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 ......................................... 3
   Virtual Machine and Platform Specifications .............................. 5
   Java Requirements ............................................................... 6
   Data Source and Storage Requirements ................................... 6
   User and Group Requirements ................................................ 7
   Security Requirements .......................................................... 8
   Client Requirements ............................................................ 8

Chapter 3 / Pre-Installation Tasks ............................................... 11
   Make Sure That You Have the Required Files ............................ 11
   Download the SAS Viya BOSH Releases ................................... 11
   Collect Pre-Deployment Information ...................................... 12

Chapter 4 / Installing SAS Viya ................................................... 15
   Upload Releases to the BOSH Director ...................................... 15
   Edit the Deployment Manifest ............................................... 16
   Use BOSH to Install .............................................................. 16
   Connect to Hadoop ............................................................... 17

Chapter 5 / Manual Configuration ............................................... 21
   Configure Your Environment with SAS Environment Manager .... 21
   Change the Administrative User Password for SAS Message Broker 24

Chapter 6 / Validating the Deployment ......................................... 27
   Validating the Cloud Foundry Deployment ................................ 27
   Log On to SAS Studio ............................................................ 28
   Access CAS Server Monitor .................................................... 28
   Verify SAS Infrastructure Data Server .................................... 28
   Verify SAS Message Broker ................................................... 30

Chapter 7 / Uninstalling SAS Viya ............................................... 31
   Uninstall the Deployment ....................................................... 31

Chapter 8 / Next Steps .................................................................. 33
   Refer to Additional Documentation ......................................... 33

Appendix 1 / Cloud Foundry Manifest Information .......................... 35
   Remove a Stemcell .................................................................. 35
   Differentiate between Multiple SAS Environments .................... 36
   Add the CAS Worker Nodes .................................................... 36
   Define Persistent Disks ............................................................ 37
   Ports ..................................................................................... 37
   Consul Settings ...................................................................... 38
   Integrate with Secure Hadoop through Kerberos ....................... 40
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 environment
- Data connector PC files
- Data connectors for Hadoop
  - SAS Data Connector to Hadoop, which enables serial processing between CAS and Hadoop
SAS Data Connector Accelerator for Hadoop, 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 17.

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 deployment manifest file.

**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

## 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/](https://www.cloudfoundry.org/certified-platforms/).

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Infrastructure Requirements</td>
<td>3</td>
</tr>
<tr>
<td>Overview of Cloud Infrastructure Requirements</td>
<td>3</td>
</tr>
<tr>
<td>Network Requirements</td>
<td>4</td>
</tr>
<tr>
<td>Runtime Environment</td>
<td>4</td>
</tr>
<tr>
<td>Orchestration Requirements</td>
<td>4</td>
</tr>
<tr>
<td>Stemcell Requirements</td>
<td>4</td>
</tr>
<tr>
<td>SAS Support for Alternative Operating Systems</td>
<td>4</td>
</tr>
<tr>
<td>Virtual Machine and Platform Specifications</td>
<td>5</td>
</tr>
<tr>
<td>Requirements for VMs Deployed by BOSH for Supporting Components</td>
<td>5</td>
</tr>
<tr>
<td>Requirements for Resources Allocated for Applications within the Elastic Runtime</td>
<td>5</td>
</tr>
<tr>
<td>Java Requirements</td>
<td>6</td>
</tr>
<tr>
<td>Data Source and Storage Requirements</td>
<td>6</td>
</tr>
<tr>
<td>Overview of Data Warehouse and Storage Requirements</td>
<td>6</td>
</tr>
<tr>
<td>Data Encoding Requirement</td>
<td>6</td>
</tr>
<tr>
<td>Supported Data Sources</td>
<td>6</td>
</tr>
<tr>
<td>Requirements to Import Data from SAS 9.4</td>
<td>7</td>
</tr>
<tr>
<td>User and Group Requirements</td>
<td>7</td>
</tr>
<tr>
<td>User Account Requirements</td>
<td>7</td>
</tr>
<tr>
<td>Security Requirements</td>
<td>8</td>
</tr>
<tr>
<td>Security Options</td>
<td>8</td>
</tr>
<tr>
<td>LDAP Server Requirements</td>
<td>8</td>
</tr>
<tr>
<td>Client Requirements</td>
<td>8</td>
</tr>
<tr>
<td>Web Browsers for SAS Viya User Interfaces</td>
<td>9</td>
</tr>
<tr>
<td>Mobile Platform Support</td>
<td>9</td>
</tr>
<tr>
<td>Database Drivers</td>
<td>9</td>
</tr>
</tbody>
</table>
Network Requirements

You can set a name for the private network in the BOSH cloud-config section of the deployment manifest. The default name for the externally visible network name for a SAS BOSH deployment is `public`. To change the name, you must define the property, `network.external.name`, in your BOSH 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.

