres",
      "uri": "/deploymentBackup/configurations/default/sources/postgres",
      "type": "application/vnd.sas.backup.configuration"
    }
  ]
}
```
Perform a Backup

To perform a backup, you must use curl or other external means to call REST APIs directly.

The backup REST call deploymentBackup/jobs submits the backup job and immediately returns an HTTP status of 202 if the request is accepted. Along with this response, there is a link containing a job identifier that can be used in a curl command to retrieve the status of the job.

Use the following curl command to start a backup:

```
-H "Content-Type: application/vnd.sas.backup.request+json" -d"{
"version": 1,
"slug": "<slug-name>",
"comments": "<comments>",
"configurationId": "<configuration-id>"
}" <protocol>://<host>:<port>/deploymentBackup/backups/jobs
```

The above curl command has the following parameters:

**slug**
User-provided identifier. An example is "weekly_backup_01".

**comments**
User-provided comments. An example is “First backup after installation”.

**configurationId**
ID of the configuration used to perform backup. Currently, only the default configuration is supported.

Here is an example of a response that you might receive after running the curl command:

```
{
"version":1,
"jobId":"8098e355-d228-4767-808c-336058e9398c",
"state":"pending",
"owner":"tara",
"startTimeStamp":"2016-12-02T04:22:59.063Z",
"links":[
{
"method":"GET",
"rel":"self",
"href":"/deploymentBackup/backups/jobs/8098e355-d228-4767-808c-336058e9398c",
"uri":"/deploymentBackup/backups/jobs/8098e355-d228-4767-808c-336058e9398c",
"type":"application/vnd.sas.backup.job"
}
]
```

The following is an example of a response that you might receive if the job is already running or if the job is pending:

```
{
    "errorCode": 0,
    "message": "A backup/restore is already in progress.",
    "details": [
        "exception: com.sas.commons.rest.exceptions.ResourceException",
        "correlator: a8447d8e-8394-4ef3-8c12-8bcc219b45f7",
        "path: /deploymentBackup/backups/jobs"
    ],
    "links": [],
    "version": 2,
    "httpStatusCode": 409
}
```

**View State of the Backup Job By JobID**

The backup occurs in the background so you need to check the status of the backup job to determine when it is complete. To see the state of a specific backup job, use the ID (of the backup job) that was returned in the response when the backup was initiated. Use the following curl command to check the state of a backup:

```
<protocol>://<host>:<port>/deploymentBackup/backups/jobs/<job-id>/state
```

Here is an example of a response that you might receive:

```
Response:
completed
```

Other statuses that you might receive are pending, running, completedWithWarning, or failed.

**View Backup Job By JobID**

You can look up a backup job that was previously run by using the backup ID. Run the following curl command:

```
<protocol>://<host>:<port>/deploymentBackup/backups/jobs/<job-id>
```

Here is an example of a response that you might receive:

```
response:
{
    "version": 1,
    "jobId": "8098e355-d228-4767-808c-336058e9398c",
    "state": "completed",
    "owner": "tara",
    "startTimeStamp": "2016-12-02T04:22:59.063Z",
    "endTimeStamp": "2016-12-02T04:23:10.281Z",
    "links": [
```

View State of the Backup Job By JobID

The backup occurs in the background so you need to check the status of the backup job to determine when it is complete. To see the state of a specific backup job, use the ID (of the backup job) that was returned in the response when the backup was initiated. Use the following curl command to check the state of a backup:

```
<protocol>://<host>:<port>/deploymentBackup/backups/jobs/<job-id>/state
```

Here is an example of a response that you might receive:

```
Response:
completed
```

Other statuses that you might receive are pending, running, completedWithWarning, or failed.

View Backup Job By JobID

You can look up a backup job that was previously run by using the backup ID. Run the following curl command:

```
<protocol>://<host>:<port>/deploymentBackup/backups/jobs/<job-id>
```

Here is an example of a response that you might receive:

```
response:
{
    "version": 1,
    "jobId": "8098e355-d228-4767-808c-336058e9398c",
    "state": "completed",
    "owner": "tara",
    "startTimeStamp": "2016-12-02T04:22:59.063Z",
    "endTimeStamp": "2016-12-02T04:23:10.281Z",
    "links": [
```
View Backup Details

You can use the following curl command to view backup details that were used in the backup. These can include state of the backup, time at which the backup occurred, or size of each of the sources used in the backup.

