<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAS Viya on Cloud Foundry: Getting Started</td>
<td>2</td>
</tr>
<tr>
<td>SAS Viya on Cloud Foundry: Cheat Sheet</td>
<td>2</td>
</tr>
<tr>
<td>SAS Viya on Cloud Foundry: Scope</td>
<td>3</td>
</tr>
<tr>
<td>SAS Viya on Cloud Foundry: Deployment Types</td>
<td>4</td>
</tr>
<tr>
<td>SAS Viya on Cloud Foundry: Backup and Recovery</td>
<td>5</td>
</tr>
<tr>
<td>Backup and Recovery: Overview</td>
<td>5</td>
</tr>
<tr>
<td>Backup and Recovery: How To</td>
<td>6</td>
</tr>
<tr>
<td>SAS Viya on Cloud Foundry: Configuration Properties</td>
<td>8</td>
</tr>
<tr>
<td>Read This First</td>
<td>8</td>
</tr>
<tr>
<td>Create and Edit Configuration Instances (Persistent)</td>
<td>8</td>
</tr>
<tr>
<td>SAS Viya on Cloud Foundry: Encryption</td>
<td>9</td>
</tr>
<tr>
<td>Read This First</td>
<td>9</td>
</tr>
<tr>
<td>Overview</td>
<td>9</td>
</tr>
<tr>
<td>How To</td>
<td>10</td>
</tr>
<tr>
<td>SAS Viya on Cloud Foundry: Licensing</td>
<td>13</td>
</tr>
<tr>
<td>Read This First</td>
<td>13</td>
</tr>
<tr>
<td>Apply New Licenses</td>
<td>13</td>
</tr>
<tr>
<td>Default CAS License Location</td>
<td>14</td>
</tr>
<tr>
<td>SAS Viya on Cloud Foundry: Monitoring</td>
<td>14</td>
</tr>
<tr>
<td>Read This First</td>
<td>14</td>
</tr>
<tr>
<td>Monitoring: How to (CAS Server Monitor)</td>
<td>14</td>
</tr>
<tr>
<td>SAS Viya on Cloud Foundry: SAS Cloud Analytic Services</td>
<td>17</td>
</tr>
<tr>
<td>Read This First</td>
<td>17</td>
</tr>
<tr>
<td>Operate</td>
<td>17</td>
</tr>
<tr>
<td>How To</td>
<td>17</td>
</tr>
<tr>
<td>Concepts</td>
<td>17</td>
</tr>
<tr>
<td>Reference</td>
<td>18</td>
</tr>
<tr>
<td>SAS Viya on Cloud Foundry: Servers and Services</td>
<td>21</td>
</tr>
<tr>
<td>Read This First</td>
<td>21</td>
</tr>
<tr>
<td>Operate</td>
<td>21</td>
</tr>
<tr>
<td>Add Service Instances</td>
<td>21</td>
</tr>
</tbody>
</table>
## SAS Viya on Cloud Foundry: Getting Started

### SAS Viya on Cloud Foundry: Cheat Sheet

The following table lists Cloud Foundry administrative functionality. For tasks that are the same on Cloud Foundry and Linux, the links go to the Linux documentation. For tasks that are different on Cloud Foundry and Linux, the differences are described in the table, or links are provided to the information that is specific to Cloud Foundry.

<table>
<thead>
<tr>
<th>Subject</th>
<th>Notes, Exceptions, and References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architecture</td>
<td>To determine which SAS components are managed by BOSH and which are managed by Cloud Foundry, see these <a href="#">diagrams</a>.</td>
</tr>
<tr>
<td>Authentication</td>
<td>LDAP connection information is in the BOSH manifest. For more information, see <a href="#">SAS Viya for Cloud Foundry: Deployment Guide</a>. For all other authentication topics, see <a href="#">SAS Viya Administration: Authentication</a>. For external credentials, Cloud Foundry supports these caslib types: Path based, DNFS, HDFS, LASR, Hadoop. For more information, see <a href="#">SAS Viya Administration: External Credentials</a>.</td>
</tr>
<tr>
<td>Backups</td>
<td>See “SAS Viya on Cloud Foundry: Backup and Recovery” on page 5.</td>
</tr>
<tr>
<td>Bridging SAS 9.4 and SAS Viya</td>
<td>SAS 9.4M4 and earlier deployments require SAS/CONNECT in order to transfer data from other SAS deployments to SAS Viya. See “Sharing Data Between SAS 9 and SAS Viya using SAS/CONNECT” in SAS/CONNECT for SAS Viya: User’s Guide. Note: When you use SAS/CONNECT to import data from SAS 9.4M4 and earlier to SAS Viya, Cloud Foundry acts as the SAS/CONNECT client. The SAS/CONNECT server must be running on the SAS 9.4 machine, and the connection to SAS 9.4 must be initiated from SAS Viya. In contrast, SAS 9.4M5 environments are integrated with SAS Viya directly. As a result, SAS/CONNECT is no longer required in order to transfer data from SAS 9.4M5. SAS/CONNECT is still supported, but if you are running SAS 9.4M5, it is no longer required in order to transfer data into SAS Viya. See “Requirements to Import Data from SAS 9.4” in <a href="#">SAS Viya for Cloud Foundry: Deployment Guide</a>.</td>
</tr>
<tr>
<td>Command-line interfaces</td>
<td>See Command-line Interfaces.</td>
</tr>
<tr>
<td>Configuration</td>
<td>For persisted changes to servers, services, and system properties, modify the manifest and redeploy. For temporary changes to services and system properties, use SAS Environment Manager. See “SAS Viya on Cloud Foundry: Configuration Properties” on page 8.</td>
</tr>
<tr>
<td>Content</td>
<td>See <a href="#">SAS Viya Administration: Content Management</a> and <a href="#">SAS Viya Administration: Promotion (Import and Export)</a>.</td>
</tr>
<tr>
<td>Subject</td>
<td>Notes, Exceptions, and References</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Data                    | The following paths must be accessible to all CAS users:  
  - CentOS: /dev/shm  
  - Ubuntu: /dev/shm and /run/shm  
  See Data Administration.                                                                                                                                                                                                                                                                                                                                                                                                       |
| Encryption: Data in     | The initial state depends on your site’s setup. The only place to set up TLS is at the load balancer, external to the SAS deployment. SAS does not install HAProxy or configure TLS internally. Because the traffic that is internal to the SAS deployment is HTTP, allow port 80 at the proxy and block port 80 at the firewall.  
  Certificates are managed by BOSH and Cloud Foundry.  
  See “SAS Viya on Cloud Foundry: Encryption”.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| (TLS)                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Encryption: Data at     | See Encryption in SAS Viya: Data at Rest.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Rest                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Environment Manager     | The dashboard and machines and services views are not available in Cloud Foundry. Otherwise, all functionality is as described in Using SAS Environment Manager.                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Identities              | See Identity Management.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | |
| Licenses                | Software license information is in the BOSH manifest. To renew, paste license file contents into the manifest and redeploy. See “SAS Viya on Cloud Foundry: Licensing” on page 13.                                                                                                                                                                                                                                                                                                                                                                      |
| Logs                    | Access microservice logs from Cloud Foundry. Access CAS logs (and logs from other BOSH-managed virtual machines) from BOSH. Use the monit command to monitor the logs for services on stateful servers.                                                                                                                                                                                                                                                                                                                                                   |
| Mobile Devices          | See SAS Viya Administration: Mobile.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Monitoring              | You can use CAS Server Monitor to monitor CAS. See “Monitoring: How to (CAS Server Monitor)” on page 14.                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Servers and Services    | Some functionality in SAS Environment Manager and CAS Server Monitor should not be used for SAS Viya on Cloud Foundry. Do not attempt to add nodes, remove nodes, or terminate a server instance from either application (or with the addNode and removeNode CAS actions). Instead, use the appropriate BOSH command. See “SAS Viya on Cloud Foundry: SAS Cloud Analytic Services” on page 17 and “SAS Viya on Cloud Foundry: Servers and Services” on page 21.                                                                                                                                 |
| Themes                  | See Themes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Troubleshooting         | See “SAS Viya on Cloud Foundry: Troubleshooting” on page 22.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Updates                 | Software updates are handled by BOSH. All instances of a particular pet must be updated simultaneously. Microservices can be updated individually.                                                                                                                                                                                                                                                                                                                                                                                                              |