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.

With Pivotal Cloud Foundry, Pivotal Elastic Runtime 1.10.x includes cf 252, which includes the service packs that SAS Viya requires. Pivotal Cloud Foundry Ops Manager 1.10.x includes BOSH Director 261.4, which supports SAS Viya.

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:

```bash
bosh releases
```

Orchestration Requirements

BOSH Director is required in order to install SAS Viya components. For information about the required versions of BOSH Director, see [https://support.sas.com/en/documentation/third-party-software-reference/viya/support-for-operating-systems.html#cf](https://support.sas.com/en/documentation/third-party-software-reference/viya/support-for-operating-systems.html#cf).

Stemcell Requirements

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

- Ubuntu Trusty 3363.19 or later. The following stemcells have been validated:
  - Amazon Web Services Xen-HVM
  - OpenStack KVM
- CentOS 3363.19 or later and based on CentOS 7.3. 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

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).
Virtual Machine and Platform Specifications

The requirements for virtual machines 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.

**Requirements for VMs Deployed by BOSH for Supporting Components**

<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>
<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>

* You can add more CAS workers by editing the deployment manifest. For more information, see “Add the CAS Worker Nodes” on page 36.

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:

**Requirements for Resources Allocated for Applications within the Elastic Runtime**

<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>51</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>
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. Alternative versions of the JRE, such as Azul Zulu or IBM SDK, Java Technology Edition, are also supported. For those vendors, the supported versions are also 1.8.x. 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 one or more SAS data connectors and a data connect accelerator on your CAS controller and CAS workers.

If your order for SAS Viya on Cloud Foundry included SAS In-Database Technologies for Hadoop, you should also have received a Software Order Email (SOE) for SAS Viya on Linux. Requirements and installation steps for Hadoop support are documented in the deployment guide that is provided as a link in the SOE. Refer to the “System Requirements” chapter of the SAS Viya on Linux 3.2: Deployment Guide for additional system requirements that apply to your Hadoop environment.

Data Encoding Requirement

UTF-8 is the only SAS session encoding that is supported by SAS Viya. If your DBMS encoding is non-UTF-8, the SAS software typically converts the data to UTF-8 to work with CAS processes. Additional settings, such as changes to environment variables, might be required if you are attempting to use a database with non-UTF-8 encoding.

You can also use SAS/CONNECT to transfer and automatically convert data from a non-UTF-8 encoded SAS session to the UTF-8 encoded SAS Viya environment. For information about how to convert data from non-UTF-8 to UTF-8, see Migrating Data to UTF-8.

Supported Data Sources

SAS Viya supports the following data sources:

- Hadoop
- PC files, which support the following file extensions:
  - .jmp
  - .spss
  - .stata
  - .xlsx or .xls
Note: Each data source also requires a data connector and possibly a data connect accelerator. Some data
connectors have individual system requirements. For additional requirements that apply to Hadoop data
connectors, see the “System Requirements” chapter of the SAS Viya on Linux 3.2: Deployment Guide.

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.

- SASHDAT on HDFS
- LASR Analytic Server (SAS 9.4)
- SAS data sets

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

Requirements to Import Data from SAS 9.4

SAS/CONNECT is required in the environment to move data from other SAS deployments and operating
systems to SAS Viya. SAS/CONNECT can convert data from a non-UTF-8 encoded SAS session to the UTF-8
format that SAS Viya requires.

SAS/CONNECT is always included with a standard SAS Viya order and is deployed automatically. However, a
license is required to enable it.

When you import SAS 9.4 data 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.

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 manifest file provides guidance for setting the required SSSD properties in your deployment manifest. For more information, see “Security Settings” on page 44.

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 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 38.

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

The SAS Studio and CAS Server Monitor user interfaces have identical web browser requirements. However, the visual user interfaces for SAS Visual Analytics, SAS Visual Statistics, and SAS Visual Data Mining and Machine Learning 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 the following website:

Mobile Platform Support

Support for mobile devices is not yet available for all SAS Viya user interfaces. For information about mobile device support, see the following website:

Database Drivers

Make sure that each client where users will access SAS software has the required database drivers already installed.
Pre-Installation Tasks

Make Sure That You Have 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, uncompress the file.