```bash
<protocol>://<host>:<port>/deploymentBackup/backups/<backup-id>
```

Here is an example of a response that you might receive:

```json
response:
{
  "version":1,
  "backupId":"8098e355-d228-4767-808c-336058e9398c",
  "slug":"curl slug",
  "name":"2016-12-01T23_22_59_063-0500",
  "state":"completed",
  "size":14811598,
  "owner":"tara",
  "startTimeStamp":"2016-12-02T04:22:59.063Z",
  "endTimeStamp":"2016-12-02T04:23:10.281Z",
  "sources":[
    {
      "version":1,
      "sourceId":"rabbitmq",
      "name":"rabbitmq",
      "address":"hostname.mycompany.com",
      "state":"completed",
      "startTimeStamp":"2016-12-02T04:22:59.062Z",
      "endTimeStamp":"2016-12-02T04:22:59.278Z",
      "size":4060
    },
    {
      "version":1,
      "sourceId":"rabbitmq",
      "name":null,
      "address":null,
      "state":null,
      "startTimeStamp":null,
      "endTimeStamp":null,
      "size":null
    }
  ]
}
```
"sourceId":"consul",
"name":"consul",
"address":"hostname.mycompany.com",
"state":"completed",
"startTimeStamp":"2016-12-02T04:22:59.062Z",
"endTimeStamp":"2016-12-02T04:22:59.316Z",
"size":347947
},
{
"version":1,
"sourceId":"postgres",
"name":"postgres",
"address":"hostname.mycompany.com",
"state":"completed",
"startTimeStamp":"2016-12-02T04:22:59.062Z",
"endTimeStamp":"2016-12-02T04:23:09.524Z",
"size":14420015
},
{
"version":1,
"sourceId":"cas-shared-default",
"name":"cas-shared-default",
"address":"hostname.mycompany.com",
"state":"completed",
"startTimeStamp":"2016-12-02T04:22:59.062Z",
"endTimeStamp":"2016-12-02T04:23:09.646Z",
"size":39576
}
],
"links": [
{
"method":"GET",
"rel":"self",
"href":"/deploymentBackup/backups/8098e355-d228-4767-808c-336058e9398c",
"uri":"/deploymentBackup/backups/8098e355-d228-4767-808c-336058e9398c",
"type":"application/vnd.sas.backup"
},
{
"method":"GET",
"rel":"configuration",
"href":"/deploymentBackup/configurations/default",
"uri":"/deploymentBackup/configurations/default",
"type":"application/vnd.sas.backup.configuration"
},
{
"method":"POST",
"rel":"startRestore",
"href":"/deploymentBackup/restores/jobs",
"uri":"/deploymentBackup/restores/jobs",
"type":"application/vnd.sas.restore.request+json",
"responseType":"application/vnd.sas.restore.job"
}]
View a Collection of All of the Running or Pending Backup Jobs

You can view the collection of all the backup jobs that are currently pending or running in the system. The curl command to view all such jobs is as follows:


Here is an example of a response that you might receive:

