SAS® Viya® 3.3 for Cloud Foundry: Deployment Guide
Contents

Chapter 1 / Introduction ................................................................. 1
  About This Guide ................................................................. 1
  What Gets Deployed ............................................................ 1
  Contact SAS Technical Support ............................................. 2

Chapter 2 / System Requirements .................................................. 3
  Virtual Infrastructure Requirements ......................................... 4
  Requirements for the Installation Machine ............................... 5
  Virtual Machine and Platform Specifications ............................ 5
  Java Requirements ................................................................ 6
  Data Source and Storage Requirements .................................... 6
  User and Group Requirements ............................................... 9
  Security Requirements ......................................................... 9
  Client Requirements ............................................................ 10

Chapter 3 / Pre-Installation Tasks .................................................. 13
  Obtain the Required Files .................................................... 13
  Download the SAS Viya BOSH Releases .................................... 13
  Collect Pre-Deployment Information ....................................... 14

Chapter 4 / Installing SAS Viya ..................................................... 17
  Upload Releases to the BOSH Director ...................................... 17
  Edit the BOSH Deployment Manifest ...................................... 18
  Use BOSH to Install ............................................................. 19
  Connect to Hadoop ............................................................... 19

Chapter 5 / Manual Configuration .................................................. 23
  Configure Your Environment with SAS Environment Manager .... 23
  Change the Administrative User Password for SAS Message Broker 27

Chapter 6 / Validating the Deployment ........................................... 29
  Validating the Cloud Foundry Deployment ............................... 29
  Log On to SAS Studio ........................................................... 30
  Access CAS Server Monitor ................................................... 30
  Verify SAS Infrastructure Data Server .................................... 30
  Verify SAS Message Broker ................................................. 32

Chapter 7 / Uninstalling SAS Viya .................................................. 33
  Uninstall the Deployment ...................................................... 33

Chapter 8 / Managing Your Software ............................................. 35
  Overview ........................................................................... 35
  Update Your Software .......................................................... 36
  Upgrade Your Software ......................................................... 37

Chapter 9 / Next Steps ................................................................. 41
  Refer to Additional Documentation ........................................ 41

Appendix 1 / BOSH Deployment Manifest Information .................... 43
  Configure a Single Network .................................................... 43
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove a Stemcell</td>
<td>43</td>
</tr>
<tr>
<td>Differentiate Multiple SAS Environments</td>
<td>44</td>
</tr>
<tr>
<td>Add CAS Worker Nodes</td>
<td>44</td>
</tr>
<tr>
<td>Define Persistent Disks</td>
<td>45</td>
</tr>
<tr>
<td>Ports</td>
<td>46</td>
</tr>
<tr>
<td>Consul Settings</td>
<td>47</td>
</tr>
<tr>
<td>Integrate with Secure Hadoop through Kerberos</td>
<td>48</td>
</tr>
<tr>
<td>Identify a CAS Administrative User</td>
<td>50</td>
</tr>
<tr>
<td>Set the CAS Data Directory</td>
<td>51</td>
</tr>
<tr>
<td>CAS Settings</td>
<td>51</td>
</tr>
<tr>
<td>Establish Communication Between the SAS Embedded Process and CAS Worker Nodes</td>
<td>51</td>
</tr>
<tr>
<td>NFS Mount Options</td>
<td>52</td>
</tr>
<tr>
<td>Security Settings</td>
<td>53</td>
</tr>
<tr>
<td>Apply the Setinit</td>
<td>53</td>
</tr>
</tbody>
</table>
Introduction

About This Guide

Use this guide to deploy SAS Viya in your environment.

- The contents of this document are subject to continual updates. Make sure that you have the latest version of this document, which is available from the SAS Viya Install Center.
- To use this guide successfully, you should have a working knowledge of BOSH and Cloud Foundry.
- Unless another situation is specifically cited, the information in this guide pertains to the software that you ordered.

What Gets Deployed

Products and Supporting Components

This guide provides information for deploying the following products and supporting components:

- SAS Visual Analytics
- SAS Visual Statistics
- SAS Visual Data Mining and Machine Learning
- SAS Cloud Analytic Services (CAS), which is the analytics and license server for SAS Viya
- SAS Studio, a web application that provides the graphical user interface for users to submit actions and code
- SAS/CONNECT, which is used to integrate SAS Viya with a SAS 9.4 (pre-M5) environment
- SAS/ACCESS to Hadoop (on SAS Viya), which enables serial processing between CAS and Hadoop
- SAS In-Database Technologies for Hadoop (on SAS Viya), which enables parallel processing between CAS and Hadoop
If your order includes SAS In-Database Technologies for Hadoop, you should also receive an order for SAS Viya for Linux. For details about connecting SAS Viya for Cloud Foundry and Hadoop, see “Connect to Hadoop” on page 19.

SAS/ACCESS to PC Files (on SAS Viya)

Note: Your license determines which software is enabled for use after deployment.

Deployment and User Interface Options

By default, a deployment installs the full suite of products and user interfaces that you ordered. In the SAS documentation, this type of deployment is referred to as a full deployment.

Although SAS recommends a full deployment, you can deploy using a programming-only option. A programming-only deployment includes SAS Studio, but it does not include the visual user interfaces that business and data analysts might prefer. Also, understand that a programming-only deployment does not include SAS Home, SAS Environment Manager, and the complete suite of services that are included with a full deployment. Therefore, make sure that you are providing your users with the features that they require.

Note: The option to deploy a programming-only environment is provided in the sample BOSH deployment manifest.

Contact SAS Technical Support

Technical support is available to all customers who license SAS software. However, we encourage you to engage your designated on-site SAS support personnel as your first support contact. If your on-site SAS support personnel cannot resolve your issue, have them contact SAS Technical Support to report your problem.

Before you call, explore the SAS Support website at support.sas.com/techsup/. This site offers access to the SAS Knowledge Base, as well as SAS communities, Technical Support contact options, and other support materials that might answer your questions.

When you contact SAS Technical Support, you are required to provide information, such as your SAS site number, company name, email address, and phone number, that identifies you as a licensed SAS software customer.
# System Requirements

**Virtual Infrastructure Requirements**
- Overview of Cloud Infrastructure Requirements ........................................... 4
- Runtime Environment ......................................................................................... 4
- Orchestration Requirements ............................................................................... 4
- Stemcell Requirements ....................................................................................... 4
- Network Requirements ......................................................................................... 5
- SAS Support for Alternative Operating Systems .................................................... 5

**Requirements for the Installation Machine** .................................................. 5

**Virtual Machine and Platform Specifications** ............................................. 5
- Requirements for VMs Deployed by BOSH for Supporting Components ........... 5
- Requirements for Resources Allocated for Applications within the Elastic Runtime 6

**Java Requirements** ...................................................................................... 6

**Data Source and Storage Requirements** ..................................................... 6
- Overview of Data Warehouse and Storage Requirements .................................. 6
- Supported Data Sources ....................................................................................... 7
- Hadoop Requirements ........................................................................................ 7
- Requirements to Import Data from SAS 9.4 ...................................................... 8
- Requirements for SAS/ACCESS Interface to Hadoop ....................................... 8
- Requirements for SAS In-Database Technologies for Hadoop ......................... 8
- Requirements for SAS/ACCESS Interface to PC Files .................................... 8

**User and Group Requirements** .................................................................. 9
- User Account Requirements ............................................................................... 9

**Security Requirements** ............................................................................... 9
- Security Options .................................................................................................. 9
- LDAP Server Requirements ............................................................................... 10

**Client Requirements** ................................................................................ 10
- Web Browsers for SAS Viya User Interfaces ..................................................... 10
- Mobile Platform Support .................................................................................... 10
- Database Drivers ................................................................................................ 11
- Screen Resolution ............................................................................................... 11
Virtual Infrastructure Requirements

Overview of Cloud Infrastructure Requirements
SAS Viya for Cloud Foundry has been tested by SAS on Cloud Foundry running on OpenStack and on Amazon Web Services (AWS).

Note: Based on the Cloud Foundry Platform as a Service (PaaS) Certification program, SAS Viya offerings will run on Cloud Foundry Certified Platforms and Cloud Foundry Open Source Software (CF-OSS) IaaS environments that meet the minimum requirements outlined in this document. For more information about the Cloud Foundry Certified Programs, see https://www.cloudfoundry.org/certified-platforms/.

Runtime Environment
SAS Viya requires version 253 of the Cloud Foundry Elastic Runtime environment. This framework provides application hosting, routing, authentication, service brokers, and messaging. It is installed along with the Cloud Foundry 253 package.

To find out the current Cloud Foundry and BOSH releases that are running in your environment, the Cloud Foundry BOSH administrator can run the following command:

```
bosh releases
```

Orchestration Requirements
BOSH Director is required in order to install SAS Viya components. BOSH Director provides cloud orchestration and management, including VM creation, deployment, and software updates. Because SAS Viya deployment uses BOSH v2 manifests, BOSH v255.4 or later is required. SAS has tested with BOSH Director 263.2.0.

If your organization’s Cloud Foundry environment uses both BOSH v1 and BOSH v2 deployment manifests, BOSH v257 or later is required.

Stemcell Requirements
SAS Viya requires one of the following types of stemcells in order to run in BOSH:

- For Ubuntu: Ubuntu Trusty 3468.22 is required. The following stemcells have been validated:
  - Amazon Web Services Xen-HVM
  - OpenStack KVM
- For CentOS: CentOS 3468.22, based on CentOS 7.3, is required.
  Stemcells that are expected to be issued in the future based on CentOS versions that are later than 7.3 might not work.
  The following stemcells have been validated:
  - Amazon Web Services Xen-HVM
  - OpenStack KVM
Network Requirements

You can set a name for the private network in the BOSH cloud-config section of the BOSH deployment manifest. The default name for the externally visible network for a SAS BOSH deployment is `public`. To change the name, you must define the property, `network.external.name`, in your BOSH deployment manifest. Its value will be the name of your preferred VIP network. This property should apply to all SAS VMs that are managed by BOSH.

Note: Do not use a value of `test` for the `network.external.name` property.

SAS Support for Alternative Operating Systems

SAS provides support on a limited basis for alternative operating system distributions that customers might select. For more information, see the official support policy statement at [http://support.sas.com/techsup/pcn/altopsys.html](http://support.sas.com/techsup/pcn/altopsys.html).