**SAS Viya on Cloud Foundry: Scope**

This document is intended for someone who is fluent in Cloud Foundry, familiar with your site’s Cloud Foundry implementation, and who has the necessary privileges for the Elastic Runtime to run Cloud Foundry command-line interface (cf CLI) commands.
Most operations tasks for SAS Viya on Cloud Foundry are performed using third-party tools such as BOSH commands and Cloud Foundry commands. Information about third-party tools is beyond the scope of SAS documentation.

This document provides following information:

- supporting facts that are specific to SAS Viya, including details, context, and references
- instructions for exceptions, where you can use a SAS component to perform an operations task

**SAS Viya on Cloud Foundry: Deployment Types**

### Full Deployment

The **full deployment** type includes all of the software to which you are entitled. This is the default type of deployment. Contrast with **programming-only deployment**.

### Programming-Only Deployment

The **programming-only deployment** type excludes SAS Home, most graphical user interfaces, and most services. This is the simplest and smallest type of deployment. Contrast with **full deployment**.
Note: If SAS Home is available (at your equivalent of http://host/SASHome), you do not have a programming-only deployment.

When programming_only=true is present in your manifest, only SAS Studio is deployed to the Cloud Foundry Elastic Runtime. Also, only BOSH virtual machines (VMs) for SAS Cloud Analytic Services (CAS) and SAS Foundation are set up.

TIP When you query the VMs, the SAS Foundation machine is identified as (objectspawner).

The other VMs present in a full deployment are not created: SAS Configuration Server (Consul), SAS Data Integration Server (PostgreSQL), SAS Message Broker (RabbitMQ), and so on.

SAS Viya on Cloud Foundry: Backup and Recovery

Backup and Recovery: Overview

Use your Cloud Foundry tools to back up and recover your environment. The following guidelines should be considered when implementing the backup and restore processes:
Scripts that call backup processes for SAS services that are deployed in BOSH (such as Postgres, Consul, and RabbitMQ) can be automated or run in an ad hoc manner.

You can create BOSH errand jobs that run those scripts directly, or you can integrate the backup scripts into other standard processes that provide the backup capabilities for your other BOSH and Cloud Foundry services.

Persistent storage attached to virtual machines managed by BOSH can provide a measure of safety to ensure that data sources that are not specifically handled by the backup utilities can still be retained and recovered.

**Note:** Assets that retain information or the state between CAS sessions or SAS sessions (for example, CAS controls and caslib information) should be backed up on persistent disks. User home directories must also be NFS mounts and capable of being backed up through your organization’s standard persistent disk backup procedures.

### Backup and Recovery: How To

#### Retrieve a Copy of the BOSH Deployment Manifest

You need to retrieve a copy of the running deployment manifest from the BOSH director. This is useful for backup and archival purposes.

1. From the command line, target the BOSH director that hosts your SAS Viya deployment. For example:
   
   ```
   bosh target 10.10.3.3
   ```

2. Run `bosh deployments` to identify the name of your current SAS Viya deployment or deployments.

3. Run BOSH `download manifest <DEPLOYMENT-NAME> <LOCAL-FILE-NAME>` to download and save each BOSH deployment manifest. Copy the manifest file to an archive location for backup purposes.

   Repeat this step for each SAS Viya deployment that you have in the BOSH manifest file.

#### Back Up the SAS Infrastructure Data Server

SAS Viya uses the PostgreSQL relational database as its SAS Infrastructure Data Server. You can use standard PostgreSQL data backup procedures to back up and restore databases that are used by SAS Viya running on Cloud Foundry. For example, you could use the pgAdmin graphical user interface for manual backups, or you can integrate the `pg_dump` utility into scheduled scripts for automatic backups.