```json
{
    "links": [
        {
            "method": "GET",
            "rel": "collection",
            "href": "/deploymentBackup/backups/jobs",
            "uri": "/deploymentBackup/backups/jobs",
            "type": "application/vnd.sas.collection",
            "itemType": "application/vnd.sas.backup.job"
        },
        {
            "method": "GET",
            "rel": "self",
            "href": "/deploymentBackup/backups/jobs?start=0&limit=10",
            "uri": "/deploymentBackup/backups/jobs?start=0&limit=10",
            "type": "application/vnd.sas.collection",
            "itemType": "application/vnd.sas.backup.job"
        },
        {
            "method": "GET",
            "rel": "backupHistory",
            "href": "/deploymentBackup/backups",
            "uri": "/deploymentBackup/backups",
            "type": "application/vnd.sas.collection",
            "itemType": "application/vnd.sas.backup.summary"
        }
    ],
    "name": "backupJobs",
    "accept": "application/vnd.sas.backup.job",
    "start": 0,
    "count": 1,
    "items": [
        {
            "version": 1,
            "jobId": "c7a3710a-2e36-44b4-8361-7aaebf9d3488",
            "state": "running",
            "owner": "tara",
            "startTimeStamp": "2017-04-19T07:43:50.262Z",
            "endTimeStamp": "2017-04-19T07:44:01.344Z",
            "links": [
                {
                    "method": "GET",
                    "rel": "self",
                    "href": "/deploymentBackup/backups/jobs/c7a3710a-2e36-44b4-8361-7aaebf9d3488",
                    "uri": "/deploymentBackup/backups/jobs/c7a3710a-2e36-44b4-8361-7aaebf9d3488",
                    "type": "application/vnd.sas.backup.job"
                }
            ]
        }
    ]
}
```
View Backup History

To see a history of previous backups, use the following curl command:


Here is an example of a response that you might receive:

response:
{
  "links": [
    {
      "method": "GET",
      "rel": "collection",
      "href": "/deploymentBackup/backups",
      "uri": "/deploymentBackup/backups",
      "type": "application/vnd.sas.collection",
      "itemType": "application/vnd.sas.backup.summary"
    },
    {
      "method": "GET",
      "rel": "self",
      "href": "/deploymentBackup/backups?start=0&limit=10",
      "uri": "/deploymentBackup/backups?start=0&limit=10",
      "type": "application/vnd.sas.collection",
      "itemType": "application/vnd.sas.backup.summary"
    },
    {
      "method": "GET",
      "rel": "next",
      "href": "/deploymentBackup/backups?start=10&limit=10",
      "uri": "/deploymentBackup/backups?start=10&limit=10",
      "type": "application/vnd.sas.collection"
    }
  ],
  "limit": 1,
  "version": 2
}
"rel": "last",
"href": "/deploymentBackup/backups?start=10&limit=10",
"uri": "/deploymentBackup/backups?start=10&limit=10",
"type": "application/vnd.sas.collection"
],
"name": "backups",
"accept": "application/vnd.sas.backup.summary",
"start": 0,
"count": 15,
"items": [
{
"version": 1,
"backupId": "8098e355-d228-4767-808c-336058e9398c",
"slug": "curl slug",
"name": "2016-12-01T23_22_59_063-0500",
"state": "completed",
"size": 14811598,
"owner": "tara",
"startTimeStamp": "2016-12-02T04:22:59.063Z",
"endTimeStamp": "2016-12-02T04:23:10.281Z",
"sources": [
{
"id": "rabbitmq",
"name": "rabbitmq",
"state": "completed"
},
{
"id": "consul",
"name": "consul",
"state": "completed"
},
{
"id": "postgres",
"name": "postgres",
"state": "completed"
},
{
"id": "cas-shared-default",
"name": "cas-shared-default",
"state": "completed"
}
],
"links": [
{
"method": "GET",
"rel": "details",
"href": "/deploymentBackup/backups/8098e355-d228-4767-808c-336058e9398c",
"uri": "/deploymentBackup/backups/8098e355-d228-4767-808c-336058e9398c",
"type": "application/vnd.sas.backup"
},
{
"method": "GET",
"rel": "configuration",
"href": "/deploymentBackup/configurations/default",
"uri": "/deploymentBackup/configurations/default",
"type": "application/vnd.sas.backup"
}]}
"type": "application/vnd.sas.backup.configuration"
```
Recovery: 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 CAS data and configuration. For instructions on manually restoring this content, see Restore CAS Server Access Controls and Caslib Information.

Note: These commands were validated using curl versions 7.54.0 and 7.19.7.

The backup and recovery service has the following caveats. The backup and recovery service:

- Cannot be used to restore CAS data and 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.
- CAS data and configuration are not restored with the Backup and Recovery service. Instructions are provided in this document for manually restoring CAS data and configuration.
- Cannot perform a recovery 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 recovery with the Backup and Recovery service. For more information, see Recover a Failed HA Cluster.
  - If you have not configured the SAS Infrastructure Data Server for HA, it is recommended that you read and perform the steps provided in this document in the section Best Practices for Postgres on a Single-Node and use pg_basebackup in addition to the Backup and Recovery service.
- Cannot use the service to recover a backup to a newly deployed environment even if the host names and IP addresses are the same.

Prerequisites
To perform a recovery, 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, then you must first use the pg_basebackup utility to restore. For more information, see Best Practices for Postgres on a Single-Node.