Requirements for the Installation Machine

When you order SAS software, SAS sends a Software Order Email (SOE) to your business or organization that includes information about the software order and some installation file attachments. You are instructed to save those files on a local machine before you start the deployment process.

Make sure that at least 40 GB of free space is available in the target directory before you run the script `get-sas-viya-bosh-releases.sh`. By default, the script downloads the content from SAS secure repositories to the current working directory.

Virtual Machine and Platform Specifications

Virtual machine requirements are typically dependent on the number of users who access the SAS Viya environment and the amount of data that is imported and analyzed. On SAS Viya for Cloud Foundry, requirements also depend on whether you are installing a full deployment or a programming-only deployment. Also, requirements for VMs that are deployed by BOSH are different from the requirements for resources that are dynamically allocated for applications within the Elastic Runtime. Cloud Foundry refers to VMs that are deployed by BOSH as component VMs. The Elastic Runtime runs on a host VM.

The following table lists minimal requirements for the component VMs that are deployed by BOSH. These VMs support both the Cloud Foundry deployment and the internal components that are required by SAS Visual Analytics, SAS Visual Statistics, and SAS Visual Data Mining and Machine Learning. An example of an internal component that is required by SAS Visual Data Mining and Machine Learning is a PostgreSQL database.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Programming-Only Deployment</th>
<th>Full Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMs</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>This minimum value assumes that a single CAS worker is defined.*</td>
<td>This minimum value assumes that a single CAS worker is defined.*</td>
</tr>
<tr>
<td>VCPUs</td>
<td>2 cores per VM</td>
<td>2 cores per VM</td>
</tr>
</tbody>
</table>

*This minimum value assumes that a single CAS worker is defined.*
<table>
<thead>
<tr>
<th>Resource</th>
<th>Programming-Only Deployment</th>
<th>Full Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>2 GB per VM</td>
<td>2 GB per VM</td>
</tr>
<tr>
<td>Disk Space</td>
<td>20 GB per VM</td>
<td>20 GB per VM</td>
</tr>
</tbody>
</table>

Note: The minimum disk space requirement is 40 GB on the VM that is created for package compilation.

The values in the following table apply to resources that are required for SAS Viya applications, particularly microservices, within the Elastic Runtime:

<p>| Table 2.2 Requirements for Resources Allocated for Applications within the Elastic Runtime |
|-----------------------------------------------|-----------------------------------------------|</p>
<table>
<thead>
<tr>
<th>Resource</th>
<th>Programming-Only Deployment</th>
<th>Full Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>1</td>
<td>92</td>
</tr>
<tr>
<td>RAM</td>
<td>2 GB</td>
<td>104 GB, or 2 GB per application</td>
</tr>
<tr>
<td>Disk Space</td>
<td>2 GB</td>
<td>104 GB, or 2 GB per application</td>
</tr>
<tr>
<td>URLs Reserved</td>
<td>1</td>
<td>51</td>
</tr>
</tbody>
</table>

* You can add more CAS workers by editing the BOSH deployment manifest. For more information, see “Add CAS Worker Nodes” on page 44.

### Java Requirements

The Java Runtime Environment (JRE) must be available in your deployment. Only the JRE is required. The full JDK is not required. However, SAS provides a recent release of the OpenJDK JRE 1.8.x in its BOSH releases.

You have the option to provide your own JRE in a custom BOSH release or in a custom stemcell. SAS Viya supports Oracle JRE SE version 1.8.x. SAS Viya supports some alternative distributions of the JRE, such as Azul Systems Zulu, as long as the version matches the one that is listed on the SAS Support website. However, the IBM SDK, Java Technology Edition is not supported.

For a list of supported JRE distributions and other requirements, see: https://support.sas.com/en/documentation/third-party-software-reference/viya/support-for-jre.html

SAS recommends that you use the most recent release of JRE 1.8.x in order to receive the latest security and bug fixes.

### Data Source and Storage Requirements

#### Overview of Data Warehouse and Storage Requirements

Additional software is required in order to facilitate data retrieval from a Hadoop data store. Depending on your Hadoop environment, you might also install a SAS/ACCESS product or a SAS In-Database Technology bundle on your CAS controller and CAS workers.
If your order for SAS Viya on Cloud Foundry included a SAS/ACCESS product, refer to the corresponding section for additional system requirements that apply to the CAS controller and CAS workers.

If your order included SAS/ACCESS Interface to Hadoop or SAS In-Database Technologies for Hadoop, you should also have received a Software Order Email (SOE) for SAS Viya on Linux. Installation and configuration steps for Hadoop support are documented in the deployment guide that is provided as a link in the SOE.

**Supported Data Sources**

SAS Viya supports the following external data sources, which require a SAS/ACCESS product or an optional SAS In-Database technology bundle to support parallel execution:

- Apache Hive
- PC files

SAS Viya also supports the following data sources, which use data connectors that are automatically included with CAS and are not separately licensed or configured:

- SAS/ACCESS to Hadoop
- LASR Analytic Server (SAS 9.4)
- SAS Scalable Performance Data Engine (SPDE)
- SAS Data Sets

SAS Viya also supports CSV files, which do not require a data connector and can be accessed directly.

A PostgreSQL database is also used as an internal data store, named SAS Infrastructure Data Server. It is based on PostgreSQL version 9 and is configured specifically to support SAS software by storing user content and preferences.

**Hadoop Requirements**

**Supported Releases of Hadoop Distributions**

SAS Viya supports multiple third-party distributions of Hadoop.

*Note:* If you upgrade your Hadoop version and have already deployed SAS Viya with SAS/ACCESS, then you must perform steps to redeploy SAS Viya with Hadoop. For more information, see [SAS Note 60118](https://support.sas.com/en/documentation/third-party-software-reference/viya/support-for-databases.html).

For the full list of supported Hadoop distributions, see: [SAS Note 60118](https://support.sas.com/en/documentation/third-party-software-reference/viya/support-for-databases.html).

You can connect to data as follows:

- For SAS/ACCESS to Hadoop, the SAS/ACCESS Interface to Hadoop or SAS In-Database Technologies for Hadoop must be installed.
- SAS/ACCESS to Hadoop and other SAS/ACCESS products have individual system requirements, which are documented below.

*Note:* Apache Hadoop 0.23, 2.4.0, and 2.7.1 and later versions require additional configuration for access to SAS/ACCESS on HDFS. Refer to the separate [SAS Viya 3.3: Deployment Guide](https://support.sas.com/en/documentation/third-party-software-reference/viya/support-for-databases.html) for Hadoop for instructions.
SAS Support for Alternative Releases of Hadoop Distributions

SAS identifies the specific set of Hadoop distributions that are supported with each SAS product release. The SAS policy that applies to alternative releases or distributions of Hadoop is documented on support.sas.com. The same policy that applies to SAS 9.4 also applies to SAS Viya.

Requirements to Import Data from SAS 9.4

For SAS 9.4 deployments that are earlier than SAS 9.4 TS1M5 (SAS 9.4M5), SAS/CONNECT is required in the environment in order to transfer data from other SAS deployments and operating systems to SAS Viya.

By contrast, SAS 9.4M5 is integrated with SAS Viya directly. As a result, SAS/CONNECT is no longer required in order to transfer data from SAS 9.4M5. All SAS programming clients in a 9.4M5 environment can call procedures that are enabled in SAS Viya and submit DATA step code, operating directly on CAS data sources. Examples of SAS programming clients are SAS Studio, SAS Enterprise Guide, SAS Data Integration Studio, and SAS Data Management Studio.

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.

SAS/CONNECT is not included with a standard SAS Viya order, and must be separately licensed.

When you use SAS/CONNECT to import data from releases prior to SAS 9.4M5 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.

Requirements for SAS/ACCESS Interface to Hadoop

SAS/ACCESS Interface to Hadoop (on SAS Viya) includes SAS Data Connector to Hadoop.

For information about supported Hadoop versions and additional requirements, see:

Requirements for SAS In-Database Technologies for Hadoop

SAS In-Database Technologies for Hadoop (on SAS Viya) includes SAS Data Connect Accelerator for Hadoop.

For information about supported Hadoop versions and additional requirements, see:

Requirements for SAS/ACCESS Interface to PC Files

SAS/ACCESS Interface to PC Files (on SAS Viya) includes SAS Data Connector to PC Files.

SAS/ACCESS Interface to PC Files enables access to the following file formats:

- .jmp
- .spss
- .stata
- .xlsx or .xls

No additional software is required.
User and Group Requirements

User Account Requirements

A few user accounts are required in order to install SAS Viya and to run the software after the deployment has completed. The topics in this section describe the requirements that apply to user accounts for a full deployment or for a programming-only deployment. A full deployment is recommended. In a full deployment, prepare accounts for both programmers and non-programmers in order to access all user interfaces.

Accounts for a Full Deployment

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

End users of SAS Viya applications will use SAS Environment Manager. The following requirements apply to these user accounts:

- Each user must be able to authenticate to your LDAP provider.
- If you plan to configure front-end single sign-on (SSO), make sure that each user can authenticate to the associated provider. This is an additional requirement rather than a replacement for the preceding requirement.
- Any user of the visual interface who also wants to authenticate to SAS Studio must also have a valid host account on the SAS Studio host. In addition, the passwords for these accounts must match.

Accounts for a Programming-only Deployment

Programmers will not log on to SAS Environment Manager. Instead, they will log on to SAS Studio. SAS Studio uses pluggable authentication modules (PAM) and host (operating system) accounts for authentication. PAM is configured automatically by the SSSD release that is included with SAS Viya for Cloud Foundry.

The following additional factors apply to the users in a programming-only deployment:

- The accounts that exist only on your LDAP server cannot log on to SAS Studio by default.
- Each SAS Studio user must have a valid host account for the VM on which the SAS Studio web application runs.
- SAS Studio users also require an LDAP account in order to access CAS. The passwords must match.
- Each user must log on with an account that has a home directory. SAS Studio requires home directories.

Security Requirements

Security Options

SAS Viya for Cloud Foundry includes a BOSH release that configures the System Security Services Daemon (SSSD) to integrate with the identity and authentication provider at your organization. Other methods are also supported for integration with an authentication provider. The sample BOSH deployment manifest provides guidance for setting the required SSSD properties in your BOSH deployment manifest. For more information, see “Security Settings” on page 53.
SAS Viya supports AES encryption for stored data tables and for files in SASHDAT format. You can enable encryption after the deployment has completed. For more information about configuring security settings, see the Encryption section of SAS Viya for Cloud Foundry: Operations.