**Note:** SAS Viya for Cloud Foundry is shipped with PostgreSQL version 9.4.9.

To back up using the `pg_dump` utility:

- Run `pg_dump` to export the SAS SharedServices database:

  ```
  $ ./pg_dump -h <PGPOOL-IP-ADDRESS> -p <PORT> -U dbmsowner -d SharedServices > /tmp/sas-viya-postgres.sql
  ```

  **TIP** If you choose to run the backup from a VM within the deployment, the `pg_dump` utility resides on the VM containing the sas-bshpostgres-stem-cell-type job in `/var/vcap/packages/sas-postgresql/opt/sas/viya/home/bin`.

When backing up the SAS Infrastructure Data Server, consider the following points:

- You should run a version of `pg_dump` on the archival machine to avoid having to use secure shell to log in to the BOSH VM.
- Use `bosh vms` to view the list of deployed VMs to identify the IP addresses used for the SAS Postgres and pgpool services.
- Make sure that you use the IP address for pgpool and the appropriate port (the default is 5432).
- When prompted for a password during connection, use the `postgres.password` property that is specified in the deployment manifest.
- Archive the exported database file per your organization's standards.

**Back Up the SAS Configuration Server**

SAS Viya uses Consul as its SAS Configuration Server. You can use standard Consul procedures to back up and restore the key/value configuration used by SAS Viya running on Cloud Foundry. You can integrate these backup procedures into your organization's standard archival practices.

Use Consul's KV API to back up the SAS Viya key/value configuration:

```
curl --header "X-Consul-Token: <CONSUL-MANAGEMENT-TOKEN>" \
   "http://<CONSUL-IP-ADDRESS>:8500/v1/kv/?recurse" \n   > sas-viya-kv.json
```

When backing up the SAS Configuration Server, consider the following points:
- Use `bosh vms` to view the list of deployed VMs to identify the IP address that is used for Consul.
- For the `X-Consul-Token` value, use the value of the `consul.tokens.management` property that is specified in the deployment manifest.
- Archive the exported JSON file that contains the key/value configurations per your organization's standards.

**Back Up the SAS Message Broker**

SAS Viya uses RabbitMQ as its SAS Message Broker. You can use standard RabbitMQ processes to back up and restore message broker definitions used by SAS Viya running on Cloud Foundry.

Use RabbitMQ's API to back up the server definitions, including exchanges, queues, bindings, users, virtual hosts, permissions, and parameters:

```
curl http://<RABITTMQ-IP-ADDRESS>:15672/api/definitions -u <CLIENT-USERID>:<CLIENT-PASSWORD> \
   sas-viya-rabbitmq.json
```

When backing up the SAS Message Broker, consider the following points:
- Use `bosh vms` to view the list of deployed VMs to identify the IP address used for RabbitMQ.
- For the `<CLIENT-USERID>` and `<CLIENT-PASSWORD>` values, use the `rabbitmq.client.userid` and `rabbitmq.client.password` property values that are specified in the deployment manifest. If no values are set for those properties, use the default values `sasclient` for the user ID and `sasclientpw` for the password.
- Archive the exported JSON file that contains the server definitions per your organization's standards.

**Restore PostgreSQL Data**

The text file containing SQL that is created by `pg_dump` can be read in by the `psql` utility. To restore a backup of the SAS Infrastructure Data Server:

- Use `psql` to import the SAS SharedServices database:

```
$ ./psql -h <PGPOOL-IP-ADDRESS> -p <PORT> -U dbmsowner -d SharedServices < sas-viya-postgres.sql
```

When restoring PostgreSQL Data, consider the following points:
- You should run `psql` from the archival machine to avoid having to use secure shell to log in to the BOSH VM.
- Make sure that you use the IP address for pgpool and the appropriate port (the default is 5432).

- When prompted for a password during connection, use the `postgres.password` property that is specified in the deployment manifest.

### Restore the Consul Configuration

Use a POST to the Consul's KV API to restore a backup of the SAS Viya key/value configuration:

```
curl --header "X-Consul-Token: <CONSUL-MANAGEMENT-TOKEN>" \
    --request POST "http://<CONSUL-IP-ADDRESS>:8500/v1/kv/<KEY>" --data
```

When restoring the Consul configuration, consider the following points:

- For the `X-Consul-Token` value, use the value of the `consul.tokens.management` property that is specified in the deployment manifest.

- Iterate over the set of keys in the previously exported JSON file and POST the value to the appropriate key.

### Restore the RabbitMQ Definitions

Use a POST to RabbitMQ's API to restore a backup of the SAS Viya message broker definitions:

```
curl -X POST -F "file=@/path/to/sas-viya-rabbitmq.json" \
```

When restoring the RabbitMQ definitions, consider the following points:

- Make sure you post using the `-F` field named `file`.

- For the `CLIENT-USERID` and `CLIENT-PASSWORD` values, use the `rabbitmq.client.userid` and `rabbitmq.client.password` property values that are specified in the deployment manifest. If no values are set for those properties, use the default values `sasclient` for the user ID and `sasclientpw` for the password.

### SAS Viya on Cloud Foundry: Configuration Properties

#### Read This First

Note: Information about SAS Viya configuration properties can be found in *SAS Viya Administration: Configuration Properties*. Any differences specific to the Cloud Foundry platform are described in this section.

#### Create and Edit Configuration Instances (Persistent)

You can persist configuration changes for the SAS Viya services by editing the BOSH manifest and redeploying.

For temporary changes to services and system properties, use *SAS Environment Manager*.

Note: Contact your BOSH administrator for the necessary permissions to access the manifest and to run BOSH.

SAS Viya service configuration properties are specified in the BOSH manifest under the `consul` instance under `config.application`.

Here is an example:
SAS Viya on Cloud Foundry: Encryption

Read This First

Note: Information about encryption can be found in *Encryption in SAS Viya: Data in Motion*. Any differences specific to the Cloud Foundry platform are described in this section.