How the Restore Process Works

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 recovery service, the following services must be running:

   - sas-viya-consul-default
   - sas-viya-rabbitmq-server-default
   - sas-viya-cascontroller-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-sasdatasvrc-postgres
sas-viya-httpproxy-default
sas-viya-authorization-default
sas-viya-configuration-default
sas-viya-identities-default
sas-viya-saslogon-default
sas-viya-geodelocator-default
sas-viya-deploymentBackup-default
sas-viya-backup-agent-default

Note: The backup-agent service must be running on all of 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.

3 You run a curl command to perform the restore, and in that command you provide the name of the backup that you want to restore. The curl command to do this can be found in Restore on a Same Deployment on page 26.

When you run the curl command, the Backup and Restore service performs validation on the backup being used for the restore by checking if the backup exists and has not been purged. The service also checks to make sure the backup files exist in the shared vault.

If the validation is successful, the Backup and Recovery service initiates the restore. The Backup and Recovery service sends a message to each of the data sources to download the backup files from the shared vault to the local vault and the files are copied for the restore. When the restore process is completed, each of the data sources sends a message of completion to the Backup and Recovery service.

4 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.

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

6 Restart all the services.

Here is a list of actions that you can perform for a restore:

- Restore on same deployment.
- View state of the restore job by ID.
- View restore job by ID.
- View restore details.
- View a collection of all of the running or pending restore jobs.
- View restore history.

**Restore on a Same Deployment**

The Backup and Recovery service currently supports restoring the complete backup. Before beginning a restore, find the most recent successful backup.

Use the name property value of the most recent backup as a value for the backupName parameter in the restore command. This name is based on the start timestamp of the backup (for example, 2016-08-04T05_29_55_910-0400).
The restore job validates the backup for completeness. If the backup used for a restore cannot be validated, then the restore cannot proceed, and you need to select another backup for restore.

Use the following curl command to perform a restore:

```
curl -H "Authorization: bearer <token>" -H "Accept: application/vnd.sas.restore.job+json" -H "Content-Type: application/vnd.sas.restore.request+json"\n  \"slug\": "<slug-name>\",\n  \"comments\": "<comments>\",\n  \"backupName\": "<backup-name>\"
}' '<protocol>://<host>:<port>/deploymentBackup/restores/jobs'
```

The above curl command has the following parameters:

**slug**

User-provided identifier. An example is `restore_to_base_01`.

**comments**

User-provided comments. An example is `Restore using weekly_backup_01`.

**backupName**

Name of the backup being used for the restore. An example is `2016-08-04T05_29_55_910-0400`.

Here is an example of a response that you might receive:

```
Response :

{
  "version": 1,
  "jobId": "c9b8c038-a0b6-43a9-98e6-1f5134e29610",
  "backupName": "2016-12-12T07_06_32_582-0500",
  "state": "pending",
  "owner": "tara",
  "startTimeStamp": "2016-12-12T12:07:42.916Z",
  "links": [
    {
      "method": "GET",
      "rel": "self",
      "href": "/deploymentBackup/restores/jobs/c9b8c038-a0b6-43a9-98e6-1f5134e29610",
      "uri": "/deploymentBackup/restores/jobs/c9b8c038-a0b6-43a9-98e6-1f5134e29610",
      "type": "application/vnd.sas.restore.job"
    },
    {
      "method": "GET",
      "rel": "details",
      "href": "/deploymentBackup/restores/c9b8c038-a0b6-43a9-98e6-1f5134e29610",
      "uri": "/deploymentBackup/restores/c9b8c038-a0b6-43a9-98e6-1f5134e29610",
      "type": "application/vnd.sas.restore"
    },
    {
      "method": "GET",
      "rel": "backup",
      "href": "/deploymentBackup/backups/71dbbe5-5929-481e-941e-07669e7efef",
      "uri": "/deploymentBackup/backups/71dbbe5-5929-481e-941e-07669e7efef",
      "type": "application/vnd.sas.backup"
    },
    {
      "method": "GET",
      "rel": "state",
      "href": "/deploymentBackup/restores/jobs/c9b8c038-a0b6-43a9-98e6-1f5134e29610/state",
```
**View State of the Restore Job By ID**

The status of the restore job can be polled by its ID using the following curl command:

```bash
<protocol>://<host>:<port>/deploymentBackup/restores/jobs/<restore-id>/state
```

Here is an example of a response that you might receive:

```
Response:
completed
```