For transmitted data, you can set up Transport Layer Security (TLS) at the load balancer. You use TLS to secure data transmissions that use SAS/CONNECT for client/server communication.

**Note:** The deployment does not support TLS for internal communication flows.

Certificates that are used for TLS are managed using BOSH and Cloud Foundry. If you are using BOSH trusted certificates, the certificates are automatically installed in the system stores for any VM that is started by BOSH. Contact your security administrator for the required certificate information.

Because the communication flow that is internal to the SAS deployment uses HTTP, make sure that you allow port 80 at the proxy server, but that you block port 80 at the firewall.

**LDAP Server Requirements**

LDAP is required for the visual interface. It is not required in a programming-only deployment.

To support the visual interface, SAS Viya must have Read access to your LDAP provider. To bind to the LDAP server, SAS Viya requires a userDN and password. LDAP anonymous binding is not supported.

LDAPS is supported, but the required certificates are not configured automatically by the deployment. For more information, see SAS Viya for Cloud Foundry: Operations.

You can supply LDAP information in the BOSH deployment manifest. Manifest settings include values that add the LDAP configuration information based on your organization’s requirements. For more information, see "Consul Settings" on page 47.

**Client Requirements**

End users can access the product user interfaces for SAS Viya applications from a desktop computer, using one of the supported web browsers. Because SAS software is not installed on this computer, the requirements are minimal. UNIX and 64-bit Windows operating systems are supported.

**Web Browsers for SAS Viya User Interfaces**

End users can access the product user interfaces for SAS Viya applications from a desktop computer, using a supported web browser. Because SAS software is not installed on this computer, the requirements are minimal. UNIX and 64-bit Windows operating systems are supported.

Some SAS Viya user interfaces include some advanced features that require recent versions of popular web browsers. For information about supported web browsers and the corresponding platforms to access SAS user interfaces, see https://support.sas.com/en/documentation/third-party-software-reference/viya/support-for-web-browsers.html.

**Mobile Platform Support**

Support for mobile devices is not yet available for all SAS Viya user interfaces. For information about mobile device support, see https://support.sas.com/en/documentation/third-party-software-reference/viya/support-for-web-browsers.html.
Database Drivers
Make sure that each client where users will access SAS software has the required database drivers already installed.

Screen Resolution
The minimum screen resolution for each client machine that will access the SAS Viya user interfaces is 1280 x 1024.
Pre-Installation Tasks

Obtain the Required Files

When you order SAS software, SAS sends a Software Order Email (SOE) to your business or organization that includes information about the software order. The SOE directs you to save its attached TGZ file and the license file to a directory on your local machine. If you have not already done so, you must save those files before performing any of the steps in this section.

In the same directory where you have saved the TGZ file, unpack the file.

```bash
tar xf SAS_Viya_CloudFoundry.tgz
```

A `sas_viya_cloudfoundry` subdirectory is added. It contains the following files:

- the license file
- the `entitlement_certificate.pem` and `SAS_CA_Certificate.pem` files
- the `get-sas-viya-bosh-releases.sh` file
- the `sas-viya-vdmml-sample-manifest.yml` file, which is a sample BOSH deployment manifest

Download the SAS Viya BOSH Releases

1. Run the `get-sas-viya-bosh-releases.sh` script to download the BOSH releases from the SAS repository.

   The following files are then available in your local directory:

   **Note:** Even though the BOSH release names contain "redhat", the releases can also be used in a deployment on CentOS stemcells. Red Hat Enterprise Linux is not supported in this release of SAS Viya for Cloud Foundry.

   **Note:** If you run the `get-sas-viya-bosh-releases.sh` script after your initial deployment, you will receive any available updates for the following files.

   - `sas-bshconsul-redhat.xxx.tgz`
   - `sas-bshgeode-redhat.xxx.tgz`
   - `sas-bshjava-redhat.xxx.tgz`
The BOSH releases are downloaded to subdirectories for Ubuntu and Red Hat releases, as appropriate.

2 Copy or move the releases to a location that is accessible by the BOSH Director.

---

**Collect Pre-Deployment Information**

You need to collect specific information before you create or modify the BOSH deployment manifest.

1 Obtain the UUID for your BOSH Director.

   ```
   bosh status --uuid
   ```

2 Review the settings in your organization’s BOSH cloud config file. The BOSH deployment manifest that you edit requires information from that source.

   ```
   bosh cloud-config
   ```

3 Obtain the available IP addresses from your organization's infrastructure-as-a-service (IaaS). If your deployment uses a CAS server in SMP mode, then your deployment requires a minimum of 8 IP addresses. If your deployment uses a CAS server in MPP mode, then your deployment requires an additional IP address.
for each CAS worker that you intend to deploy. Additional IP addresses are needed if you increase the number of instances of any component.

4 Review the target Cloud Foundry org and space to which you intend to deploy the SAS Viya microservices and apps. You must know the API endpoint, the org and space, and the user ID and password for an administrator in that org.

5 Define a host and domain for use as the route to the SAS Viya microservices and apps. For example, if you use sas-viya as the host and sas.mycompany.com as the domain, the route would be sas-viya.sas.mycompany.com.
Installing SAS Viya

Upload Releases to the BOSH Director

Ensure that the BOSH Director is set as the target.

```
bosh target URL-of-BOSH-Director
```

SAS Viya for Cloud Foundry includes BOSH releases for both Ubuntu and CentOS (Red Hat) stemcells. Decide which releases to upload based on the stemcell type that your organization prefers. Upload those releases with the following commands:

**Note:** For `package-type` in the following commands use `ubuntu` for Ubuntu-based releases, and `redhat` for CentOS-based releases. Replace “xxx” with the date stamp that is specified in the release filename.

```
bosh upload release sas-bshconsul-package-type.xxx.tgz
bosh upload release sas-bshgeode-package-type.xxx.tgz
bosh upload release sas-bshjava-package-type.xxx.tgz
bosh upload release sas-bshlibpng-package-typee.xxx.tgz
bosh upload release sas-bshnfs-package-type.xxx.tgz
bosh upload release sas-bshnuma-package-type.xxx.tgz
bosh upload release sas-bshpgpool-package-type.xxx.tgz
bosh upload release sas-bshpostgres-package-type.xxx.tgz
bosh upload release sas-bshrabbitmq-package-type.xxx.tgz
bosh upload release sas-bshsssd-package-type.xxx.tgz
bosh upload release sas-bshvdmmlcas-package-type.xxx.tgz
bosh upload release sas-bshvdmmlmic-package-type.xxx.tgz
bosh upload release sas-bshvdmmlsas-package-type.xxx.tgz
```

If you have chosen to deploy using Ubuntu stemcells, upload an additional release with the following command:

```
bosh upload release sas-bshpkginst-ubuntu.xxx.tgz
```

Alternatively, to upload all the releases with a single command, use the following:

```
for release in $(ls -l *.tgz | awk '{print $9}'); do bosh upload release $release; done
```
Edit the BOSH Deployment Manifest

Note: SAS Viya 3.3 on Cloud Foundry supports high availability (HA) for the CAS workers and the microservices and applications deployed to the Cloud Foundry Elastic Runtime environment. For information about adding additional instances of microservices and applications, see Add Service Instances. Other components will support HA in future releases of SAS Viya.

1 Make a copy of the sas-viya-vdmml-sample-manifest.yml from your Software Order Email (SOE) with a name that is meaningful for your SAS Viya Deployment. Here is an example:

   cp sas-viya-vdmml-sample-manifest.yml SAS-Viya-manifest.yml

   **Note:** For the remainder of this document, that new file is referred to as SAS-Viya-manifest.yml. If you name the file differently, use that name in place of SAS-Viya-manifest.yml.

2 Move SAS-Viya-manifest.yml to a location that is accessible to the BOSH Director, if necessary.

3 With a text editor, open SAS-Viya-manifest.yml.

   vi SAS-Viya-manifest.yml

4 You must make two kinds of changes to the SAS-Viya-manifest.yml in order to describe your deployment.

   **Note:** Do not change any content in the sections that are delimited by # DO NOT CHANGE ANYTHING BELOW THIS LINE and # DO NOT CHANGE ANYTHING ABOVE THIS LINE.

   **a** The first section of the BOSH deployment manifest is enclosed in brackets: <% at the beginning and %> at the end. Within this section, content that is enclosed in quotation marks can be modified, using the following guidelines:

   - Empty quotation marks (" ") indicate that you should add a value. Here is an example:

     director_uuid = ""

   - Quotation marks that enclose content indicate that the content is a default value that you can either accept or change as needed. Here is an example:

     centos_stemcell_name = "bosh-openstack-kvm-centos-7-go_agent"

   - If a value should be selected from a set of choices, those choices are indicated in a comment that precedes the variable. Here is an example:

     # Valid values for cas_mode are smp or mpp
     cas_mode = "smp"

   **b** Throughout the BOSH deployment manifest, some variables are marked by the phrase TODO. These variables should be replaced by multi-line values, such as for setinit information. When you add values to these variables, be sure to remove the existing comments, including the phrase TODO.

5 Save and close the SAS-Viya-manifest.yml file.

You can also use the sas-viya-vdmml-sample-manifest.yml to create a custom BOSH deployment manifest that specifically matches your organization's requirements. For details about specific deployment manifest settings, see “BOSH Deployment Manifest Information” on page 43.
Use BOSH to Install

1. Set the BOSH deployment to reference SAS-Viya-manifest.yml.
   
   ```
   bosh deployment SAS-Viya-manifest.yml
   ```

2. Deploy the software.
   
   ```
   bosh deploy && bosh run errand microservices
   ```

3. Check for failures in the log output from the BOSH errand.

   The Cloud Foundry Elastic Runtime has a setting to control the maximum wait time that is allowed for an application or service to start during a `cf push` operation. The default time-out setting is three minutes. If the SAS Viya products in your order take longer than three minutes to start, you might see an error like the following:

   ```
   INFO - Failed to deploy N services: names-of-services.
   ```

   In some cases, the Cloud Foundry Command Line Interface (cf CLI) reports `App failed`. This message might be inaccurate because Cloud Foundry and the cf CLI can have different time-out values, so services might have started even though the cf CLI reports a failure. Run the following command to verify the status of an application or service:

   ```
   cf apps app-name
   ```

   If necessary, use the cf CLI to start the application or service manually. Run the following command:

   ```
   cf start app-name
   ```

---

Connect to Hadoop

If your SAS Viya on Cloud Foundry order includes SAS In-Database Technologies for Hadoop, you also should have received an order for SAS Viya on Linux. Deploy the Linux order on a machine that meets the requirements that are described in SAS Viya 3.3: Deployment Guide, but with modifications.