Overview

SAS provides encryption in two contexts for Cloud Foundry:

- **Data in motion** is data that is being transmitted to another location. Data is most vulnerable while in transit. Sensitive data in transit should be encrypted. You can protect all traffic in transit between servers and clients. This document covers encrypting data in motion.

  Note: Certificates are managed using BOSH and Cloud Foundry.

- **Data at rest** is data stored in databases, file servers, endpoint devices, and various storage networks. This data can be on-premises, virtual, or in the cloud. This data is usually protected in conventional ways by firewalls. Numerous layers of defense are needed, and encrypting sensitive data is another layer. See *Encryption in SAS Viya: Data at Rest*.

When you deploy SAS Viya on Cloud Foundry, the following encryption information applies to the installation:
Certificates used for TLS are managed using BOSH and Cloud Foundry. If you are using the BOSH trusted certificates, any virtual machine started by BOSH will have the certificates installed in the system stores. Contact your security admin to get the certificate information that you need.

SAS does not install HAProxy or configure TLS internally. You can set up TLS for Cloud Foundry at the load balancer, external to the SAS deployment.

Use SAS/CONNECT and configure TLS if you are transferring data between a SAS 9.4 (version prior to SAS 9.4m5) and SAS Viya 3.3 or are using a programming-only deployment of SAS Viya 3.3. See “Import Data Using SAS/CONNECT Secured by TLS” on page 10.

Configure LDAPS. See “Configure SAS Viya to Connect to LDAPS Provider” on page 12.

Note: All discussion of TLS is also applicable to the predecessor protocol, Secure Sockets Layer (SSL).

How To

Import Data Using SAS/CONNECT Secured by TLS

Overview

SAS programming clients in a 9.4M5 environment can call procedures that are enabled in SAS Viya 3.3 and submit DATA step code, operating directly on CAS data sources. As a result, SAS/CONNECT is no longer required as a separate product in order to transfer data from SAS 9.4M5 to SAS Viya 3.3.

However, SAS/CONNECT is required to transfer data from SAS 9.4M4 and earlier deployments to SAS Viya. When you use SAS/CONNECT to import data from SAS 9.4M4 and earlier to SAS Viya, Cloud Foundry acts as the SAS/CONNECT client. The SAS/CONNECT server must be running on the SAS 9.4 machine, and the connection to SAS 9.4 must be initiated from SAS Viya.

When you use SAS/CONNECT, you must secure SAS/CONNECT by configuring TLS.

Sign On to a SAS/CONNECT Spawner Using TLS

Note: These instructions apply to SAS 9.4M4 and earlier deployments and to a SAS Viya 3.3 programming-only deployment.

For SAS 9.4M4 and earlier, SAS/CONNECT is used as a bridge to access data between SAS 9.4 and SAS Viya. You can use TLS to secure that bridge when you sign on to the SAS/CONNECT spawner from the SAS/CONNECT client. The sign-on command starts a SAS/CONNECT server.

In a SAS Viya 3.3 programming-only deployment, you must also use the instructions in this section to configure TLS for SAS/CONNECT.

Certificates used for TLS are managed using BOSH and Cloud Foundry. If you are using the BOSH trusted certificates, any virtual machine started by BOSH has the certificates installed in the system stores. Contact your security administrator to get the certificate information that you need.

Configure TLS for SAS/CONNECT

1. Sign in with administrator privileges to the machine containing the SAS/CONNECT spawner.

2. In the connect_usermods.sh file located in /opt/sas/viya/config/etc/connect/default, set up TLS by adding the SSL encryption options. Edit the connect_usermods.sh file, and add the following encryption options to the USERMODS= line to encrypt the connection for the SAS/CONNECT spawner. Note that this file needs to have global Read permissions: -rw-r--r--

   In the following code example, the names of the certificate file and the private key file are just example names. These would be the names of the files that you placed in the /opt/sas/viya/config directories.

   Note: The options are enclosed in double quotation marks.
The NETENCRYPT option specifies that encryption is required.

The NETENCRYPTALGORITHM= option specifies that the spawner is started using TLS.

The SSLCERTLOC= option specifies the location of a file that contains a digital certificate for the machine’s public key. This is used by the server to send to clients for authentication.

Note:
If the certificate is not self-signed, the file specified by the SSLCERTLOC= option needs to be a certificate chain file that starts with the server identity certificate and includes the signing intermediate CA certificates. The root CA certificate does not need to be included in the certificate chain.

The SSLPVTKEYLOC= option specifies the location of the file that contains the private key that corresponds to the digital certificate that was specified by the SSLCERTLOC= option.

The SSLPVTKEYPASS= option specifies the password that TLS requires to decrypt the private key. The private key is stored in the file that was specified by the SSLPVTKEYLOC= option.

Note: SAS first looks for CA certificates in a file named trustedcerts.pem, located in the /opt/sas/viya/config/etc/SASSecurityCertificateFramework/cacerts directory. Therefore, the SSLCALISTLOC= system option is not required if you are storing your trusted certificates in the default location. However, if you choose not to use the default location to store certificates, you need to specify the SSLCALISTLOC= option with a location for the certificates for the SAS/CONNECT client and spawner.

For each of the preceding examples, the default location is used.

3 Start the SAS/CONNECT spawner.

   sudo service sas-viya-connect-default start

4 The SAS/CONNECT spawner runs the connectserver.sh script, which runs the connectserver_usermods.sh script. The connectserver_usermods.sh script is located in /opt/sas/viya/config/etc/connectserver/default. Edit the connectserver_usermods.sh file, and add the following encryption options to the USERMODS_OPTIONS= line. Note that this file needs to have global Read permissions: -rw-r--r--

   USERMODS_OPTIONS= -netencrypt ssl
tls/certs/Server.crt
private/key
-sslpvtkeypass 'password'

Note: The options are enclosed in double quotation marks.

Note: The certificates specified above are your server certificates.