**View Restore Job By ID**

You can look up a restore job that has previously run by using its restore ID:

```bash
<protocol>://<host>:<port>/deploymentBackup/restores/jobs/<restore-id>
```

Here is an example of a response that you might receive:

```
Response:
{
    "version": 1,
    "jobId": "bd4024e9-fb3d-41e1-bb0e-3fddb3fc4d5e",
    "backupName": "2016-11-28T04_19_22_052-0500",
    "state": "completed",
    "owner": "tara",
    "startTimeStamp": "2016-11-28T09:30:11.826Z",
    "endTimeStamp": "2016-11-28T09:31:52.978Z",
    "links": [
        {"method": "GET", "rel": "self", "href": "/deploymentBackup/restores/jobs/bd4024e9-fb3d-41e1-bb0e-3fddb3fc4d5e",
         "uri": "/deploymentBackup/restores/jobs/bd4024e9-fb3d-41e1-bb0e-3fddb3fc4d5e",
         "type": "application/vnd.sas.restore.job"},
        {"method": "GET", "rel": "details", "href": "/deploymentBackup/restores/jobs/bd4024e9-fb3d-41e1-bb0e-3fddb3fc4d5e",
         "uri": "/deploymentBackup/restores/bd4024e9-fb3d-41e1-bb0e-3fddb3fc4d5e",
         "type": "application/vnd.sas.restore"},
        {"method": "GET", "rel": "backup", "href": "/deploymentBackup/backups/305436aa-af28-43c7-b6cd-0b71abd5e6c3",
         "uri": "/deploymentBackup/backups/305436aa-af28-43c7-b6cd-0b71abd5e6c3",
         "type": "application/vnd.sas.backup"
    ]
}
```
View Restore Details

To view restore details for each of the sources included in the restore, you can use the curl command, shown below. (Examples of restore details include the state of the restore, time taken, and so on.)

```
<protocol>://<host>:<port>/deploymentBackup/restores/<restore-id>
```

Here is an example of a response that you might receive:

```
Response:
{
  "version": 1,
  "restoreId": "bd4024e9-fb3d-41e1-bb0e-3fddb3fc4d5e",
  "backupName": "2016-11-28T04_19_22_052-0500",
  "slug": "new-restore-slug",
  "name": "2016-11-28T04_30_11_826-0500",
  "state": "completed",
  "size": 0,
  "owner": "tara",
  "startTimeStamp": "2016-11-28T09:30:11.826Z",
  "endTimeStamp": "2016-11-28T09:31:52.978Z",
  "sources": [
    {
      "version": 1,
      "sourceId": "rabbitmq",
      "name": "rabbitmq",
      "address": "127.0.0.1",
      "state": "completed",
      "startTimeStamp": "2016-11-28T09:30:11.812Z",
      "endTimeStamp": "2016-11-28T09:30:12.349Z",
      "size": 0
    },
    {
      "version": 1,
      "sourceId": "consul",
      "name": "consul",
      "address": "127.0.0.1",
      "state": "completed",
      "startTimeStamp": "2016-11-28T09:30:11.812Z",
      "endTimeStamp": "2016-11-28T09:30:12.349Z",
      "size": 0
    },
    {
      "version": 1,
      "sourceId": "postgres",
      "name": "postgres",
      "address": "127.0.0.1",
      "state": "completed",
      "startTimeStamp": "2016-11-28T09:30:11.812Z",
      "endTimeStamp": "2016-11-28T09:30:12.349Z",
      "size": 0
    }
  ]
}
```
View a Collection of All of the Running or Pending Restore Jobs

You can view the collection of all the restore jobs that are pending or running currently in the system. Run the following curl command to view all such jobs:

<protocol>://<host>:<port>/deploymentBackup/restores/jobs

Here is an example of a response that you might receive:

```
response:
{
  "links": [
    
    { "method": "GET",
      "rel": "collection",
      "href": "http://example.com/deploymentBackup/restores/jobs",
      "type": "application/vnd.sas.collection"},

    { "method": "GET",
      "rel": "self",
      "href": "http://example.com/deploymentBackup/restores/bd4024e9-fb3d-41e1-bb0e-3fddb3fc4d5e",
      "type": "application/vnd.sas.restore"}
  ]
}
```
"method": "GET",
"rel": "self",
"href": "/deploymentBackup/restores/jobs?start=0&limit=10",
"uri": "/deploymentBackup/restores/jobs?start=0&limit=10",
"type": "application/vnd.sas.collection",
"itemType": "application/vnd.sas.restore.job"
},