**Note:** Perform the steps that are described in the deployment guide but with the following modifications in order to deploy only Hadoop from that order.

1. Review the “System Requirements” chapter.
   
   a. Meet the requirements that are described in Hardware Requirements ⇒ Hardware Requirements for SAS Visual Analytics and SAS Visual Statistics (Requirements for Single-Machine Deployment, Programming Interface Only)
      
      **Note:** However, be sure to modify the memory requirements. Hadoop requires only 32 MB of RAM.

   b. Meet the requirements that are described in Data Source and Storage Requirements ⇒ Hadoop Requirements ⇒ Requirements for SAS Data Connector to Hadoop or Requirements for SAS Data Connect Accelerator for Hadoop, as appropriate.

   c. Meet the requirements that are described in User and Group Requirements ⇒ Set Up the cas Account
      
      **Note:** Ensure that the sas and cas users are located on the machine on which you are installing the software.

2. Review the “Pre-installation Tasks” chapter.

   In Perform Linux Tuning ⇒ Set the ulimits, perform all steps to adjust ulimits, as necessary.
In the "Installing SAS Viya with Ansible" chapter, skip to **Edit the Inventory File**.

a. In **Define the Machines in the Deployment**, define one target reference, which is the machine on which you are installing the software.

b. In **Assign Machines to Target Groups**, remove the machine name from all host groups except `[sas-casserver-primary]` and `[sas-all-children]`.

c. Specify the machine that you listed as the target (in step 3.a) in the `[sas-casserver-primary]` host group. Do not modify the `[sas-all-children]` host group.

The results without the descriptive comments appear as follows:

```plaintext
controller-1 ansible_host=host.example.com ansible_user=user1 ansible_ssh_private_key_file=/home/user/id_rsa

[AdminServices]

[CASServices]

[CoreServices]

[DataServices]

[HomeServices]

[ReportServices]

[ReportViewerServices]

[ThemeServices]

[programming]

[configuratn]

[consul]

[httpproxy]

[pgpoolc]

[rabbitmq]

[sasdatasvrc]

[sas-casserver-primary]

controller-1

[sas-casserver-worker]

[sas-all:children]
AdminServices
CASServices
CoreServices
DataServices
HomeServices
```
4 In the "Install SAS Viya with Ansible" chapter, Modify the vars.yml File Specify the Installation Type, set sas_install_type to programming.

5 Deploy the software using the appropriate command from the following list:

<table>
<thead>
<tr>
<th>Does not require passwords</th>
<th>ansible-playbook -i hosts site.yml</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requires a sudo password only</td>
<td>ansible-playbook -i hosts site.yml --ask-become-pass</td>
</tr>
<tr>
<td>Requires an SSH password only</td>
<td>ansible-playbook -i hosts site.yml --ask-pass</td>
</tr>
<tr>
<td>Requires both a sudo and an SSH password</td>
<td>ansible-playbook -i hosts site.yml --ask-pass --ask-become-pass</td>
</tr>
</tbody>
</table>

6 After the deployment is complete, follow the instructions in "Appendix 4 – Hadoop Deployment: Configuring SAS Access to Hadoop and SAS Data Connector to Hadoop" to configure the Hadoop parts.

Note: In Configure SAS/ACCESS to Hadoop and SAS Data Connector to Hadoop Install the Hadoop JAR Files on the CAS Controller, perform the manual steps only by using Install the Hadoop JAR Files Manually.
Manual Configuration

Configure Your Environment with SAS Environment Manager

The tasks in this section are applicable if you deployed all of your software (full deployment). If you deployed the programming interface only, skip this section.

Sign In as the sasboot User

Your SAS environment is deployed with an initial administrator account that is named sasboot. Follow these steps:

1. Locate the SAS-Viya-manifest.yml file in the sas_viya_cloudfoundry subdirectory of the directory where you unzipped your deployment files.

2. Locate the following line:
   
   `sas_logon_initial_pwd = "SAS-logon-initial-password"

   **Note:** This is the password that you will use to sign in as sasboot to SAS Environment Manager.

3. Locate the following lines:
   
   `cf_deployment_host = "deployment-host"
   cf_deployment_domain = "deployment-domain"

   **Note:** These are the host and domain name for the SAS Environment Manager URL.

4. Sign in to SAS Environment Manager by using a URL with the following format and the sasboot credentials:

   `http://deployment-host.deployment-domain/SASEnvironmentManager`

5. Click the **Yes** button for all of the assumable groups so that you have the permissions to perform subsequent tasks.
Configure the Connection to Your Identity Provider

After installing a new SAS Viya deployment, you must configure the connection to your identity provider before your users can access SAS Environment Manager and SAS Visual Analytics. Complete these steps while you are signed in as the sasboot user.

Note: Only LDAP-based identity providers are supported. These instructions assume that you have basic familiarity with LDAP administration. For details about properties, see "sas.identities.providers.ldap" in SAS Viya Administration: Configuration Properties.

If you have already set up LDAP through the manifest file, skip to step 6.

1. Select the icon from the side menu to open the Configuration page.

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

3. In the sas.identities.providers.ldap.user section, click . In the New Configuration window, do the following:
   a. Specify a value for the following required field: baseDN. For the remaining fields, review the default values and make changes, as necessary. The default values are appropriate for most sites.

   TIP In this step, consider specifying a custom filter to limit the group accounts that SAS Viya returns from your provider.

   b. Click Save.

4. In the sas.identities.providers.ldap.group section, click . In the New Configuration window, do the following:
   a. Specify a value for the following required field: baseDN. For the remaining fields, review the default values and make changes, as necessary. The default values are appropriate for most sites.

   Note: When using the LDAP protocol, passwords are transmitted over the network in plaintext. To secure the deployment, SAS recommends that you configure LDAPS. For details, refer to “Configure SAS Viya to Connect to LDAPS Provider” in SAS® Viya 3.3 Administration: Data in Motion.

   For each property that represents a group-level field in SAS, specify a corresponding property in the LDAP provider software.

   TIP In this step, consider specifying a custom filter to limit the group accounts that SAS Viya returns from your provider.

   b. Click Save.

5. In the sas.identities.providers.ldap.connection section, click . In the New Configuration window, do the following:
   a. Specify values for the following required fields: host, password, port, url, and userDN. For the remaining fields, review the default values and make changes, as necessary. The default values are appropriate for most sites.

   b. Click Save.
From the SAS Environment Manager side menu, select to open the Users page.

On the Users page, select Users from the list in the toolbar. Your users should appear after a few minutes. It is not necessary to restart any servers or services. Then select Groups from the list to display your groups.

Verify that user and group information is displayed correctly. If not, make any necessary changes to the identities service properties.

**Configure the Connection to the Mail Service**

After installing a new SAS Viya deployment, you must configure the connection to your mail service. Complete these steps while you are signed in as the sasboot user.

1. Select the from the side menu to open the Configuration page.

2. On the Configuration page, select Basic Services from the list, and then select Mail service from the list of services.

3. In the sas.mail section, click . In the Edit Configuration window, follow these steps:
   a. Specify a value for the following required fields: host and port. For the remaining fields, review the default values and make changes, as necessary. The default values are appropriate for most sites.
   b. Click Save.

4. (Optional) To enable the health check for the mail service, perform the following steps.
   a. Select the from the side menu to open the Configuration page.
   b. On the Configuration page, select Basic Services from the list, and then select Mail service from the list of services.
   c. In the management.health.mail section, click .
   d. Turn the enabled toggle to on.
   e. Click Save.

When this toggle is set, health checks will be enabled after the mail service is restarted. If the mail host is not configured or is configured incorrectly, or if it cannot connect to the SMTP mail server, the mail service will indicate it is in a failed state.

**Set Up Administrative Users**

While you are signed on to SAS Environment Manager as the sasboot user, set up at least one SAS Administrator user, as follows:

1. From the SAS Environment Manager side menu, select to open the Users page.

2. On the Users page in SAS Environment Manager, select Custom Groups from the list in the toolbar.

3. In the left pane, click SAS Administrators.

4. In the Members section of the right pane, click , and add one or more members to the group (including your own account, if applicable).
5 Sign out from SAS Environment Manager so that you are no longer signed in as the sasboot user.

6 If you added your own account to the SAS Administrators group, you can sign on again to SAS Environment Manager using that account.

Open SAS Environment Manager from a URL with the following format:

http://http-proxy-host-name/SASEnvironmentManager

**TIP** Since SAS Administrators is an assumable group, the following prompt is displayed: *Do you want to opt in to all of your assumable groups?*. Select **Yes** if you want the extra permissions that are associated with the SAS Administrators group. The selection remains in effect until you sign out.

**Sign In Using LDAP Credentials**

Open SAS Environment Manager from a URL with the following format:

http://http-proxy-host-name/SASEnvironmentManager

Sign in as one of the SAS Administrators that you set up in “Set Up Administrative Users” on page 25.

**Disable the Password Reset Feature and Reset the sasboot Password**

When you are finished setting up LDAP and the initial administrative users, you should reset the password for the sasboot user. For additional security, you can then disable the password reset feature. This prevents password reset links from being written to the log each time the SASLogon service is restarted.

1 Sign in to SAS Environment Manager as an administrative user and select ⬟ from the side menu to open the Configuration page.

2 On the Configuration page, select **Definitions** from the drop-down list.

3 In the left pane, select **sas.logon.initial**. Then select ⬇ at the top of the right pane. If a definition already exists, you can select ⬇ to edit the existing definition.

4 In the New sas.logon.initial Configuration window or the Edit sas.logon.initial Configuration window, set **reset.enabled** to **off**.

5 Click **Save**.

6 Restart the SASLogon service. For more information, see Other Servers and Services: Operate in SAS Viya for Cloud Foundry: Operations.

*Note:* After you disable this feature, you can still change the sasboot password if the existing password is known. Enter the URL for SAS Viya with the path */SASLogon/change_password*. If you are already signed in as another user, first sign out and then sign back in as sasboot using the current password. You can then complete the steps to change the password.