5 After a spawner is started on a SAS/CONNECT server, a SAS/CONNECT client can connect to it. The following example shows how to connect a client to a spawner that is running on a SAS/CONNECT server:

   options netencrytalgorithm=SSL;
   %let myserver=<myHost.myDomain.com> <port>;
   SIGNON myserver user=sasdemo passwd=password;

   If the spawner requires TLS encryption (NETENCRYPTALGORITHM=SSL), the SAS/CONNECT client needs to locate the root CA certificate to validate the spawner’s certificate. For a LINUX client, SAS first looks for the root CA certificate in the trustedcerts.pem file in /opt/sas/viya/config/etc/
SASSecurityCertificateFramework/default. Otherwise, you need to specify the location of the root CA certificate by using system option SSLCALISTLOC= or environment variable SSL_CERT_DIR= or SSLCACERTDIR=.

For a Windows SAS/CONNECT client, import the trusted root CA certificate into the Windows trusted root certificate store.

For information about SAS system options, see “Reference” in Encryption in SAS Viya: Data in Motion.

Configure SAS Viya to Connect to LDAPS Provider

Note: LDAP is required in a full deployment. It is not required in a programming-only deployment.

Lightweight Directory Access Protocol (LDAP) connections can be established in a TLS session so that all data that is sent between the LDAP client and LDAP server is encrypted. LDAP over TLS is known as LDAPS.

To connect to an LDAPS provider, SAS Viya needs access to the CA certificate used by the LDAPS provider. Certificates are managed using BOSH and Cloud Foundry. If you are using the BOSH trusted certificates, any Virtual Machine started by BOSH would have the certificates installed in the system stores. Contact your security admin to get the certificate information that you need.

Note: Only LDAP-based identity providers are supported. These instructions assume that you have basic familiarity with LDAP administration.

1 Log on to your machine as a user with root, SAS Admin, or sudo privileges.

2 Add your certificates to BOSH.

3 Use the SAS Environment Manager to set the configuration property sas.identities.providers.ldap.connection. Specify an LDAPS port number (by default LDAPS is 636) and specify LDAPS in the url field. You can also use the port value 3269 (Global Catalog) for LDAPS.

   a If the Configuration page of SAS Environment Manager is not already displayed, select Resources ➔ Configuration from the side menu.

   b Select Basic Services from the list, and then select the Identities service from the list of services.

   c In the sas.identities.providers.ldap.connection section, click ➔. In the Edit sas.identities.providers.ldap.connection Configuration window, do the following:

      i Update values for the port field, adding an LDAPS port value. Update the url field to specify LDAPS. For the remaining fields, review the default values and make changes as necessary. The default values are appropriate for most sites.

      ii Click Save.

For additional configuration instructions, see “Consul Settings” in SAS Viya for Cloud Foundry: Deployment Guide. For details about the sas.identities.providers.ldap.connection property, see “Configuration Properties: Reference (Services)” in SAS Viya Administration: Configuration Properties.

4 If needed, restart the SAS Logon Manager service by running the following command:

   sudo service sas-viya-saslogon-default restart

   Note: It might take several minutes to restart SAS Logon Manager.

If needed, restart the Identifies service.

   sudo service sas-viya-identities-default restart
SAS Viya on Cloud Foundry: Licensing

Read This First

Note: Information about SAS Viya configuration properties can be found in SAS Viya Administration: Licensing. Any differences specific to the Cloud Foundry platform are described in this section.

SAS Viya uses a single licensing file. Both SAS Cloud Analytic Services (CAS) and SAS Foundation use the same license.

During installation, a license is applied to both the CAS in-memory compute engine and the SAS Foundation compute engine. You apply a new license to enable new products or to extend expiration dates on existing products.

The contents of the license file resides in the BOSH manifest.

Apply New Licenses

Use BOSH to apply a new SAS license when your current license has expired, or when you are adding new SAS products to your deployment. BOSH applies your new license to the CAS controller and also to SAS Foundation.

1 Move the current license file into a backup location.

2 Using a text editor, open your new SAS license file, and copy its contents into the paste buffer.

   For information about where to locate your new license file and how to identify it, see "Locate My License File" in SAS Viya Administration: Licensing.

3 Open your BOSH manifest file, and locate the line that contains setinit.

4 Replace the previous license (setinit) with the contents of your new license file that you copied in Step 2.

   Note: Make sure that the license contents begins under the x in the word text as shown in the following example.

   ```
   setinit:
   text: |
   PROC SETINIT RELEASE='V03';
   SITEINFO NAME='My Site'
   SITE=12345678 OSNAME='LIN X64' RECREATE WARN=55 GRACE=45
   BIRTHDAY='23JUN2017'D EXPIRE='30SEP2017'D PASSWORD=111111111;
   CPU MODEL=' ' MODNUM=' ' SERIAL=' ' NAME=CPU000;
   CPU MODEL=' ' MODNUM=' ' SERIAL='+9999' NAME=CPU001;
   CPU MODEL=' ' MODNUM=' ' SERIAL='+9999' NAME=CPU002;
   EXPIRE 'PRODNUM000' '18AUG2017'D / CPU=CPU000 CPU001
   CPU002;
   ```

5 Set the BOSH deployment to reference SAS-Viya-manifest.yml.

   ```
   bosh deployment SAS-Viya-manifest.yml
   ```

6 Deploy the software.

   ```
   bosh deploy
   ```

7 Verify that your SAS Foundation license has been renewed by following the steps in "View SAS Foundation License Information" in SAS Viya Administration: Licensing.
Verify that your SAS Cloud Analytic Services license has been renewed by following the steps in “View SAS Cloud Analytic Services License Information” in SAS Viya Administration: Licensing.

Default CAS License Location

The default location for the SAS Cloud Analytic Services (CAS) license on Cloud Foundry is: /var/vcap/packages/cas-dmml/opt/sas/viya/config/etc/cas/default/.