"method": "GET",
"rel": "restoreHistory",
"href": "/deploymentBackup/restores",
"uri": "/deploymentBackup/restores",
"type": "application/vnd.sas.collection",
"itemType": "application/vnd.sas.restore.summary"
]
],
"name": "restoreJobs",
"accept": "application/vnd.sas.restore.job",
"start": 0,
"count": 1,
"items": [

{ "version": 1,
"jobId": "c9b8c038-a0b6-43a9-98e6-1f5134e29610",
"backupName": "2016-12-12T07_06_32_582-0500",
"state": "running",
"owner": "tara",
"startTimeStamp": "2016-12-12T12:07:42.916Z",
"links": [

{ "method": "GET",
"rel": "self",
"href": "/deploymentBackup/restores/jobs/c9b8c038-a0b6-43a9-98e6-1f5134e29610",
"uri": "/deploymentBackup/restores/jobs/c9b8c038-a0b6-43a9-98e6-1f5134e29610",
"type": "application/vnd.sas.restore.job"
},

{ "method": "GET",
"rel": "details",
"href": "/deploymentBackup/restores/c9b8c038-a0b6-43a9-98e6-1f5134e29610",
"uri": "/deploymentBackup/restores/c9b8c038-a0b6-43a9-98e6-1f5134e29610",
"type": "application/vnd.sas.restore"
},

{ "method": "GET",
"rel": "backup",
"href": "/deploymentBackup/backups/71dibe5-5929-481e-941e-07669e7eefee",
"uri": "/deploymentBackup/backups/71dibe5-5929-481e-941e-07669e7eefee",
"type": "application/vnd.sas.backup"
},

{ "method": "GET",
"rel": "state",
"href": "/deploymentBackup/restores/jobs/c9b8c038-a0b6-43a9-98e6-1f5134e29610/state"}
View Restore History

To view a history of previous restore operations, use following curl command:

```bash
<protocol>://<host>:<port>/deploymentBackup/restores
```

Here is an example of a response that you might receive:

Response:

```json
{
  "links": [
    {
      "method": "GET",
      "rel": "collection",
      "href": "/deploymentBackup/restores",
      "uri": "/deploymentBackup/restores",
      "type": "application/vnd.sas.collection",
      "itemType": "application/vnd.sas.restore.summary"
    },
    {
      "method": "GET",
      "rel": "self",
      "href": "/deploymentBackup/restores?start=0&limit=10",
      "uri": "/deploymentBackup/restores?start=0&limit=10",
      "type": "application/vnd.sas.collection",
      "itemType": "application/vnd.sas.restore.summary"
    }
  ],
  "name": "restores",
  "accept": "application/vnd.sas.restore.summary",
  "start": 0,
  "count": 4,
  "items": [
    {
      "version": 1,
      "restoreId": "c21d994c-ec4d-4e69-a866-8398ed20460a",
      "backupName": "2016-11-23T05_14_19_865-0500",
      "slug": "new-restore-slug",
      "name": "2016-11-23T05_31_08_594-0500",
      "state": "completed",
      "size": 0,
      "owner": "tara",
      "startTimeStamp": "2016-11-23T10:31:08.594Z",
      "endTimeStamp": "2016-11-23T10:32:03.527Z",
      "sources": [
        {
          "id": "rabbitmq",
```
"name": "rabbitmq",
"state": "completed"
},
{
  "id": "consul",
  "name": "consul",
  "state": "completed"
},
{
  "id": "postgres",
  "name": "postgres",
  "state": "completed"
}
],
"links": [
  {
    "method": "GET",
    "rel": "details",
    "href": "/deploymentBackup/restores/c21d994c-ec4d-4e69-a866-8398ed20460a",
    "uri": "/deploymentBackup/restores/c21d994c-ec4d-4e69-a866-8398ed20460a",
    "type": "application/vnd.sas.restore"
  },
  {
    "method": "GET",
    "rel": "backup",
    "href": "/deploymentBackup/backups/e8d405d5-314d-48e4-9701-407487619dcd",
    "uri": "/deploymentBackup/backups/e8d405d5-314d-48e4-9701-407487619dcd",
    "type": "application/vnd.sas.backup"
  },
  {
    "method": "GET",
    "rel": "configuration",
    "href": "/deploymentBackup/configurations/default",
    "uri": "/deploymentBackup/configurations/default",
    "type": "application/vnd.sas.backup.configuration"
  }
]
In the case where 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.
   
   ```bash
   sudo /etc/init.d/sas-viya-all-services stop
   ```

2. Archive or rename the existing node0 directory.
   
   ```bash
   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.

---

**Restore an Unresponsive SAS Infrastructure Data Server**

---
mkdir node0
chmod 700 node0
cd node0

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

tar -xvf ../pgbaseBKPTar/base.tar.gz

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

5 Ensure that `hot_standby` property is set to `off` in the postgresql.conf file. If it is not set to "off", then set it to "off". The postgresql.conf file can be found in the `/opt/sas/viya/config/data/sasdatasvrc/postgres/node0 directory.

echo "hot_standby = off" >> postgresql.conf

6 Start the Consul service and then start the database service.

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

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

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

Verify that primary data server has started without any issues and has a status of “2”. For example:

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

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

   PGPoll is running with PID=4733
   Checking Postgresql nodes status...

   node_id | hostname        | port | status | lb_weight | role
   ---------+-----------------+------|--------+-----------+---------
   0  | myhost.domain.com | 5432 | 2      | 1.000000  | primary

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

   echo "hot_standby = on" >> postgresql.conf

---

**Backup and Recovery for Programming-Only Deployments**

**How To**

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

**CAUTION!** It is strongly recommended that you periodically back up each CAS server’s stored access control and caslib information. 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.

To back up a CAS server’s access controls and caslib information:
To use SAS Studio to create a session, see “Access the Monitor” in the “Using the CAS Server Monitor” section of SAS Viya 3.2: Administration Guide.

To perform the backup, run the following code in SAS Studio:

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

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 will be 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. Both the `permstore` and `backup` directories need to have Read and Write access by the cas user. For more information about `permstore`, see “Access Control Options” in the “Reference” section of SAS Viya Administration: SAS Cloud Analytic Services.

### Back Up Configuration Information

The following are located the 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`

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

- `/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 "Configuration Properties: How To" in SAS Viya Administration: Configuration Properties.

### Restore CAS Server Access Controls and Caslib Information

To restore a CAS server’s access controls and caslib information:

1. **Stop the server.** See “Start and Stop Cloud Analytic Services” in SAS Viya Administration: Servers.

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 `vaultLocation` you specified when configuring your backup. The `permstore` directory is under the `<backupId>/cas-shared-default` folder. The `permstore` directory needs to have Read and Write access by the cas user. If you specified a location in the `path=`` "` option when creating a backup, then that is the content that you should restore.
Restart the server. See “Start and Stop Cloud Analytic Services” in SAS Viya Administration: Servers.

---

**Backup and Recovery Troubleshooting and Frequently Asked Questions**

**Backup and Recovery: Troubleshooting**

**Backup and Recovery: Logs**

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

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

- The backup files are dumped to `/opt/sas/viya/config/backup/xxxx/` on the host where a data source resides. Here `xxxx` is the name of the backup based on the timestamp when that backup happened. This is the location of the local vault.

**Backup and Recovery: Error and Warning Messages**

**Note:** This information does not apply to a programming-only deployment.

Here is the explanation for some common error and warning messages and tips for resolving them:

1. **A backup/restore is already in progress:**
   **Explanation:** This message indicates that there is already a backup or restore operation in progress. You cannot initiate multiple backup/restore operations at the same time.

2. **Backup with "<xxx>" not found:**
   **Explanation:** Indicates that there is no backup with ID "<xxx>" found.
   **TIP** In this case, the user has to correct the ID that the backup is trying to use.

3. **Could not find configuration with ID "{0}"**
   **Explanation:** Indicates that the configurationId provided in the backup request is not available or supported.
   **TIP** Currently `default` is the only value that is supported for configurationId. Modify the backup request body to set the configurationId to `default` and try again.

**Backup and Recovery: Frequently Asked Questions**

This information does not apply to a programming-only deployment.

What does the status “unknown” for a source mean?
If the status of a source is "unknown," then either the source does not have a backup agent installed beside it or the backup agent is not running. If the source does not have a backup agent, contact your administrator. If the source does have a backup agent, then restart the backup agent service.