**Configure SAS Viya to Connect to LDAPS Provider**

After the deployment is complete, be aware that your system is not yet secured. To configure LDAPS, see “Configure SAS Viya to Connect to LDAPS Provider” in Encryption in SAS Viya: Data in Motion.
Change the Administrative User Password for SAS Message Broker

Note: The tasks in this section are applicable only if you deployed all of your software.
You must change the administrative user password for SAS Message Broker immediately after you have deployed SAS Viya.

Note: The steps in this section update the password for the default administrator user account sasclient.

1. With a text editor, open SAS-Viya-manifest.yml.
   `vi SAS-Viya-manifest.yml`

2. To change the password for the default administrative user, sasclient, add the following property for the rabbitmq job and add the rabbitmq.client.password as a property at the end of the rabbitmq job property.

   ```yaml
   - name: rabbitmq
     instances: 1 # DO NOT CHANGE
     jobs:
     - {name: rabbitmq, release: sas-bshrabbitmq-<%= package_type %>
     - {name: consul, release: sas-bshconsul-<%= package_type %>
     vm_type: <%= vm_type %>
     stemcell: <%= stemcell %>
     networks:
     - name: <%= private_network_name %>
       default: [dns, gateway]
     - name: <%= public_network_name %>
       static_ips: [ <%= rabbitmq_ip %>]
     properties:
     rabbitmq:
     client:
       password: MySpecialPassword
   ```


4. To obtain a list of virtual machines (VMs), run the following command:
   `bosh vms deployment-name`

   Note: You can find the deployment name in the manifest file as follows:
   `name: sas-vdmml-stemcell-name`

   A listing of VMs that contains a rabbitmq line is displayed. Here is an example:
   `rabbitmq/0 (b89e0987-d6d1-4ae1-b5df-b084aa83beea)`
   The 0 is the index of the VM.

5. To update the environment with the new RabbitMQ values, run the following command:
   `bosh recreate rabbitmq index --force`

   Here is an example:
   `bosh recreate rabbitmq 0 --force`
Validating the Cloud Foundry Deployment

Validate the deployment of SAS Viya on Cloud Foundry as follows:

1. Verify that the BOSH managed services are running and that the applications are running in the Pivotal Cloud Foundry Elastic Runtime. To verify that all of the virtual machines (VMs) for the SAS Viya instances are running, run the following command:

   ```
bosh instances
   ```

   A table is displayed that provides an overview of the instances in the current SAS Viya deployment.

2. To verify that all of the SAS Viya microservices and applications are deployed, run the following command:

   ```
cf apps
   ```

   The applications that are deployed to Cloud Foundry by the microservices BOSH release will be displayed. The names, number of instances, and memory will vary depending on the settings that you specified in the BOSH deployment manifest. For example, if you use the sample BOSH deployment manifest and set the cf_app_prefix variable to sasviya, you will see application names such as sasviya-reports and sasviya-themes.

3. To obtain a listing of the IP addresses that are associated with the deployment, run the following command:

   ```
bosh vms
   ```

   **Example output:**

   RSA 1024 bit CA certificates are loaded due to old openssl compatibility
   Acting as user 'admin' on 'company-bosh'
   Deployment 'sas-vdmml-ubuntu'

   Director task 732

   Task 732 done

   +------------------------------------------------------------+---------+-----+---------+----------------+
   | VM                                                         | State   | AZ  | VM Type | IPs            |
   +------------------------------------------------------------+---------+-----+---------+----------------+
Log On to SAS Studio

To ensure that SAS Studio has been deployed correctly and is working, simply log on to it:

1. Open SAS Studio from a URL with this format:
   
   http://<hostname>/SASStudio

2. Log on using the credentials for your operating system account.

Note: To log off from SAS Studio, click Sign Out on the toolbar. Do not use the Back button on your web browser.

Access CAS Server Monitor

To verify that CAS Server Monitor has been successfully deployed, access it by opening a web browser and entering the URL in the address field in the following format:

http://cas_controller-IP-address:8777

Note: To find out the IP address, see “Validating the Cloud Foundry Deployment” on page 29.

Here is an example:


Log on using one of the SAS Administrator users that you established in “Set Up Administrative Users” on page 25.

Note: In a full deployment, dual authentication occurs for logon to CAS Server Monitor and access to CAS from SAS Studio.

Verify SAS Infrastructure Data Server

Note: If you deployed the programming-only interface, skip this section.

During deployment, SAS Infrastructure Data Server performs a verification check and creates a log of that process. Use these steps to verify that SAS Infrastructure Data Server has been deployed correctly.

1. Consolidate the log files by running the following command:
The output displays the location of the logs. Here is an example:

RSA 1024 bit CA certificates are loaded due to old openssl compatibility
Acting as user 'admin' on deployment 'machine-name' on 'stobosh-microbosh'

Director task 719
  Started fetching logs for pgpool/560a40d3-95ba-4b0c-979a-de8428f464b2 (0) >
  Finding and packing log files. Done (00:00:01)

Task 719 done

Started         2017-06-13 13:11:23 UTC
Finished        2017-06-13 13:11:24 UTC
Duration        00:00:01
Downloading log bundle (6f24fddf-3acd-4ae6-62b2-1ffe615fab1a)... 

Logs saved in '*/home/log-file-location/pgpool.0.date-time-stamp'

2 Unpack the log files by running the following command:

    tar xvf /home/log-file-location/pgpool.0.date-time-stamp.tgz

Here is typical output:

    ./
    ./monit/
    ./monit/monit_debugger.pgpool.log
    ./monit/consul.err.log
    ./monit/monit_debugger.consul.log
    ./monit/watcher.log
    ./monit/consul.log
    ./monit/monit_debugger.pgpool_watcher.log
    ./monit/pgpool.log
    ./consul/
    ./consul/consul.stderr.log
    ./consul/sas-consul_2017-06-13_12-40-14.log
    ./consul/consul.stdout.log
    ./pgpool/
    ./pgpool/pgpool_status
    ./pgpool/pgpool.log

3 Open the /pgpool/pgpool.log file.

Here is an example of the log for a successful deployment:

    [pgpool] start called at Tue Jun 13 00:19:21 UTC 2017
    [pgpool] start called at Tue Jun 13 00:20:22 UTC 2017
    [pgpool] Consul status peers: [192.168.10.142:8300]
    [pgpool] Primary node registered in Consul: 10.104.162.176
    [pgpool] We are going to sleep and then exit in order to give the data nodes a chance to start first
    [pgpool] Primary node status is down...sleeping and looping until it comes up
    [pgpool] Create the pool_password file
    [pgpool] Create the oiddir, /var/vcap/sys/log/pgpool/oiddir
    [pgpool] Run pgpool
    [pgpool] Register pgpool node in Consul
    2017-06-13 00:20:28 [No Connection] MAIN[7679] [No Connection]@[No Connection]:
    LOG:  Backend status file /var/vcap/sys/log/pgpool/pgpool.status does not exist
A log for a failed verification contains error messages or other output that is not the direct output of database queries.

Verify SAS Message Broker

Note: This section is applicable only if you have a full deployment. If you have a programming-only deployment, skip this section.

To verify that CAS Server Monitor has been successfully deployed, access it by opening a web browser and entering the URL in the address field in the following format:

http://RabbitMQ-IP-address:15672/#/

Note: To find out the IP address, see “Validating the Cloud Foundry Deployment” on page 29.

Here is an example:

Uninstalling SAS Viya

Uninstall the Deployment

1. Create a list of the apps in the Elastic Runtime.
   
   `cf apps | grep Cloud-Foundry-app-prefix`

   The *Cloud-Foundry-app-prefix* is the value that you used in the BOSH deployment manifest for the *cf_app_prefix* variable.

2. Stop each app that was listed by the previous step.
   
   `cf stop app-name`

3. Delete each app that was listed by the previous step.
   
   `cf delete -r app-name`

4. To uninstall, run the following command:
   
   **Note:** This command calls the stop command before it deletes the virtual machines (VMs). The stop command should halt any processes that might interfere with deletion.

   `bosh delete deployment deployment-name`

   You can find the deployment name in the BOSH deployment manifest:

   `name: sas-vdmm1-stemcell-name`

5. Identify the releases that are used in the deployment.
   
   `bosh releases`

6. Delete each release that is named sas-bsh* from the results in the previous step.
   
   `bosh delete release release-name`

   Here is an example:

   `bosh delete release sas-bshvdmmlsas-redhat`

7. Remove the directory where the SAS software is located.
   
   `rm -r SAS-software-directory`

8. Remove the microservices using any of the community-supported plug-ins for the Cloud Foundry command-line interface that can delete applications based on a wildcard pattern.
Note: SAS uses persistent disks. The results from the preceding steps include orphaned disks, but they should not affect software usage. BOSH eventually cleans up orphaned disks automatically. However, you can remove orphaned disks using any of these methods:

1 Remove individual disks using BOSH commands:
   a To obtain a list of orphaned disks:
      bosh disks --orphaned
   b To remove each specified disk:
      bosh delete disk disk-ID
   c Remove all the orphaned disks:
      bosh cleanup --all
      Note: The cleanup command deletes all orphaned disks and unused releases across the entire BOSH Director.

2 Use the console that is provided by your IaaS to look for and manage orphaned disks.
Managing Your Software

Overview

What Is an Update?
An update replaces some or all of your deployed software with the latest versions of that software. Updated software is intended to be compatible with the existing configuration, content, and data. To perform an update, you will run the same tools that were run during the initial deployment. You do not need a new order to perform an update. You might determine that your software needs updating or you might be notified by SAS that updates are available.

What Is an Upgrade?
An upgrade adds significant feature changes or improvements to your deployed software. To perform an upgrade, you will run the same tools that were run during the initial deployment. You will need a new order to upgrade your deployed software. An upgrade might require changes to the deployed software’s configuration. You might determine that your software needs upgrading or you might be notified by SAS that upgrades are available. SAS recommends creating a backup of the deployed software environment before performing an upgrade.
Update Your Software

Overview
You must update your deployed software environment in order to bring the environment’s software to the latest version. You can also modify your deployment from programming-only to full.

Updating SAS Viya software requires an outage period because some SAS Viya services are stopped and restarted automatically during the update process.