\texttt{tar xf SAS\_Viya\_Cloudfoundry.tgz}

A \texttt{sas\_viya\_cloudfoundry} subdirectory is added. It contains the following files:

- the license file
- the \texttt{entitlement\_certificate.pem} and \texttt{SAS\_CA\_Certificate.pem} files
- the \texttt{get-sas-viya-bosh-releases.sh} file
- the \texttt{sas-viya-vdmml-sample-manifest.yml} file, which is a sample deployment manifest file

Download the SAS Viya BOSH Releases

1. Run the \texttt{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:

\textbf{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.

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

- \texttt{sas-bshconsul-redhat.xxx.tgz}
- \texttt{sas-bshgeode-redhat.xxx.tgz}
- \texttt{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 SAS 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

1. Ensure that the BOSH Director is set as the target.
   
   ```
   bosh target URL-of-BOSH-Director
   ```

2. 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
   ```

3. 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
   ```
Edit the Deployment Manifest

Note: SAS Viya 3.2 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 Other Servers and Services: 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:

```bash
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.

```bash
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 manifest file 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:

  ```yaml
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:

  ```yaml
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:

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

b Throughout the manifest file, 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 deployment manifest that specifically matches your organization’s requirements. For details about specific deployment manifest settings, see “Cloud Foundry Manifest Information” on page 35.

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.

```bash
bosh deploy && bosh run errand microservices
```

**Note:** Check for failures in the log output from the BOSH errand.

---

### Connect to Hadoop

If your SAS Viya for Cloud Foundry order includes SAS In-Database Technologies for Hadoop, you also should have received an order for SAS Viya for Linux. The Linux deployment is used only to deploy the parts of the software that are required to connect to Hadoop by the Cloud Foundry deployment.

Using the [SAS Viya 3.2: Deployment Guide](#), deploy the Linux order with the following modifications in order to deploy only SAS In-Database Technologies for Hadoop from that order.

1 Go to the “Introduction” chapter.
   - If you plan to access data in Hive from SAS Viya, familiarize yourself with “Hadoop Scenario 1: Access to Data in Hive.”
   - If you plan to load and save data in HDFS as SASHDAT tables, familiarize yourself with the “Remote Access to HDFS” strategy under “Hadoop Scenario 2: CAS SASHDAT Access to HDFS.”
     **Note:** SAS Viya for Cloud Foundry supports remote access to SASHDAT in HDFS, but it does not support deploying CAS on Hadoop nodes.

2 Go to the “System Requirements” chapter.
   - Follow the steps in "Hardware Requirements for SAS Visual Analytics and SAS Visual Statistics (Requirements for Single-Machine Deployment, Programming Interface Only)."
   - Follow the steps in "Requirements for SAS Data Connector to Hadoop" or "Requirements for SAS Data Connect Accelerator for Hadoop," as appropriate.
   - Follow the steps in the "Set Up the cas Account" section.
     **Note:** Ensure that the sas and cas users are located on the machine on which you are installing the software.

3 Go to the "Pre-installation Tasks" chapter.
   Follow the steps in the "Set the ulimits" section to adjust ulimits, as necessary.

4 Go to the "Installing SAS Viya with Ansible" chapter.
   - Follow the steps in "Define the Machines in the Deployment" section, and define one target reference, which is the machine on which you are installing the software.
   - Follow the steps in "Assign Machines to Target Groups" section, and remove the machine name from all host groups except `[sas-casserver-primary]` and `[sas-all-children]`.
   - 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:

```bash
controller-1 ansible_host=host.example.com ansible_user=user1 ansible_ssh_private_key_file=*
```
Go to the "Install SAS Viya with Ansible" chapter.
Follow the steps in "Install Consul on CAS Hosts" section, and set `sas_consul_on_cas_hosts` to `false`.

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

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

7 After the deployment process is complete, choose the appropriate strategy:

- To enable access to data in Hive from SAS Viya, follow the steps in “Appendix D: Hadoop Deployment: Configuring SAS Access to Hadoop, SAS Data Connector to Hadoop and Optionally, the SAS Data Connect Accelerator for Hadoop.”

  Note: To install the JAR files on the CAS controller, follow the steps in "Install the Hadoop JAR Files Manually."

- To load and save data in HDFS as SASHDAT tables, follow the steps in "Appendix E: Hadoop Deployment: Configuring CAS SASHDAT Access to HDFS."

8 After the Hadoop library JAR files and configuration files have been collected from the Hadoop cluster, they must be made available to the CAS controller machine. Choose one of the following strategies:

- Build a custom BOSH stemcell that includes these files.
- Build a custom BOSH release that includes these files and that lays them down appropriately.
- Copy the files to a directory location that is accessible to NFS. Include that location in the `fstab` property of the manifest file so that the pathname is mounted on the virtual machines.
- Use the pre-deploy or post-deploy sections of the manifest file to copy the files from an accessible location to the virtual machine.