SAS Viya on Cloud Foundry: Monitoring

Read This First

Note: Information about monitoring can be found in SAS Viya Administration: Monitoring. Any differences specific to the Cloud Foundry platform are described in this section.

Monitoring: How to (CAS Server Monitor)

Access CAS Server Monitor

To log on to CAS Server Monitor, open a web browser and enter the URL http://controller-machine:8777 in the address field.

You must have an active CAS Server session in order to access CAS Server Monitor.

For more information, see “Access the Monitor” in SAS Viya Administration: SAS Cloud Analytic Services.

Monitor CAS Process Performance

The CAS processes you can monitor with these steps correspond to SAS server processes. You can separately monitor each session that is started from the CAS server.

1. In CAS Server Monitor, beneath the Cloud Analytic Services banner, click .

2. Select Add View ➔ CAS Process CPU Usage.

   The Process CPU Usage panel on the window displays a set of histograms. There is one histogram for each machine and the corresponding CAS server process. The histogram in the upper left is the CAS controller node. If you are not an administrator, only the histogram for the CAS controller node is displayed.

   Each histogram displays the percentage of CPU usage, from 0 to 100%.

   Use these histograms to note patterns of CPU usage among the CAS nodes.

The **CAS Process Metrics** panel on the window displays a set of histograms. There is one set of three histograms for each machine and the corresponding CAS server process. If you are not an administrator, only the set of histograms for the CAS controller node is displayed.

Each set of histograms displays the percentage of CPU used, amount of resident memory used, and amount of virtual memory used for the CAS process.

4 Click □ if you want to stop metric collection. Click ► to resume collection.

**Monitor CPU Usage for a Session**

1 In CAS Server Monitor, select ▶ on the left side of the window.

2 Select **Add Session View** and select a session.

   The panel for the session displays a set of histograms, with one histogram for each machine in the grid. If you are not an administrator, only the histogram for the CAS controller node is displayed. The top half of the histogram displays the percentage of CPU load used by the session, and the bottom displays the amount of resident memory used for the session.

**Monitor Host Performance**

CAS Server Monitor displays histograms that enable you to view the CPU load and memory usage for all machines in your CAS server. Follow these steps:

1 In CAS Server Monitor, select ▶ on the left side of the window.

2 To view the CPU load, select **Add View ▸ Host CPU Load Average**.

   The **Host CPU Load Average** panel on the window displays a set of histograms. There is one histogram for each machine in the CAS grid. If you are not an administrator, only the histogram for the CAS controller node is displayed.

   Each histogram displays the CPU load on the machine, using the same format as the Linux `xload` command. Each division on the histograms represents one load average point. The highest point on each histogram is displayed to the right of the histogram.
Use these histograms to note usage patterns among the CAS nodes. For example, if you notice that the load on a worker node machine is significantly and consistently higher than the load on other machines, you can use the **Show Processes** function to check for other running processes or defunct processes. See “Monitor Process Information” in SAS Viya Administration: Monitoring for instructions on this function.

3 To view the memory usage, select **Add View ⇒ Host Memory Usage**.

The **Host Memory Usage** panel on the window displays a set of histograms. There is one histogram for each machine in the CAS grid. If you are not an administrator, only the histogram for the CAS controller node is displayed.

Each histogram displays the percentage of memory used on the machine, from 0 to 100%. The percentage of memory used is displayed in green, at the top of the histogram. The percentage of virtual memory used is displayed in orange, at the bottom of the histogram.

Use these histograms to note patterns of memory usage among the CAS nodes. For example, if the memory usage is consistently high on a machine, its memory might need to be increased.

4 Click ❯ if you want to stop metric collection. Click ◀ to resume collection.

**Monitor Process Information**

1 Perform one of these actions in CAS Server Monitor:
   - Select ❯ on the left side of the window and open one of the views from the **Add View** or **Add Session View** menus. Click ◀ to the right of a histogram. Select **Show Processes**.
   - Click ❯ and select the **Nodes** tab. Click ◀ on the right side of a node’s row and select **Show Processes**.

2 The Processes window appears. The window displays this information:
   - Metrics for the selected node, including uptime, number of processes, memory usage, CPU load, and file usage
   - A histogram of the CPU load for the node
   - A table containing the output from the `top` command for the selected node. The output includes metrics such as CPU usage, time, and threads for each process. If you are a SAS administrator, the window displays information about all processes. If you are not a SAS administrator, you can view information about only your own processes.

**Change the Monitoring Display Options**

When you are viewing the histograms in the **Resource Monitor** view in CAS Server Monitor, you can control how the histograms are displayed.
To change how quickly the graph data is refreshed, move the slider next to the **Speed** label.

To change the size of the histograms, move the slider next to the **Size** label.

The default layout for a histogram view is a grid. To change to a single column, click the column icon in the banner for a view. To return to a grid layout, click the grid icon.

To change the default view for the **Resource Monitor** view, select **userid ⇒ Settings** in the upper right of the CAS Server Monitor window. You can select a default monitor view and layout.

---

### SAS Viya on Cloud Foundry: SAS Cloud Analytic Services

#### Read This First

**Note:** Information about SAS Cloud Analytic Services (CAS) can be found in *SAS Viya Administration: SAS Cloud Analytic Services*. Any differences specific to the Cloud Foundry platform are described in this section.

#### Operate

Like the other SAS Viya servers, SAS Cloud Analytic Services runs in a BOSH virtual machine and is operated and managed through BOSH in a typical manner.

For more information, contact your site’s Cloud Foundry administrator.

#### How To

**Adjust Caslib Management Privileges**

Caslib management privileges are stored in the CAS permstore file. For SAS Viya on Cloud Foundry, the default permstore is stored on the BOSH persistent disk. Therefore, the permstore persists when redeploying, as long as the deployment is not deleted before being redeployed with BOSH.