You will need the location of the directory where you stored deployment and maintenance files. For more information about this directory, see “Obtain the Required Files” on page 13.

Update Your SAS Viya Software

Overview
The update process brings your deployed software up-to-date with the latest compatible software. You used BOSH to install SAS Viya 3.3 on Cloud Foundry. You will perform the update with the same command that was used to install SAS Viya, and you will use the same software order.

Update with BOSH
To update a SAS Viya deployment using BOSH:

1  (Optional) Create a list of the existing installed software before you begin.
   Create a file that lists the names and versions of all the BOSH releases of the SAS Viya software that are installed. Create this file in the directory where you stored deployment and maintenance files. For more information about this directory, see “Obtain the Required Files” on page 13. For example, you can run the following command to create a text file that lists all the SAS BOSH releases:

   ```bash
   bosh deployments > viya_releases.txt
   ```

2  (Optional) To modify the deployment type from a programming-only deployment to a full deployment, perform the following steps:
   a  With a text editor, open the sas-viya-vdmml-sample-manifest.yml file.
      A programming-only deployment will contain the following line:

      ```yaml
      programming-only = true
      ```
   b  Change `true` to `false`.
   c  Save and close the SAS-Viya-manifest.yml file.

3  To start the update, run the same command and options that you ran when you performed the initial deployment. Complete the tasks in “Installing SAS Viya” on page 17.

4  (Optional) After the update process has completed, record the new list of installed software.
   Create a file that lists the names and versions of all the BOSH releases of the SAS Viya software that are installed. Create this file in the directory where you stored deployment and maintenance files. For more information about this directory, see “Obtain the Required Files” on page 13. For example, you can use the following command to create a text file that lists all the SAS BOSH releases:

   ```bash
   bosh deployments > new_viya_releases.txt
   ```
You can see the differences between the previous and current deployments by comparing the lists of installed software before the update (Step 1 on page 36) and after the update.

## Upgrade Your Software

### Overview

An upgrade adds significant feature changes or improvements to your deployed software. To perform an upgrade, you will run the same tools that were run during the initial deployment. You will need a new software order to upgrade your deployed software. An upgrade might require changes to the deployed software’s configuration.

You might determine that your software needs to be upgraded or you might be notified by SAS that upgrades are available. SAS recommends that you create a backup of the deployed software environment before performing an upgrade.

Upgrading SAS Viya software requires an outage period because some SAS Viya services are stopped and restarted automatically during the upgrade process.

You will need the location of the directory where you stored deployment and maintenance files. For more information about this directory, see “Obtain the Required Files” on page 13.

### Prepare to Upgrade Your SAS Viya Software

To prepare to upgrade a SAS Viya deployment:

**Note:** Be aware that system requirements for RAM, CPU, and disk space are likely to change with each SAS Viya release. Verify that your environment meets the requirements that are listed in “System Requirements” on page 3.

1. (Optional) Create a list of the existing installed software before you begin.
   
   Create a file that lists the names and versions of all the BOSH releases of the SAS Viya software that are installed. Create this file in the directory where you stored deployment and maintenance files. For more information about this directory, see “Obtain the Required Files” on page 13. For example, you can run the following command to create a text file that lists all the SAS BOSH releases:

   ```
   bosh deployments > viya_releases.txt
   ```

2. When performing an upgrade, you receive a new Software Order Email (SOE) from SAS. Perform the tasks in “Pre-Installation Tasks” on page 13.

3. Perform the tasks in “Upload Releases to the BOSH Director” on page 17.

### Upgrade Your SAS Viya Software

To upgrade a SAS Viya deployment:

1. If the deployment uses a custom theme, perform the following steps:
   
   a. As a member of either the Application Administrators group or the SAS Administrators group, log on to SAS Theme Designer.
   
   b. Select the custom theme.
   
   c. Click Unpublish.
Click **Publish**.

When the theme’s status changes to Published, log off from SAS Theme Designer.

2 To stop existing applications in the Cloud Foundry Elastic Runtime, perform the following steps:
   a Using a text editor, create the following script.
   ```bash
   export APP_PREFIX=prefix
cf apps | grep '{APP_PREFIX}-' | awk '{print $1}' | xargs -I% -P5 cf stop %
   ```
   *Prefix* specifies the value that you used in the BOSH deployment manifest for the `cf_app_prefix` variable.
   b Run the script that you just created.

3 To remove defunct microservices from the Cloud Foundry Elastic Runtime, perform the following steps:
   a Using a text editor, create the following script.
   ```bash
   export APP_PREFIX=prefix
cf delete ${APP_PREFIX}-recipeExecutionProvider -f -r
cf delete ${APP_PREFIX}-dataPreparationPlans -f -r
cf delete ${APP_PREFIX}-SASVisualDataBuilder -f -r
   ```
   *Prefix* specifies the value that you used in the manifest for the `cf_app_prefix` variable.
   b Run the script that you just created.

4 Copy the sas-viya-vdmml-sample-manifest.yml from your Software Order Email (SOE) to a new file with a name that is meaningful for your SAS Viya deployment. Here is an example:
   ```bash
   cp sas-viya-vdmml-sample-manifest.yml SAS-Viya-manifest.yml
   ```
   **Note:** The new file is referred to as SAS-Viya-manifest.yml in this guide. If you name the file differently, use that name in place of SAS-Viya-manifest.yml.

5 Copy the variable values from your SAS Viya 3.2 BOSH deployment manifest to the new SAS Viya 3.3 BOSH deployment manifest. Both manifests contain an initial section that is enclosed in brackets: `<% at the beginning and `%>` at the end.
   Within this section, copy the variable values from your SAS Viya 3.2 manifest to the new SAS Viya 3.3 manifest.
   **Note:** SAS Viya 3.3 requires a newer BOSH stemcell than the one used in SAS Viya 3.2. For the specific requirement, see “System Requirements” on page 3.
   **Note:** The variable `datamining_pwd` is new for SAS Viya 3.3. Specify an appropriate value.

6 Edit the SAS Viya 3.3 BOSH deployment manifest file. From the SAS Viya 3.2 BOSH deployment’s manifest file, copy the following items to the new manifest file:
   - key_value_data additions in Consul
   - sssd.conf file and certificate information
   - nfs fstab information
   - any other necessary environment configuration
   **Note:** Review “BOSH Deployment Manifest Information” on page 43 for issues that should be considered in the new manifest file.
Although SAS Viya 3.2 supported the use of nonalphanumeric characters (such as punctuation characters) in passwords, SAS Viya 3.3 does not support nonalphanumeric characters in the dbmsowner account’s password.

Note: Changing the dbmsowner user password is not required when upgrading programming-only environments.

Edit the SAS Viya 3.3 BOSH deployment manifest template. In the section POSTGRES CONFIGURATION DEFAULTS, find the following line:

```
db_user_pwd="password"
```

Replace the existing value `password` with a password that contains only alphanumeric characters.

Perform the tasks in "Use BOSH to Install" on page 19.

Perform the task in "Connect to Hadoop" on page 19.

After the software has been installed, complete the following tasks, as appropriate:

a  “Manual Configuration” on page 23.

b  “Validating the Deployment” on page 29.

(Optional) After the upgrade process has completed, create a new list of installed software.

Create a file that lists the names and versions of all the BOSH releases of the SAS Viya software that are installed. Create this file in the directory where you stored deployment and maintenance files. For more information about this directory, see “Obtain the Required Files” on page 13. For example, you can use the following command to create a text file that lists all the SAS BOSH releases:

```
bosh deployments > new_viya_releases.txt
```

You can see the differences between the previous and current deployments by comparing the lists of installed software before the upgrade (Step 1 on page 37) and after the upgrade.

Preserve Access Controls for Database Caslibs

SAS Viya 3.3 includes changes to how access controls for database caslibs are stored. Path-based caslibs that use a directory as a data source are unaffected.

TIP  If you have database caslibs in a SAS Viya 3.2 deployment, but you do not have access controls or you do not need to preserve the access controls, you can drop the caslib and add an identical caslib with the same name. Using the same name enables SAS Visual Analytics reports to remain valid. Drop and add the caslib after the upgrade to SAS Viya 3.3 has completed.

Immediately after the upgrade to SAS Viya 3.3 has completed, the change to the access controls prevents data access with caslibs that use databases. Specifically, the server cannot perform the loadTable, save, columnInfo, and fileInfo actions. Here is the error message that is displayed:

```
Caslib caslib-name is from an old release and cannot be used. Create a new caslib and copy the access controls to it.
```

To preserve existing access controls, perform the following steps for each database caslib after SAS Viya 3.3 has been deployed and SAS Cloud Analytic Services (CAS) has been started with the new release.

1  Temporarily add a caslib with the same data source as the original caslib. Use a temporary name such as OdbcclibNew. Use the same database server, port, schema, and so on, as applicable for the data source.

2  From a SAS session that is running SAS Viya 3.3 or SAS 9.4M5, run the copyObjects action. In this example, odbcclib is the existing caslib and temp-odbcclib is the new temporary caslib.
CAUTION! The copyObjects action is a restricted action that is designed for this specific purpose. Do not attempt to use it for any other purpose elsewhere.

```plaintext
cas;
proc cas;
    accessControl.assumeRole / adminRole="data";
run;

    accessControl.copyObjects / 
        fromObjectSelector={caslib="odbclib" objType="caslib"}
        toObjectSelector={caslib="temp-odbclib" objType="caslib"};
run;
```

3 Drop the original caslib. In the example, odbclib is the caslib.

4 Add a caslib that is identical to the original caslib. Use the same name as the original caslib and the same data source information.

5 Restore the access controls from the temporary caslib to the newly created caslib:

```plaintext
cas;
proc cas;
    accessControl.copyObjects / 
        fromObjectSelector={caslib="temp-odbclib" objType="caslib"}
        toObjectSelector={caslib="odbclib" objType="caslib"};
run;

    accessControl.dropRole / adminRole="data";
run;
```

6 Drop the temporary caslib.
Next Steps

Refer to Additional Documentation

Refer to Additional Documentation

After you validate the deployment, you can perform initial administrative tasks. For more information, refer to SAS Viya on Cloud Foundry: Getting Started.

Refer to the appendix in this guide for additional tasks that you might perform, based on your environment. For usage information, refer to the Help that is available from the SAS Viya product and administrative interfaces.