Note: Do not use the same pathname for `hadoop.client.config.filepath` and `hadoop.client.jar.filepath`. Each pathname must be unique. This is a requirement for both the Cloud Foundry deployment and the Linux deployment.

9 After the Hadoop files have been saved according to the strategy chosen from the previous step, you can remove the Linux deployment using the instructions in the SAS Viya 3.2: Deployment Guide. For any future update to the software, you can re-install SAS In-Database Technologies for Hadoop.
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
   
   Select 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. If the Configuration page of SAS Environment Manager is not already displayed, select Resources ➜ Configuration from the side menu ➔.

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.
      For each property that represents a user-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.

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.
      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.

6. From the SAS Environment Manager side menu, select Previous ➜ Users.
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.

### 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. On the Users page in SAS Environment Manager, select Custom Groups from the list in the toolbar.
2. In the left pane, click SAS Administrators.
3. In the Members section of the right pane, click , and add one or more members to the group (including your own account, if applicable).
4. Sign out from SAS Environment Manager so that you are no longer signed in as the sasboot user.
5. 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 23.

### Reset the sasboot Password and Disable the Password Reset Feature

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 Resources ➤ Configuration from the side menu .
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.

Restrict Folder Creation at the Root Level

SAS administrators are typically the only users who create folders at the root level. To restrict all other users from creating content at the root level, refer to “Restrict Creation of Top-Level Folders” in SAS Viya Administration: General Authorization.

Configure Security

After the deployment is complete, be aware that your system is not yet secured. For information about security, refer to the table in SAS Viya for Cloud Foundry: Operations.

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, locate the 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:
     consul:
   ```
server: false
join_hosts:
  - <%= consul_ip %>
rabbitmq:
  client:
  password: MySpecialPassword

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

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-vmml-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 Deployment

**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:

   ```bash
   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:

   ```bash
   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 deployment manifest file. For example, if you use the sample 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:

   ```bash
   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

Access CAS Server Monitor

Verify SAS Infrastructure Data Server

Verify SAS Message Broker
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 27.

   Here is an example:


   Log on using one of the SAS Administrator users that you established in "Set Up Administrative Users" on page 23.

   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:
bosh logs pgpool 2 --job

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 o IID dir, /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
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 27.

Here is an example:

Uninstalling SAS Viya

Uninstall the Deployment

1. 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.
   
   ```shell
   bosh delete deployment deployment-name
   ```
   
   You can find the deployment name in the manifest file:
   
   ```yaml
   name: sas-vdmml-stemcell-name
   ```

2. Create a list of the apps in the Elastic Runtime.
   
   ```shell
   cf apps | grep Cloud-Foundry-app-prefix
   ```
   
   The **Cloud-Foundry-app-prefix** is the value that you used in the manifest file for the `cf_app_prefix` variable.

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

4. Identify the releases that are used in the deployment.
   
   ```shell
   bosh releases
   ```

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

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

7. 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:
      
      ```shell
      bosh disks --orphaned
      ```
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.
Next Steps

Refer to Additional Documentation

Refer to Additional Documentation

- After you validate the deployment, you can perform initial administrative tasks. For details, refer to **SAS Viya on Cloud Foundry: Orientation**.
- For usage information, refer to the Help that is available from the SAS Viya product and administrative interfaces.
- Refer to the appendixes in this guide for additional tasks that you might perform, based on your environment.
Appendix 1

Cloud Foundry Manifest Information

Remove a Stemcell

Differentiate between Multiple SAS Environments

Add the CAS Worker Nodes

Define Persistent Disks

Ports

PostgreSQL Ports

Geode Ports

Consul Settings

Integrate with Secure Hadoop through Kerberos

Identify a CAS Administrative User

CAS Settings

Establish Communication Between the SAS Embedded Process and CAS Worker Nodes

NFS Mount Options

Add NFS Mount Capability

Remove NFS Mount Capability

Security Settings

Apply the Setinit

Remove a Stemcell

To remove a single type of stemcell from the manifest file:

1. In the Stemcell Management section of the manifest file, remove or comment out (by adding a number sign) the appropriate variables. For example, to remove CentOS stemcells, modify the section as follows:

```sh
# 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.

2. In the stemcells section, remove or comment out the appropriate variables. For example, to remove CentOS stemcells, modify the section as follows:

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

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

3 Save and close the manifest file.

Differentiate between 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 manifest. Ensure that the value for `cf_app_prefix` is unique for each SAS environment that is listed in the manifest. A unique value is prepended to each standard app name in order to differentiate between SAS environments.

Add the 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.config.mode` property is set to `mpp`. If you use the sample manifest, set the value of the `<%= cas_mode %>` variable to `mpp`.

- name: cas_controller
  . . .
  properties:
  cas:
    config:
      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 manifest, the value of the `<%= cas_worker_count %>` variable is calculated based on the number of addresses that you specify.