For more information, see:
- adjusting caslib management privileges using [SAS Environment Manager](#)
- adjusting caslib management privileges using [CAS Server Monitor](#)

**Manage CAS Nodes and Terminate CAS Sessions**

**CAUTION!** Some functionality in CAS Server Monitor and SAS Environment Manager should not be used for SAS Viya on Cloud Foundry. Do not attempt to add nodes, remove nodes, or terminate a server instance from CAS Server Monitor or SAS Environment Manager. Instead, use the appropriate BOSH command.

To add additional CAS worker nodes, see “Add CAS Worker Nodes” in SAS Viya for Cloud Foundry: Deployment Guide.

#### Concepts

SAS Cloud Analytic Services (CAS) can be deployed on a cluster of machines. Unlike on native operating systems, SAS Viya on Cloud Foundry does not support CAS co-located with Hadoop.
Reference

CAS Configuration File Options

Usage

On Cloud Foundry, SAS Cloud Analytic Services (CAS) configuration file options are specified in the BOSH manifest under the cas_controller instance under cas.config. The BOSH deployment automatically shares CAS properties from the CAS controller job with the CAS worker jobs.

Note: When specifying a CAS configuration file option, the cas. prefix is not needed. The BOSH deployment process adds the prefix for you.

Here is an example:

```yaml
- name: cas_controller
  instances: 1 # DO NOT CHANGE
  jobs:
    <% if programming_only == false %>
    - {name: consul, release: sas-bshconsul-<%= package_type %>
    <% end %>
    - {name: install_config_nfs, release: sas-bshnfs-<%= package_type %>
    - {name: install_config_sssd, release: sas-bshsssd-<%= package_type %>
    - {name: install_java, release: sas-bshjava-<%= package_type %>
    - {name: install_libpng, release: sas-bshlibpng-<%= package_type %>
    - {name: install_numa, release: sas-bshnuma-<%= package_type %>
    <% if stemcell == "ubuntu" %>
```
- {name: install_packages, release: sas-bshpkginst-<%= package_type %>
<% end %>
- name: cas_controller
  release: sas-bshvdmmmlcas-<%= package_type %>
  provides:
    controller: {as: cas_controller}
  vm_type: <%= vm_type %>
  stemcell: <%= stemcell %>
  persistent_disk_type: <%= disk_type %>
  networks:
    - name: <%= private_network_name %>
      default: [dns, gateway]
    - name: <%= public_network_name %>
      static_ips: [<%= cas_controller_ip %>]
  properties:
    cas:
      workerips: <%= cas_worker_ips %>
      key: <%= cas_key %>
      config:
        gcport: 5580
        mode: <%= cas_mode %>
        <% if programming_only == false %>
        servicesbaseurl: <%= servicesbaseurl %>
        <% end %>
        <% if cas_mode == "mpp" %>
        initialworkers: 1
        <% end %>
        <% end %>

Differences in CAS Configuration File Options Specific to SAS Viya on Cloud Foundry

Here are the CAS configuration file options specific to SAS Viya on Cloud Foundry:

- cas.PERMSTORE

  Here is an example showing the CAS permstore location on Cloud Foundry:

  ```
  cas.permstore=’/var/vcap/store/cas_controller/permstore’
  ```

CAS Environment Variables

Usage

On Cloud Foundry, SAS Cloud Analytic Services (CAS) environment variables are specified in the BOSH manifest under the cas_controller instance under cas.environment. The BOSH deployment automatically shares CAS environment variables from the CAS controller job with the CAS worker jobs.

Note: When specifying a CAS environment variable, the env. prefix is not needed. The BOSH deployment process adds the prefix for you.

Here is an example:

- name: cas_controller
  instances: 1 # DO NOT CHANGE
  jobs:
    <% if programming_only == false %>
    - {name: consul, release: sas-bshconsul-<%= package_type %>
    <% end %>
    - {name: install_config_nfs, release: sas-bshnfs-<%= package_type %>
    - {name: install_config_sssd, release: sas-bshsssd-<%= package_type %>

- {name: install_java, release: sas-bshjava-<%= package_type %>
- {name: install_libpng, release: sas-bshlibpng-<%= package_type %>
- {name: install_numa, release: sas-bshnuma-<%= package_type %>

<% if stemcell == "ubuntu" %>
- {name: install_packages, release: sas-bshpkginst-<%= package_type %>
<% end %>

- name: cas_controller
  release: sas-bshvdmmlcas-<%= package_type %>
  provides:
    controller: {as: cas_controller}
  vm_type: <%= vm_type %>
  stemcell: <%= stemcell %>
  persistent_disk_type: <%= disk_type %>
  networks:
    - name: <%= private_network_name %>
      default: [dns, gateway]
    - name: <%= public_network_name %>
      static_ips: <%= cas_controller_ip %>
  properties:
    cas:
      workerips: <%= cas_worker_ips %>
      key: <%= cas_key %>

```environment:
  CAS_DISK_CACHE: /var/vcap/store/cas_disk1:/var/vcap/store/cas_disk2:/var/vcap/store/cas_disk3
```

config:
  gcport: 5580
  mode: <%= cas_mode %>

<% if programming_only == false %>
  servicesbaseurl: <%= servicesbaseurl %>
<% end %>

<% if cas_mode == "mpp" %>
  initialworkers: 1
<% end %>

Differences in CAS Environment Variables Specific to SAS Viya on Cloud Foundry

Here are the CAS environment variables specific to SAS Viya on Cloud Foundry:

- **env.CAS_INSTALL**
  
  Here is an example showing the CAS installation directory on Cloud Foundry:

  ```
  env.CAS_INSTALL="/var/vcap/packages/cas-dmml/opt/sas/viya/home/SASFoundation"
  ```

- **env.CAS_LICENSE**
  
  Here is an example showing the CAS license location on Cloud Foundry:

  ```
  env.CAS_LICENSE="/var/vcap/packages/cas-dmml/opt/sas/viya/config/etc/cas/default/license.sas"
  ```
SAS Viya on Cloud Foundry: Servers and Services

Read This First

Information about SAS Viya servers and services can be found in the following documents. Any differences specific to the Cloud Foundry platform are described in this section.