If you are using a Hadoop data source, you should also refer to the appendixes in the SAS Viya for Linux Deployment Guide for additional tasks that you must perform in your environment.
Appendix 1

BOSH Deployment Manifest Information

Configure a Single Network ......................................................... 43
Remove a Stemcell .................................................................. 43
Differentiate Multiple SAS Environments .................................. 44
Add CAS Worker Nodes ............................................................. 44
Define Persistent Disks ............................................................... 45
Ports ........................................................................................... 46
  PostgreSQL Ports ................................................................... 46
  Geode Ports ......................................................................... 46
  SAS Compute Server Port ....................................................... 47
Consul Settings ......................................................................... 47
Integrate with Secure Hadoop through Kerberos ......................... 48
Identify a CAS Administrative User .......................................... 50
Set the CAS Data Directory ...................................................... 51
CAS Settings .............................................................................. 51
Establish Communication Between the SAS Embedded Process and CAS Worker Nodes .................................................. 51
NFS Mount Options .................................................................. 52
  Add NFS Mount Capability .................................................... 52
  Remove NFS Mount Capability .............................................. 52
Security Settings ....................................................................... 53
Apply the Setinit ....................................................................... 53

Configure a Single Network

If you want a network topology that is different from the one that is defined in the sample BOSH deployment manifest, edit the manifest as appropriate. SAS applications and microservices that are deployed to the application run time will require connectivity to the BOSH managed services. Plan your software-defined network topology and configuration to account for this requirement.

Remove a Stemcell

To remove a single type of stemcell from the BOSH deployment manifest:
In the Stemcell Management section of the BOSH deployment manifest, remove or comment out (by adding a number sign) the appropriate variables. For example, to remove CentOS stemcells, modify the section as follows:

```yaml
# centos_stemcell_name = "bosh-openstack-kvm-centos-7-go_agent"
# centos_stemcell_version = "3421"
ubuntu_stemcell_name = "bosh-openstack-kvm-ubuntu-trusty-go_agent"
ubuntu_stemcell_version = "3421"
```

Alternatively, you can remove the two lines that refer to CentOS.

In the stemcells section, remove the appropriate variables. For example, to remove CentOS stemcells, delete the highlighted lines:

```yaml
stemcells:
- alias: ubuntu
  name: <%= ubuntu_stemcell_name %>
  version: <%= ubuntu_stemcell_version %>
- alias: centos
  name: <%= centos_stemcell_name %>
  version: <%= centos_stemcell_version %>
```

Save and close the BOSH deployment manifest.

---

**Differentiate Multiple SAS Environments**

Attempting to deploy multiple SAS environments to a single org and space results in application naming conflicts. To avoid naming conflicts, use the `cf_app_prefix` variable in the Cloud Foundry information section of the BOSH deployment manifest. Ensure that the value for `cf_app_prefix` is unique for each SAS environment that is listed in the BOSH deployment manifest. A unique value is prepended to each standard app name in order to differentiate between SAS environments.

**Add CAS Worker Nodes**

SAS Viya for Cloud Foundry supports CAS servers running in either symmetric multiprocessing (SMP) or multiple parallel processing (MPP) mode. If you deploy CAS in MPP mode, you can specify the number of CAS worker nodes to be created. You must have a unique IP address that is assigned by your infrastructure provider for each of the worker nodes that you add.

In the CAS controller instance definition, make sure that the CAS configuration is set to `mpp`. If you use the sample BOSH deployment manifest, set the value of the `cas_mode` variable to `mpp`.

```yaml
# CAS CONFIGURATION DEFAULTS #################################################
#   Valid values for cas_mode are smp or mpp
# cas_mode = "mpp"
```

Make sure that you have an IP address for each CAS worker node that you want to create. Modify the `cas_worker_ips` variable to include a comma-separated string of IP addresses, one for each node that you want to add. If you are using the sample BOSH deployment manifest, the value of the `<%= cas_worker_count %>` variable is calculated based on the number of addresses that you specify.

```yaml
# IP ADDRESSES ##############################################################
# Collection of IPs that need to be acquired from the infrastructure
# i.e. OpenStack, AWS, etc.
```
sas_ip = ""
cas_controller_ip = ""
# The cas_worker_ips only needs to be provided if cas_mode == "mpp"
cas_worker_ips = ""
...

If you create a custom BOSH deployment manifest, specify the number of CAS worker nodes that you need using the `instances` setting within the CAS worker instance definition. Set the value of `static_ips` using a list of comma-separated IP address values. The number of addresses that you specify must match the number of CAS worker instances that you want to create.

Note that you can increase the number of CAS workers deployed after the SAS Viya system is running by increasing the value of `instances` and assigning the appropriate number of IP addresses.

---

**Define Persistent Disks**

Software that is deployed using BOSH releases might need to store persistent data. SAS Viya on Cloud Foundry uses standard BOSH mechanisms for attaching a persistent disk to the virtual machines (VMs) that are created by the release jobs. You are able to attach (or re-attach) the persistent disk to a VM following start, restart, stop, or terminate operations.

You can use the BOSH deployment manifest to apply an appropriately sized persistent disk to a VM. You can use standard disk types that are defined by your organization or infrastructure provider and that are typically identified in the BOSH cloud-config file. Here is an example:

```yaml
disk_types:
  - name: small
disk_size: 3000
  - name: medium
disk_size: 10000
  - name: large
disk_size: 20000
  - name: xlarge
disk_size: 30000
```

The sample BOSH deployment manifest provides a single variable named `disk_type` for the persistent disk type. However, if your deployment requires persistent disks of varying sizes, you can add additional variables for use throughout the BOSH deployment manifest. As an alternative, for each instance, you can use the `named-disk-type` as the `persistent_disk_type`. The `named-disk-type` is defined in the BOSH cloud-config file. Here is an example:

```yaml
- name: cas_controller
  instances: 1
...
  vm_type: <%= vm_type %>
persistent_disk_type: <%= disk_type %> | named-disk-type
  stemcell: <%= stemcell %>
```

As another example, to set the persistent disk to 30GB, you could set `persistent_disk_type` to `xlarge` in the cloud-config file.

```yaml
persistent_disk_type: "xlarge"
```
Ports

**PostgreSQL Ports**

PostgreSQL server configuration includes a port definition. This value is set in the sample BOSH deployment manifest using the variable postgres_config_port in the POSTGRES CONFIGURATION DEFAULTS, or you can set it specifically in the properties section of the postgresql instance definition.

```yaml
- name: postgresql
  ...
  properties:
    postgres:
      config:
        port: numeric-port-value
```

SAS Viya uses pgpool as the connection pooling and load balancing service for PostgreSQL. Configuration for pgpool includes a port definition. This value is set in the sample BOSH deployment manifest using the variable pgpool_config_port in the POSTGRES CONFIGURATION DEFAULTS, or you can set it specifically in the properties section of the pgpool instance definition.

```yaml
- name: pgpool
  ...
  properties:
    pgpool:
      config:
        port: numeric-port-value
```

**Geode Ports**

Geode provides the dynamic replication and caching service for SAS Viya. It consists of two parts: a cacheserver and a locator. Each Geode component is deployed in its own instance.

Geode Cacheserver includes two ports, one for client connections (10444) and another for its HTTP server (25555). These values are not defined in the sample BOSH deployment manifest, but you can override the default values by setting the following properties:

```yaml
- name: geode-cacheserver
  ...
  properties:
    cacheserver:
      server_port: numeric-port-value
    geode:
      server_port: numeric-port-value
```

Geode Locator includes two ports, one for discovery (10334) and another for its HTTP server (25555). These values are not defined in the sample BOSH deployment manifest, but you can override the default values by setting the following properties:

```yaml
- name: geode-locator
  ...
  properties:
    locator:
      port: numeric-port-value
    geode:
      server_port: numeric-port-value
```
SAS Compute Server Port

The SAS Compute Server uses a launcher process that has a default port (6543). The default port number is not defined in the sample BOSH deployment manifest. However, you can override the default port number by creating a new port number property in the instance where the compute server is specified. In the sample Bosh deployment manifest, that instance is the object spawner.

```yaml
- name: object_spawner
  instances: 1 # DO NOT CHANGE
  templates:
    - {name: install_java, release: sas-bshjava-<%= package_type %>}
    - {name: install_config_nfs, release: sas-bshnfs-<%= package_type %>}
    - {name: install_config_sssd, release: sas-bshsssd-<%= package_type %>}
    - {name: install_numa, release: sas-bshnuma-<%= package_type %>}
    - {name: install_libpng, release: sas-bshlibpng-<%= package_type %>}
  <%- if stemcell == "ubuntu" %>
    - {name: install_packages, release: sas-bshpkginst-<%= package_type %>}
  <%- end %>
- name: object_spawner
  properties:
    computesrv:
      port: numeric-port-value
      release: sas-bshvdmmlsas-<%= package_type %>
      consumes:
        cas: {from: cas_controller}
```

Consul Settings

SAS Viya on Cloud Foundry uses Consul as a store for key-value configuration data. You can control some settings for Consul through the BOSH deployment manifest.

You must specify initial key_value_data that is loaded into Consul at deployment and during configuration. The values are set via a YAML configuration based on the values in config.application.sas in the consul block. All SAS Viya deployments must include the following variables:

- config.application.sas.url.httpd, which is the combination of the host and the domain from the microservices and the HTTP or HTTPS protocol, depending on whether port 80 or 443 is specified.

- config.application.sas.identities.providers.ldap.connection, config.application.sas.identities.providers.ldap.user, and config.application.sas.identities.providers.ldap.group, which take a set of values that adds the LDAP configuration information based on your organization’s requirements.

Here is an example:

Note: For improved readability, a variable in the following example occupies two lines. However, you should use only one line for that variable in your BOSH deployment manifest.

```yaml
- name: consul
  properties:
    consul:
      ...
      key_value_data: |
        config:
          application:
```

Consul Settings
Note: The values for the LDAP user and the group settings are site-specific, and the information that you specify varies according to your organization’s rules. Consult with the LDAP administrators in your organization to validate the settings.

You can set a custom Consul datacenter name. The default is dc1. This value is set in the sample BOSH deployment manifest using the variable <%= consul_datacenter %>, or you can set it in the properties section of the Consul instance definition.

```yaml
- name: consul
  properties:
    consul:
      ...  
      datacenter: <%= consul_datacenter %>
```

If you change the Consul datacenter name, you must add a property to the global properties list so that each Consul agent can be set appropriately.

```yaml
properties:
  consul:
    datacenter: <%= consul_datacenter %>
```

Note: For a complete list of configuration properties that you can set in the Consul instance group in the config.application section, see “Configuration Properties: Reference (Services)” in “SAS Viya Administration”.

---

**Integrate with Secure Hadoop through Kerberos**

If your deployment needs to integrate with a secure Hadoop deployment through Kerberos, perform the following steps.

1. To create the krb5.conf file, add the following lines to the properties section of the BOSH deployment manifest:

   ```yaml
   properties:
   ...  
   ```

   **Note:** The indentation is important. Ensure you use the same indentation that is shown in the example.
Integrate with Secure Hadoop through Kerberos

2 If you are using Ubuntu stemcells and the Kerberos default ticket location (/tmp), the group permissions for /tmp must be modified. Add the following line to the `pre_deploy_script` variable that you added in step 1.

```bash
chgrp root /tmp
```

3 In order for the workspace server process to know about the auto-generated Kerberos token, add the following lines to the BOSH deployment manifest. For improved readability, several commands in the following code occupy two lines. However, make sure that you enter the command on a single line.

```
#!/bin/bash
if [ -f /var/vcap/data/packages/sas-workspace/*/opt/sas/viya/config/etc/workspaceserver/default/workspaceserver_usermods.sh ]; then
  sed -i /workspace_user/d /var/vcap/data/packages/sas-workspace/*/opt/sas/viya/config/etc/workspaceserver/default/workspaceserver_usermods.sh
  echo 'workspace_user=$(whoami)
  workspace_user_ccaches=$(find /tmp -maxdepth 1 -user $workspace_user -type f -name "krb5cc_*" -printf "%T@ %p\n" | sort -k 1nr | sed "s/^[^ ]* //"
  if [ ! -z $workspace_user_ccaches ]; then export KRB5CCNAME=$workspace_user_ccaches; fi' >> /var/vcap/data/packages/sas-workspace/*/opt/sas/viya/config/etc/workspaceserver/default/workspaceserver_usermods.sh
fi
```
4 If you are using Ubuntu stemcells, in order to link Ubuntu with the gss library, add the following lines to the `post_deploy_script` variable that you added in step 3. For improved readability, several commands in the following code occupy two lines. However, make sure that you enter the command on a single line.

```bash
post_deploy_script: |
  #!/bin/bash
  if [ -f /var/vcap/data/packages/sas-workspace/*/opt/sas/viya/config/etc/workspaceserver/default/workspaceserver_usermods.sh ]
    then
      sed -i /TKSECURE_GSSAPI_LIBRARY/d /var/vcap/data/packages/sas-workspace/*/opt/sas/viya/config/etc/workspaceserver/default/workspaceserver_usermods.sh
      echo 'export TKSECURE_GSSAPI_LIBRARY=/usr/lib/x86_64-linux-gnu/libgssapi_krb5.so' >> /var/vcap/data/packages/sas-workspace/*/opt/sas/viya/config/etc/workspaceserver/default/workspaceserver_usermods.sh
      sed -i /workspace_user/d /var/vcap/data/packages/sas-workspace/*/opt/sas/viya/config/etc/workspaceserver/default/workspaceserver_usermods.sh
    ...

Identify a CAS Administrative User

If you are performing a programming-only deployment and want to change the CAS administrative user from the default of cas to another user, you can define that user in the BOSH deployment manifest.

1 Open the BOSH deployment manifest.

2 Add the `ADMIN_USER` variable to the `cas_controller` block as shown in the following example.

   Note: The indentation is important. Ensure you use the same indentation that is shown in the example.

   ```yaml
   - name: cas_controller
     release: sas-bshvdmmlcas-<%= package_type %>
     provides:
       controller: {as: cas_controller}
     vm_type: <%= vm_type %>
     stemcell: <%= stemcell %>
     networks:
       - name: <%= private_network_name %>
         default: [dns, gateway]
       - name: <%= public_network_name %>
         static_ips: [<%= cas_controller_ip %>]
     properties:
       cas:
         key: <%= cas_key %>
   environment:
     ADMIN_USER: CAS-administrator-user-ID
     config:
       mode: <%= cas_mode %>
   ```

3 Save and close the BOSH deployment manifest.
Set the CAS Data Directory

The CAS data directory is the location that product caslibs are written to. For BOSH, it must be a location that persists across virtual machine restarts. The default location for the CAS data directory is `/var/vcap/store/cas_controller/data/cas/default`. If you want to change this location, ensure that the location that you choose also persists across restarts.

1. Open the BOSH deployment manifest.
2. Change the `datadir` variable in the `cas_controller` block as shown in the following example.

   ```yaml
   - name: cas_controller
     instances: 1
     jobs:
     ...
     properties:
       cas:
         workerips: <%= cas_worker_ips %>
         key: <%= cas_key %>
         datadir: path-to-CAS-data-directory
   ```

3. Save and close the BOSH deployment manifest.

CAS Settings

For a complete list of CAS server options that you can set in the `cas_controller` instance group under `cas.config`, see CAS Configuration File Options.

For a complete list of CAS environment variables that you can set in the `cas_controller` instance group under `cas.environment`, see CAS Environment Variables.

Establish Communication Between the SAS Embedded Process and CAS Worker Nodes

When using the SAS Embedded Process to load data in parallel, the SAS Embedded Process in Hadoop must be able to communicate with the CAS worker nodes. The CAS worker nodes must have IP addresses that are open for communication with the SAS Embedded Process. The sample BOSH deployment manifest creates communication paths through the general static IP addresses for the worker nodes.

However, there is an issue due to the location of these worker nodes being communicated from the CAS controller to the SAS Embedded Process. This means that the CAS controller has to communicate the public IP address to the SAS Embedded Process, but it is most often communicating to the worker nodes themselves via the private IP address. This issue will be resolved in a future SAS Viya release.

Until then, the workaround is to modify the `/etc/hosts` file to resolve the IP addresses. Your workaround strategy depends on how your software is administered. Consult with your Cloud Foundry administrator, your
IaaS administrator, and the SAS representatives assisting with your deployment for a workaround strategy. The SAS representatives can identify options that are available to you.

NFS Mount Options

Add NFS Mount Capability

SAS Viya on Cloud Foundry includes an NFS BOSH release that enables you to configure NFS details in the BOSH deployment manifest. You can set either of two properties in the global properties section:

- **nfs_mounts**, whose value is a space-separated list of mounted volumes:
  ```yaml
  properties:
    nfs_mounts: host-1:volume-1:mount-point-1 host-2:volume-2:mount-point-2...
  ```

- **fstab**, which enables you to control which file systems are mounted when the VMs are started. You enter the value of the `fstab` property in the `/etc/fstab` file in the form `file-system-specifier mount-point file-system-type [mount-options]` with one file system mount per line.
  ```yaml
  properties:
    fstab: |
    # file-system-specifier-1:/EXPORT path-to-local-1 nfs NFS-options
    # file-system-specifier-2:/EXPORT2 path-to-local-2 nfs NFS-options
  ```

The `nfs_mounts` property is recommended if you intend for BOSH to manage the VMs entirely. Use the `fstab` property if you might need to reboot the VMs from the infrastructure-as-a-service (IaaS) layer.

Remove NFS Mount Capability

In order to remove NFS mount capability at the initial deployment, perform the following steps:

1. In the properties section of the BOSH deployment manifest, comment out the `fstab` variable by adding number signs (`#`) at the beginning of each line. Here is an example:
   ```yaml
   properties:
   ... # fstab: |
   # TODO - Provide the contents of your desired /etc/fstab additions. This string
   # will be appended to the existing /etc/fstab file and a mount request issued.
   setinit:
   ```

2. In the `cas_controller`, `cas_worker`, and `object_spawner` sections of the BOSH deployment manifest, comment out the line that contains the following code:
   ```yaml
   - {name: install_config_nfs, release: sas-bshnfs-<%=package_type %>
   ```
   For example, the `cas_controller` section is modified as follows:
   ```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_numa, release: sas-bshnuma-<%= package_type %>
   ```
In the `releases` section of the BOSH deployment manifest, comment out the line that contains the following code:

```
"-{name: sas-bshnfs-<%= package_type %>, version: latest}
```

Here is an example:

```
releases:
  - {name: sas-bshconsul-<%= package_type %>, version: latest}
  - {name: sas-bshgeode-<%= package_type %>, version: latest}
  - {name: sas-bshjava-<%= package_type %>, version: latest}
  - {name: sas-bshlibpng-<%= package_type %>, version: latest}
  #-{name: sas-bshnfs-<%= package_type %>, version: latest}
  - {name: sas-bshnuna-<%= package_type %>, version: latest}
  - {name: sas-bshpgpool-<%= package_type %>, version: latest}
```

### Security Settings

SAS Viya for Cloud Foundry includes a BOSH release that configures System Security Services Daemon (SSSD) to integrate with your organization’s standard identity and authentication provider.

To use the SSSD BOSH release, you must set the following global properties in the BOSH deployment manifest:

- `sssd_cert` is the certificate that is used to interact with the supporting LDAP server, which is used for authentication. This certificate is written to `/etc/ssl/certs/sssd`
- `sssd_conf` specifies the contents of the sssd.conf file for the appropriate VMs that are used by the SAS Viya system. This configuration information is written to `/etc/sssd/sssd.conf`

Your site might use another method to integrate with its authentication provider. For example, Centrify is a typical security product. If you use another method, you would substitute your own release for the SAS SSSD release.

The sample BOSH deployment manifest that is included with your order uses the SSSD BOSH release.

### Apply the Setinit

SAS Viya uses a single licensing file that is specified in the BOSH deployment manifest. Unless you moved the license file after you uncompressed the TAR file from your Software Order Email, the license file is the text file in the `sas_viya_cloudfoundry` subdirectory. Copy the text from the license file and paste it to the BOSH deployment manifest as the value for `setinit:text`. Here is an example:

```
setinit:
  text: |
    PROC SETINIT RELEASE='V03';
    SITEINFO NAME='some-id-here'
    SITE=00000000 OSNAME='LIN X64' RECREATE WARN=30 GRACE=30
    ...
```

Note that the included text is passed to a SAS server and must be valid SAS code. If you are using the sample BOSH deployment manifest, make sure that you remove the YAML comment from the text before you paste it to the manifest.