```bash
# 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 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 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 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 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 manifest using the variable `<%= postgres_config_port %>`, or you can set it specifically in the properties section of the `postgresql` instance definition.

```yaml
- name: postgresql
  ...
```
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 manifest using the variable `<%= pgpool_config_port %>`, 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 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 manifest, but you can override the default values by setting the following properties:

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

**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 manifest file.

```yaml
- name: consul
  properties:
    consul:
      ...
      key_value_data: |
        config:
          application:
            sas:
              url:
                httpd: http://Cloud-Foundry-host.Cloud-Foundry-domain
            sas.identities.providers.ldap.connection:
              host: your-LDAP-host
              password: your-LDAP-password
              port: your-LDAP-port
              url: ldap://\${sas.identities.providers.ldap.connection.host}:
                \${sas.identities.providers.ldap.connection.port}
        userDN: CN=your_CN_namespace,OU=your-OU-namespace,DC=your-DC-information
        sas.identities.providers.ldap.user:
          baseDN: your-base-DN
        sas.identities.providers.ldap.group:
          baseDN: OU=your-LDAP-group-names,DC=your-DC-information
        oauth2:
          adminId: sas.admin
          adminSecret: sas.admin.secret
```

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 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 %>` | custom-datacenter-name
```

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 %>` | custom-datacenter-name
```

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” in “SAS Viya for Cloud Foundry: Operations”.
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 manifest file:

   ```bash
   properties:
   ...
   java_home: <%= java_home %>
   pre_deploy_script: |
   #!/bin/bash
   rm -f /etc/krb5.conf
   touch /etc/krb5.conf
   echo '[logging]'
   default = FILE:/var/log/krb5libs.log
   kdc = FILE:/var/log/krb5kdc.log
   admin_server = FILE:/var/log/kadmind.log
   [libdefaults]
   default_realm = kerberos-domain-name
   dns_lookup_realm = false
   dns_lookup_kdc = false
   ticket_lifetime = 24h
   renew_lifetime = 7d
   forwardable = true
   ...
   [realms]
   kerberos-domain-name = {
   kdc = fully-qualified-domain-name
   admin_server = fully-qualified-domain-name
   }
   [domain_realm]
   .domain-name = kerberos-domain-name' >> /etc/krb5.conf
   ...

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
   properties:
   ...
   java_home: <%= java_home %>
   pre_deploy_script: |
   chgrp root /tmp
   rm -f /etc/krb5.conf
   touch /etc/krb5.conf
   ...
   ...

3. In order for the workspace server process to know about the auto-generated Kerberos token, add the following lines to the manifest file. 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
   properties:
   ...
   java_home: <%= java_home %>
   pre_deploy_script: |
   ...
   ```

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

1. Open the manifest file.

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.
CAS Settings

For a complete list of CAS server options that you can set in the cas_controller instance group under cas.config, see “Configuration File Options” in “SAS Viya for Cloud Foundry: Operations”.

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” in “SAS Viya for Cloud Foundry: Operations”.

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 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 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:

```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.

```plaintext
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 manifest file, comment out the `fstab` variable by adding number signs (`#`) at the beginning of each line. Here is an example:

   ```plaintext
   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 manifest file, comment out the line that contains the following code:

   ```plaintext
   - {name: install_config_nfs, release: sas-bshnfs-<%=package_type %>
   ```

   For example, the `cas_controller` section is modified as follows:

   ```plaintext
   - name: cas_controller
     instances: 1 # DO NOT CHANGE
     jobs:
     <% if programming_only == false %>
       - {name: consul, release: sas-bshconsul-<%= package_type %>
       <%
     <%
     <%
     ```

3. In the `releases` section of the manifest file, comment out the line that contains the following code:

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

   Here is an example:

   ```plaintext
   releases:
   - {name: sas-bshconsul-<%= package_type %>, version: latest}
   - {name: sas-bshgeode-<%= package_type %>, version: latest}
   - {name: sas-bshjava-<%= package_type %>, version: latest}
   - {name: sas-bsplibpng-<%= 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 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 manifest `sas-viya-vdmml-sample-manifest.yml` 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 manifest as the value for `setinit:text`. Here is an example:

```yaml
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 manifest, make sure that you remove the YAML comment from the text before you paste it to the manifest.