- SAS Viya Administration: General Servers and Services
- SAS Viya Administration: Programming Run-Time Servers
- SAS Viya Administration: Infrastructure Servers

Operate

Servers

Like typical BOSH applications, SAS Viya servers also run on BOSH virtual machines and are operated and managed through BOSH.

Note:
Whenever you restart the SAS Viya servers, you must also restart the SAS Viya services.

For more information, contact your site’s Cloud Foundry administrator.

Services

SAS Viya services run in the Cloud Foundry Elastic Runtime.

Sign in to your Cloud Foundry secure administrative host (jump server) from where you can run the necessary Cloud Foundry command-line interface (cf CLI) commands to stop, start, and restart SAS Viya services.

To see the complete list of SAS Viya services follow the initial steps in “Edit Configuration Instances” in SAS Viya Administration: Configuration Properties.

To restart all SAS Viya services, run the following command from your jump server:

```
for i in $(cf a | awk '{print $1}' | tail -n +5); do cf restart ${i}; done
```

For more information, consult with your site’s Cloud Foundry administrator.

Add Service Instances

Although SAS Viya on Cloud Foundry does not support multiple instances of servers running on the BOSH director, you can add multiple instances of services that run on the Elastic Runtime.

Note: Any changes to applications that are not included in the manifest are lost the next time you redeploy with BOSH.

Sign in to your Cloud Foundry secure administrative host (jump server) from where you can run the following command: `cf scale application-name -i number-of-instances`.

For more information about how to use the Cloud Foundry command-line interface (cf CLI), see your Cloud Foundry documentation.
To add additional CAS worker nodes, see “Add CAS Worker Nodes” in SAS Viya for Cloud Foundry: Deployment Guide.

---

## SAS Viya on Cloud Foundry: Troubleshooting

### SAS Studio appears to be unresponsive.

**Explanation:**
Performing a BOSH `recreate` on the CAS controller while a CAS session is still running might be the cause.

**Resolution:**
SAS Studio eventually responds.

In the future, stop all CAS sessions before issuing the BOSH `recreate` command.

**ERROR:** Contact your SAS Installation Representative to obtain your updated SAS Installation Data (SID) file, which includes SETINIT information.

**Explanation:**
Your SAS Viya license has expired.

**Resolution:**
Follow the steps in “Apply New Licenses” on page 13.

### Stopping and restarting BOSH VMs.

**Explanation:**
When the SAS Viya servers running in the BOSH virtual machines (VMs) are shut down and restarted, several processes are not able to properly initialize.

**Resolution:**
Stop and restart the following SAS Viya servers and services in this sequence:

1. Stop SAS Cache Server:
   ```
   bosh stop geode-cacheserver 0 --force
   ```
2. If the following services are running, stop them:
   - saslogon
   - search
   - searchindex
   - monitoring
   ```
   cf stop SASLogon-app-name
   cf stop search-app-name
   cf stop searchindex-app-name
   cf stop monitoring-app-name
   ```

   **TIP** To determine the correct app name for each service, run the following command: `cf apps | egrep “SASLogon|search|searchIndex|monitoring”`.

3. Make sure that SAS Cache Locator is running:
- `bosh ssh geode-locator 0`
- `sudo su`
- `monit status`

4 Verify that the process `cachelocator` has a status of `running`.

5 Start `sas-cacheserver`:
   ```
   bosh start geode-cacheserver 0 --force
   ```

6 Make sure that all the VMs are running:
   ```
   bosh vms
   ```

7 Verify that all the VMs have a status of `running`.

8 Start the services that you stopped in Step 2.
   ```
   cf start SASLogon-app-name
   cf start search-app-name
   cf start searchindex-app-name
   cf start monitoring-app-name
   ```

9 Make sure that the services that you started in Step 8 are actually running:
   ```
   cf app SASLogon-app-name
   cf app search-app-name
   cf app searchindex-app-name
   cf app monitoring-app-name
   ```

10 Verify that each service has a status of `started`.

11 Run the following commands to fix SAS Studio start failures:
   ```
   bosh recreate object_spawner --force
   bosh recreate cas_controller --force
   bosh recreate cas_worker --force
   ```

ERROR: File was not found. File =/var/vcap/packages/cas-dmml/opt/sas/viya/config/etc/SASSecurityCertificateFramework/private/cas/shared/default/encryption.key. System Error Code = 2.

Explanation:
This error is expected. It does not impact the running of the system as TLS is not turned on.

Resolution:
You can safely ignore this error.

ERROR: An exception has been encountered.
Please contact technical support and provide them with the following traceback information:
The SAS task name is [sasxkern]
Segmentation Violation
Traceback of the Exception:
/var/vcap/data/packages/sas-workspace/...
...

Explanation:
The SAS Object Spawner fails to start and generates errors in various logs.
Resolution:
This can occur intermittently. Using BOSH, perform a recreate of the object spawner VM and the errors will resolve.

ADD NEW CASLIBS (INFO): **User must be a member of the SASAdministrators group**
Enter credentials for https://my_machine.example.com:
Login failed. Bad userid or password.
ADD NEW CASLIBS (ERROR): Failed to login as sasboot.
CAS UPDATE (ERROR): Unable to update caslibs controls

Explanation:
The script that is upgrading caslib access controls is not using the correct TLS certificates, and CAS server validation fails.

Resolution:
To use the correct certificates, you must define the SSL_CERT_FILE environment variable for the executing script. Define SSL_CERT_FILE for the pre_deploy_script property in your BOSH manifest file.

Here is an example:

```bash
name: cas_controller
  ...
  ...
  properties:
    pre_deploy_script: |
      #!/bin/bash
      sed -i-e '/# constants/a SSL_CERT_FILE=\path-to-system-trust-store\' /
      /var/vcap/jobs/cas_controller/bin/add_new_caslib_controls.sh
```

For Ubuntu stem cells, the path to the system truststore is typically /etc/ssl/cert/cacertificates.crt. For CentOS stem cells, the path to the system truststore is typically /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem.