# Contents

**Chapter 1 / Introduction**                                      | 1
  - About This Guide                                               | 1
  - How Deployment Works                                           | 1
  - SAS Products and Supporting Components                        | 2
  - Contact SAS Technical Support                                   | 2

**Chapter 2 / System Requirements**                              | 3
  - Cloud Platform Software Requirements                           | 3
  - Supported Data Sources                                          | 4
  - Virtual Machine Operating System and Software Requirements      | 4
  - Security Requirements                                           | 6
  - Client Requirements                                             | 6

**Chapter 3 / Pre-installation Tasks**                           | 7
  - Enable Required Ports                                           | 7
  - Required NFS Mount Points                                       | 8

**Chapter 4 / Installing SAS Visual Investigator on SAS Viya**    | 9
  - Prepare the Installation Tools                                 | 9
  - Prepare the Installation Environment                           | 12
  - Install SAS Visual Investigator (Standard)                     | 17
  - Installing SAS Visual Investigator with Disaster Recovery      | 18

**Chapter 5 / Post-installation Tasks**                          | 21
  - Configure Your Environment with SAS Environment Manager       | 21
  - Configure and Onboard Initial Tenant                           | 24

**Chapter 6 / Validating the Deployment**                        | 29
  - Verify RabbitMQ                                                 | 29
  - Verify PostgreSQL                                               | 29
  - Validate Elasticsearch                                          | 30
  - Validate Consul                                                 | 30

**Chapter 7 / Completing the Deployment**                        | 33
  - Further Documentation                                          | 33

**Chapter 8 / Managing Your Software**                           | 35
  - Upgrade SAS Visual Investigator                                 | 35
  - Roll Back a Failed Upgrade                                      | 39

**Chapter 9 / Uninstalling SAS Viya**                            | 41
  - Uninstall SAS Viya                                              | 41

**Chapter 10 / Appendix A: Troubleshooting**                     | 43
  - BOSH                                                           | 43
  - Cloud Foundry Run Time                                         | 46
Contents
Introduction

About This Guide

Use this guide to deploy SAS Visual Investigator in a private cloud.

- Because the contents of this guide are subject to continual updates, make sure that you have the latest guide. You can always access the latest release of this guide from the following site:
  
  SAS Viya Deployment Guides

  If you accessed this guide directly from the Software Order Email, you are viewing the latest guide. If you are viewing a saved copy of the PDF version of this guide, the content might be outdated.

- To use this guide successfully, you should have a working knowledge of BOSH, Cloud Foundry, and VMware vSphere or OpenStack, depending on your environment.

How Deployment Works

SAS Visual Investigator takes advantage of industry-standard software and tools to deploy to the cloud.

- Cloud Foundry is the supported PaaS.

- VMware vSphere and OpenStack are the supported IaaS environments.

  Note: For vSphere environments, you can deploy SAS Visual Investigator to support disaster recovery. During this type of deployment, a secondary software stack, called the standby site, is made available for use in the event of a planned or unforeseen outage.

- BOSH is used to upload the required stemcells and releases for SAS Visual Investigator. After the stemcells and releases are in place, you will create files that are used in deploying the services and applications. Deploying SAS Visual Investigator consists of deploying stateful services to BOSH, and deploying stateless microservices to Cloud Foundry.

- The SAS Visual Investigator services and applications are packaged as a single file. You will access the container from a binary installer file that you download from SAS.
SAS Products and Supporting Components

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

- SAS Visual Investigator 10.4
- SAS Cloud Analytic Services (CAS), which is used as the run-time environment and the analytics server for SAS Visual Investigator
- SAS/ACCESS Interface to ODBC (on SAS Viya)
- SAS/ACCESS Interface to PostgreSQL (on SAS Viya)

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

CloudPlatformSoftwareRequirements

CloudFoundryRequirements........................................................................................................3
BOSHDirector..................................................................................................................................4
OtherRequiredThird-PartySoftware.................................................................................................4

SupportedDataSources..................................................................................................................4

VirtualMachineOperatingSystemandSoftwareRequirements.........................................................4
RequirementsfortheDeploymentMachine......................................................................................4
BOSHVirtualMachineRequirements...............................................................................................5

SecurityRequirements....................................................................................................................6
UserAccounts....................................................................................................................................6
Authentication.................................................................................................................................6

ClientRequirements......................................................................................................................6
WebBrowserRequirements..............................................................................................................6

Cloud Platform Software Requirements

Cloud Foundry Requirements

SAS Visual Investigator requires Cloud Foundry cf-deployment 1.0.16 or later.
The supported stemcell type is CentOS 3541.5, based on CentOS 7.x.
The following settings are required in your Cloud Foundry environment:

Table 2.1 Required Cloud Foundry Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required Value</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>max_package_size</td>
<td>9663676416</td>
<td>/instance_groups/name=api/jobs/name=cloud_controller_ng/properties/cc/packages/</td>
</tr>
<tr>
<td>maximum_app_disk_in_mb</td>
<td>4096</td>
<td>/instance_groups/name=api/jobs/name=cloud_controller_ng/properties/cc</td>
</tr>
<tr>
<td>maximum_health_check_timeout</td>
<td>900</td>
<td>/instance_groups/name=api/jobs/name=cloud_controller_ng/properties/cc</td>
</tr>
</tbody>
</table>
For additional information about the supported run-time environment and stemcells, see https://support.sas.com/en/documentation/third-party-software-reference/viya/34/support-for-operating-systems.html.

**BOSH Director**

BOSH Director is required in order to install SAS Viya components. BOSH Director provides cloud orchestration and management, including VM creation, deployment, and other software life cycle events. SAS Visual Investigator deployment uses BOSH manifest schema v2 only. BOSH CLI v2 2.0.48 or later is required.

- Set the value for `max_upload_size` to 20000m under the Blobstore and Director sections of the BOSH Director deployment manifest.
- Increasing the values for `max_threads` and `workers` properties can improve the performance of BOSH Director. The minimum recommended value for `max_threads` is 32, and for `workers`, 10.

**Other Required Third-Party Software**

The following third-party software is included with your SAS software:

- HashiCorp Consul – Enables service discovery and configuration.
- PostgreSQL – Creates the SAS Infrastructure Data Server, which stores user content such as reports, custom groups, audit records, and preferences.
- RabbitMQ – Provides an open-source, standards-based platform for SAS components and applications to send and receive messages.
- Elasticsearch – Provides search capabilities.
- SAS Cache Locator – Used for session caching.

**Supported Data Sources**

The following external data stores are supported by SAS Visual Investigator:

- Data sources accessible with an ODBC driver
- PostgreSQL 9.4

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.

**Virtual Machine Operating System and Software Requirements**

**Requirements for the Deployment Machine**

The VM instance or physical machine that is used to install SAS Visual Investigator has the following requirements:

- Red Hat Enterprise Linux or CentOS 7.2 or later must be installed.
The systemd-nspawn component must be installed.

50 GB of free space must be available.

**BOSH Virtual Machine Requirements**

The requirements for virtual machines are typically dependent on the number of users who access the SAS Visual Investigator environment and the amount of data that is imported and indexed. However, with SAS Visual Investigator for Cloud Foundry, requirements for the VMs that are deployed by BOSH are different from the requirements for resources that are dynamically allocated for applications within the Cloud Foundry Elastic Runtime environment. Although the Elastic Runtime runs on host VMs called *cells* in Cloud Foundry, VMs that are deployed by BOSH are referred to as *component VMs*.

BOSH component VMs are not dynamically allocated. Use the guidelines in the following table to allocate initial VM resources in BOSH:

<table>
<thead>
<tr>
<th>Role</th>
<th>VCPUs</th>
<th>Disk Space</th>
<th>RAM</th>
<th>Storage Volume (Minimum)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cache</td>
<td>4</td>
<td>40 GB</td>
<td>8 GB</td>
<td>20 GB</td>
</tr>
<tr>
<td>CAS Controller</td>
<td>2</td>
<td>20 GB</td>
<td>2 GB</td>
<td>20 GB</td>
</tr>
<tr>
<td>CAS Workers</td>
<td>8</td>
<td>40 GB</td>
<td>16 GB</td>
<td>20 GB</td>
</tr>
<tr>
<td>Consul</td>
<td>2</td>
<td>20 GB</td>
<td>2 GB</td>
<td>20 GB</td>
</tr>
<tr>
<td>Elasticsearch Master</td>
<td>2</td>
<td>20 GB</td>
<td>2 GB</td>
<td>20 GB</td>
</tr>
<tr>
<td>Elasticsearch Client</td>
<td>4</td>
<td>40 GB</td>
<td>4 GB</td>
<td>20 GB</td>
</tr>
<tr>
<td>Elasticsearch Data</td>
<td>16</td>
<td>40 GB</td>
<td>32 GB</td>
<td>20 GB</td>
</tr>
<tr>
<td>PgPool</td>
<td>8</td>
<td>40 GB</td>
<td>8 GB</td>
<td>20 GB</td>
</tr>
<tr>
<td>PostgreSQL</td>
<td>16</td>
<td>40 GB</td>
<td>32 GB</td>
<td>20 GB</td>
</tr>
<tr>
<td>RabbitMQ</td>
<td>4</td>
<td>40 GB</td>
<td>4 GB</td>
<td>20 GB</td>
</tr>
</tbody>
</table>

The size of the storage volume shown is the minimum amount. For CAS workers, Elasticsearch data, and the PostgreSQL database (SAS Infrastructure Data Server), you will need to adjust the size of the volume to accommodate the amount of data that is generated by end users. You can determine this amount based on the number of users and their expected usage levels.

If you decide to use a single VM for CAS, and use only the controller node without workers, follow the guidelines for CAS workers that are provided in the table.

**Note:** For Scenario Administrator flows, the recommended sizing of all CAS workers for a single CAS instance uses the following formula:

\[
\text{size of the data in GB} \times \text{number of users of Scenario Administrator} \times 15
\]
Security Requirements

User Accounts

The user account that is used to perform the deployment process must have sudoers privileges and a home directory.

SAS Viya requires a predefined user account that enables the administrator to log on after the deployment has completed. This account is called viadmin in this document. Before the deployment process is started, the viadmin user account must exist as a valid LDAP user.

The administrator creates groups for users as well as a group for administrators by adding users and groups through the Administration interface.

Authentication

SAS Visual Investigator supports LDAP for user authentication. Microsoft Active Directory and OpenLDAP are supported LDAP implementations. In addition, the CAS server uses OAuth tokens for all clients in your deployment.

Before SAS Visual Investigator is deployed, ensure that these requirements have been met:

☐ Make sure that SAS Visual Investigator users are able to authenticate to your LDAP provider.

☐ Make sure that SAS Visual Investigator has Read access to your LDAP server.

Note: To bind to the LDAP server, SAS Visual Investigator requires a userDN and password. LDAP anonymous binding is not supported.

☐ (Optional) If you are deploying multi-tenancy, verify that tenants are set up in LDAP. Use the documentation that is appropriate for your LDAP implementation to set them up.

After the deployment has completed, the designated administrator uses SAS Environment Manager to configure the authentication providers. For more information, see “Configure Your Environment with SAS Environment Manager” on page 21.

The administrator then logs on to the SAS Visual Investigator Administration interface as the viadmin user in order to manage user accounts and groups. For more information, see Managing Users, Groups, and Capabilities in SAS Visual Investigator: Administrator’s Guide.

Client Requirements

Web Browser 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.

For information about supported web browsers to access SAS Visual Investigator user interfaces, see https://support.sas.com/en/documentation/third-party-software-reference/viya/34/support-for-web-browsers.html.
Pre-installation Tasks

Enable Required Ports

The following ports are used by SAS Visual Investigator and should be available before you begin to deploy your software. The same ports should also be available for any firewalls that are configured on the operating system or the network.

<table>
<thead>
<tr>
<th>Process</th>
<th>Required Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPD</td>
<td>80 (internal)</td>
<td></td>
</tr>
<tr>
<td>default Erlang Port Mapper Daemon (epmd) port</td>
<td>443 (external)</td>
<td></td>
</tr>
<tr>
<td>SAS Infrastructure Data Server</td>
<td>5430–5439</td>
<td>For a single server deployment with no failover, ports 5430-5432 must be opened. Additional standby nodes each get the next available port number sequentially up to 5439.</td>
</tr>
<tr>
<td>CAS Server Starting Port</td>
<td>5577</td>
<td>Used by clients to make binary connections to CAS.</td>
</tr>
<tr>
<td>CAS Communicator Port</td>
<td>5580</td>
<td></td>
</tr>
<tr>
<td>SAS Messaging Broker</td>
<td>5671, 5672, 15672, 25672</td>
<td></td>
</tr>
<tr>
<td>SAS Configuration Server</td>
<td>8300–8309, 8500 and 8501</td>
<td>SAS uses HashiCorp Consul as its configuration server. All Consul ports should be open to TCP and UDP traffic.</td>
</tr>
<tr>
<td>Object Spawner</td>
<td>8591</td>
<td></td>
</tr>
<tr>
<td>CAS Server Monitor</td>
<td>8777</td>
<td>Used by clients to make REST HTTP calls to CAS, as with the Python REST interface.</td>
</tr>
<tr>
<td>Process</td>
<td>Required Port</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Elasticsearch</td>
<td>9200</td>
<td></td>
</tr>
<tr>
<td>Default PgPool port</td>
<td>9432</td>
<td></td>
</tr>
<tr>
<td>SAS Cache Locator</td>
<td>10335</td>
<td></td>
</tr>
<tr>
<td>SAS/CONNECT Spawner</td>
<td>17551</td>
<td></td>
</tr>
<tr>
<td>SAS Cloud Analytic Services Server</td>
<td>19990-19999</td>
<td></td>
</tr>
<tr>
<td>SAS Cache Server</td>
<td>40404</td>
<td></td>
</tr>
</tbody>
</table>

**Required NFS Mount Points**

The following mount points are required on the NFS server before you begin deploying your software.

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Directory on the NFS Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAS</td>
<td>license</td>
</tr>
<tr>
<td>PostgreSQL</td>
<td>postgresql</td>
</tr>
<tr>
<td>Elasticsearch</td>
<td>elasticsearch</td>
</tr>
</tbody>
</table>

**Note:** The directory names must exist on the NFS server before deployment.
Installing SAS Visual Investigator on SAS Viya

Prepare the Installation Tools
- Download the Binary Installer File
- Unzip the Downloaded File
- Extract the Binary File
- Start the Container
- Sign On to the Container
- Access Product Help

Prepare the Installation Environment
- Set the Site Name
- Edit the Configuration Files
- Save the Configuration File
- Authenticate to Cloud Foundry and BOSH
- Upload the BOSH Stemcells
- Upload the BOSH Releases
- (Optional) Set the Replication Configuration
- Create the Files for Deployment
- Prepare to Examine the Files
- Examine the Files Related to BOSH
- Examine the Files Related to Cloud Foundry
- Using Logs

Install SAS Visual Investigator (Standard)
- Overview
- Deploy the Stateful Services to BOSH
- Deploy the Stateless Applications and Microservices

Installing SAS Visual Investigator with Disaster Recovery
- Prepare the Standby Site
- Install the Standby Site

Prepare the Installation Tools

Download the Binary Installer File
Download the binary installer file to a physical machine or a virtual machine (VM) that has access to the IaaS environment. The VM is used as the secure administration host (jump server) for the installation.
Download the binary installer file sas.bin to the `/home/installer-ID` directory on the jump server. For example, if the binary installer file has been placed on a web server, you can use the `wget` command to download the binary installer file. Here is an example:

```bash
wget http://0.0.0.0/visualinvestigator__10_4__xxx_lax.zip
```

Note: `xxx` represents digits that are provided automatically. Use this value in subsequent commands.

## Unzip the Downloaded File

Unzip the downloaded file using the `unzip` utility:

```bash
unzip visualinvestigator__10_4__xxx_lax.zip
```

## Extract the Binary File

After the downloaded file has been unzipped, extract the binary file:

```bash
bash visualinvestigator__10_4__xxx_lax.bin
```

Here is an excerpt of the results:

Validating archive...
Extracting to `/home/test/sas`...

The installer creates a top-level directory named `sas`, which contains two subdirectories: `bin` and `image`.

Here are typical results:

```
2016-06-20 14:53:04 -- http://10.120.16.120/visualinvestigator__10_4__xxx_lax.zip
Connecting to 0.0.0.0:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5508425807 (5.1G) [application/octet-stream]
Saving to: 'visualinvestigator__10_4__xxx_lax.zip'
100%[=============================================] 5,508,425,807 74.4MB/s in 1m 43s

2016-06-20 14:54:47 (50.8 MB/s) - 'visualinvestigator__10_4__xxx_lax.zip' saved [5508425807/5508425807]
```

**bin**
- consists of a single Bash script named `start`.

**image**
- is a systemd-nspawn namespace container that is invoked by the `start` Bash script and contains functionality that is used in deployment activities for SAS Visual Investigator. The container can be shut down and restarted whenever these functions are needed.
- In addition, the entire container, with any changes that are made, can be repackaged, archived, or moved to another server or a VM as needed.

## Start the Container

To start the container, run the `start.sh` script from the user’s home directory:

```
./sas/bin/start
```

Here are typical results:

Starting SAS Visual Investigator Deployment Container...
Spawning container <instance>.<hostname>.unx.sas.com on /home/test/sas/image.
Press `^C` three times within 1s to kill container.
```
systemd 219 running in system mode. (+PAM +AUDIT +SELINUX +IMA -APPARMOR +SMACK +SYSVINIT +UTMP
```
Sign On to the Container

1. After the container is started, a login prompt is displayed:

   CentOS Linux 7 (Core)
   Kernel 3.10.0-862.3.2.el7.x86_64

   npl40801 login: sas

2. At the prompt, enter the user ID `sas` and then enter this password in the specified casing `XyZZy`.

   After you sign on successfully, the screen appears as follows:

   Last login: Wed Jun 15 12:41:34 on console

   Site Unset 12:23:56 !4 [-]

   The prompt now includes the string, Site Unset, followed by a timestamp. The Z shell (zsh) is set automatically. It is the standard shell for a SAS Visual Investigator deployment.

   **Note:** You should change the password immediately.

   **Note:** Do not change shells. Any other shell might produce unexpected results.

   The window of your X terminal emulator displays the title `Container`. The title is a reminder that your work environment is within the container and that you are no longer working within the host system.

Access Product Help

To access Visual Investigator help, run the following command:

   `sas help -g`

To show product information, run the following command:

   `sas show info`

Here is the output:

   SAS Visual Investigator : Info

   Product
   Name : SAS Visual Investigator
   Version: 10.4.xxxx
   Build Date: 2018-2-7.xxxxxxx

   Note: The information displayed by the `sas show info` command will change after loading the data from the JSON configuration file.

   For more details about your configuration, run the following command:

   `sas conf use configuration-filename`
Prepare the Installation Environment

Set the Site Name

The site name uniquely identifies your deployment. The container can manage multiple deployments at different sites. This enables you to manage development, test, and production environments from a single deployment container. You can also manage a paired set of sites that will act as a warm backup for disaster recovery.

To set the site name, run the command:

```
sas site set site-name
```

The name can contain only lowercase alphabetic characters, numbers, and hyphens. Nonalphanumeric characters, including a space, are not allowed. SAS recommends a site name that is three to ten characters long.

The site name will also be used as the datacenter name in Consul.

Note: Once the site name has been set, it will appear at the far left side of the prompt, replacing the initial value, Site Unset.

Set the Configuration File

1. You must choose a template file as a basis for the configuration file that you will set, edit, and save. To list the available template files, run the command:

```
sas conf list
```

Here are the results:

```
SITE CONFIGURATIONS:
SYSTEM CONFIGURATIONS:
    openstack
    vsphere
SEE ALSO:
    sas conf set <configurationName>  Change the active configuration
```

2. Select the template file (vSphere or OpenStack) that corresponds with the underlying IaaS for your Cloud Foundry installation and run the following command:

```
sas conf set configuration-name
```

where `configuration-name` is any of the system configurations listed by the `sas conf list` command. If you intend to use disaster recovery, specify the `vsphere` configuration value.

3. Save the configuration file with a new configuration filename that is meaningful in your environment.

```
sas conf save file-name
```

Here is the output:

```
Saved configuration file: file-name
```

4. Set the new configuration file as the active configuration file for the framework to use.

```
sas conf set filename
```

Here is the output:

```
Now using configuration: filename
```
Edit the Configuration Files

Once the template file is ready to use, edit the configuration file using the vim editor, using the following command:

```
sas conf edit
```

**Note:** SAS has configured the vim utility to check JSON syntax. If the file contains invalid JSON syntax, you will be notified when you exit the utility.

Save the Configuration File

To save the changes that you have made to a permanent location, run the following command:

```
sas conf save file-name
```

Here is the output:

```
Saved configuration file: file-name
```

This command does not change the active configuration file. Instead, it saves a copy of it to a saved configuration directory. A more direct way to get the configuration name is to run the command:

```
sas conf name
```

Here is the output:

```
single
```

Authenticate to Cloud Foundry and BOSH

Now that you have entered the information about your Cloud Foundry installation and the servers to be created, you need to connect to Cloud Foundry. This step is required even if the jump server is signed on to Cloud Foundry and BOSH. This step is also required whenever you change your configuration to a new configuration that has different authentication details.

To authenticate, run the command:

```
sas cf auth
```

Here is typical output:

```
BOSH Authentication
Using environment '1.1.1.1' as client 'admin'

Name    ocfdeploy
UUID    1a23456a-aaaa-78cc-bbbb-910a2b3cefg4
Version 264.7.0 (00000000)
CPI     vsphere_cpi
Features compiled_package_cache: disabled
cfgserver: disabled
dns: enabled
snapshots: disabled
User    admin

Succeeded

Cloud Foundry Authentication
api endpoint: https://api.run.xxx.test.com
api version: 2.103.0
```
If authentication is successful, then you know that the data that you entered for the Cloud Foundry and BOSH environments is correct. If authentication is not successful, refer to the data that you entered for the director and run-time sections of the configuration file. Correct them for your installation and try again.

CAUTION! If you do not have a working connection to both BOSH and Cloud Foundry, do not continue to the next section.

Upload the BOSH Stemcells

Once connectivity to the BOSH environment is established, you must upload the required stemcells for the creation of virtual machines (VMs). This is done in the IaaS using the BOSH Cloud Provider Interface (CPI).

1. Check to see whether the required stemcells are already installed. Run the following command:

   ```
   bosh -e environment-alias stemcells
   ```

   The `environment-alias` is one of the System Configurations listed in the output when you ran the `sas conf list` command in “Set the Configuration File” on page 12.

   If the output contains the following information, the correct stemcell is already installed. You can skip the remainder of this section.

   ```
   Name="bosh-openstack-kvm-centos-7-go_agent"
   Version="3541.5"
   ```

2. If the `bosh-openstack-kvm-centos-7-go_agent` stemcell is not installed, run the following command:

   ```
   sas deploy stemcells
   ```

   Two stemcells are delivered: one each for OpenStack and vSphere.

3. To ensure that the correct stemcells are loaded, even if there are existing stemcells, run the following command:

   ```
   sas bosh upload stemcells
   ```

   If the correct stemcells are already installed, you receive a warning message stating that the correct version already exists. You can safely ignore this message and continue with the upload.

Upload the BOSH Releases

Now you need to upload the included BOSH releases to the BOSH blob storage so that they are available to BOSH when it is time to deploy the services.

To upload the BOSH releases, run the following command:

   ```
   sas deploy releases
   ```

The following release packages are delivered, one for each of the stateful services.

- Cloud Analytic Server (CAS)
- Consul
- Elasticsearch
- PGPool
- PostgreSQL
- RabbitMQ
(Optional) Set the Replication Configuration

This setting permits your deployment to use disaster recovery, and it enables you to add the standby site when you are ready. If your system is enabled for disaster recovery, you do not have to create the standby site immediately. The standby instance can be created at any convenient time in the future.

**Note:** You must enable your deployment for disaster recovery before deploying the software. Disaster recovery works by copying important data from the active site to a standby site, where it can be used if the active site goes down. Configuring replication permits your deployment to use disaster recovery. For more information about disaster recovery and the standby site, see "Installing SAS Visual Investigator with Disaster Recovery" on page 18.

To set the replication configuration:

1. Establish the replication pattern from the active site to the standby site.
   ```bash
   sas replicate set active-site-name to standby-site-name
   ```
2. Save the configuration.
   ```bash
   sas conf save
   ```
3. Synchronize the active site's configuration data with that of the remote location.
   ```bash
   sas site sync -v
   ```
   The data is synchronized to the `/sites` directory. The `-v` flag is optional and is used to show all the files that are synchronized.

Create the Files for Deployment

Once the stemcells and releases are in place, you must create files that are used in deploying SAS Visual Investigator services and apps. This step should be performed each time there is a change in the active configuration file.

The configuration file provides the values to be substituted into the template files that are part of the framework. To create the file system and files, run the following command:

```bash
sas deploy files
```
As the command runs, it copies the JAR files that will be deployed in Cloud Foundry. Then it performs the token substitution on the various files that are required for deploying the solution.

When file creation is complete, token substitution is checked to determine whether there are any unresolved tokens. If tokenization is successful, the message *All tokens successfully resolved* is displayed. If tokenization is incomplete and an error message is shown, the configuration file is incomplete and needs to be edited again.

Prepare to Examine the Files

Examination of the BOSH and Cloud Foundry manifest files is required in order to verify that the information in the files is correct. You must have knowledge about the Cloud Foundry environment and the vim utility.

**Note:** Do not change the information in the manifest files manually because the data comes from the configuration file. Any changes should be made to the configuration file. The contents of the `site-name` directory should then be deleted, and the command to deploy files should be rerun to create a new set of manifest files.
Examine the Files Related to BOSH

The manifest files that deploy stateful services into the BOSH managed environment are located in the `/home/sas/site-name/services` directory in the container.

To examine the manifest files:

1. Change to the `/home/sas/site-name/services` directory.
2. Run the following command to display the vim editor:
   ```
   vi */man*.yml
   ```
   This displays the vim editor in the window, with the first file in the vim buffer. Use the `vim:n` command to edit the next file match. Use the `:rew` command to rewind to the beginning if you want to review all files again.

Note: It is acceptable to change the configurable entries in the jobs section of the manifest.yml file, which is in the Postgres directory under the `services` directory. They are intended to be managed outside the framework.

When examining the manifest files, check the following items:

- Make sure that `director_uuid` matches what was entered in the configuration file.
- Verify that the IP address is the correct one entered for each server. Look under `jobs` and then `static_ips`.

Once you have examined the BOSH manifest files, examine the script files in the services directory. To examine the script files:

1. Change to the `/home/sas/site-name/services` directory.
2. Run the following command to display the vim editor:
   ```
   vi */*.sh
   ```
   The most important script in this group is the `post_deploy_consul.sh` script. In this file, check for empty values ("") and determine whether an empty value is reasonable. Some expected empty values include the `archivelocation.storage.local.destination` property and in the `Folder` loop at the bottom of the file. A property with an empty value might indicate that a JSON property in the configuration file was not specified. If you discover any entries like this, return to the configuration file and make sure that all required entries are completed. Then delete the contents of the home directory and re-create the files.

Note: The following `service_tag` parameters are blank for all environments: `elasticsearch/deploy.sh service_tags`, `postgres/deploy.sh service_tags`, and `rabbitmq/deploy.sh service_tags`. This is standard and can be ignored.

Note: If you are using OpenStack, the static_ips addresses in the `cas-worker.yml` and `manifest-data.yml` files are blank. This is standard for OpenStack and can be ignored.

Examine the Files Related to Cloud Foundry

Manifest files that deploy stateless applications and microservices into the Cloud Foundry run-time environment are located in the `/home/sas/apps` directory in the container.

To examine the manifest files:

1. Change to the `/home/sas/site-name/apps` directory.
2. Run the following command to display the vim editor:
   ```
   vi */man*.yml
   ```
In these files, check for empty values (""') and determine whether an empty value is reasonable. This might indicate that a JSON property in the configuration file was not specified. If you discover any entries like this, return to the configuration file and make sure that all required entries are completed. Then delete the directories under the/home/sas directory and re-create the files.

Using Logs

Log data for applications and microservices is provided through the Cloud Foundry Loggregator system. Using a Cloud Foundry firehose and nozzle to collect log data and to redirect it to a logging server is the standard method of providing access to application logs. The rsyslog logging service has been added to the services that are deployed in Cloud Foundry BOSH. This information can be routed to any rsyslog server over TCP. This method is compatible with any of the various log store and display applications.

Install SAS Visual Investigator (Standard)

Overview

Installing SAS Visual Investigator consists of the following tasks:

- Install the stateful services to BOSH.
- Install the stateless applications and microservices.

Deploy the Stateful Services to BOSH

To deploy the stateful services to BOSH, run the following command:

```
sas deploy services
```

When deployments are complete, test the applications to ensure that the installation is working as expected. For more information, see “Validating the Deployment” on page 29.

**CAUTION!** Do not proceed to the next task if you see any errors during the installation of the stateful services. For error recovery, see “Appendix A: Troubleshooting” on page 43.

Deploy the Stateless Applications and Microservices

1. To Install the stateless applications and microservices, run the following command:

```
sas deploy apps
```

This command is similar to the command that installs the stateful services. The `sas deploy apps` command runs the `deploy.sh` script in the /home/sas/apps directory. This script executes each of the `deploy.sh` scripts in the subdirectories under the apps directory. These scripts deploy application JAR files in the Cloud Foundry run-time environment.

2. To display the status of the full installation, run the following command:

```
sas show status
```

_Note:_ The `sas show status` command implicitly performs a status check of the VMs and it also runs the `cf apps` and `cf routes` commands. To ensure that all applications are fully started, run the command:

```
sas show instances.
```
This will return the actual state of the applications within the Cloud Foundry runtime.

3 Run the following command to display information about the installed applications:

```
sas show info
```

The results include information about the product, the configuration, the URLs that enable you to connect to the application interfaces, and the environment. All the information is surfaced from the configuration file.

4 To ensure that the stateful services and applications are up and in a satisfactory condition, run the command,

```
sas show details
```

This will check the applications’ health endpoint for each application and also show the health status of the stateful services as reported to Consul.

Here is an excerpt of typical output:

```
Service Status

  pass cas-acme-default (Success)
  pass cas-shared-default (Success)
  pass consul -111-222-7-86 (Agent alive and reachable)
  pass consul -111-222-7-87 (Agent alive and reachable)
  ...

App Status

  pass audit (UP)
  pass authorization (UP)
  pass datahub (UP)
  pass entityResolution (UP)
  ...
```

---

**Installing SAS Visual Investigator with Disaster Recovery**

Deployments with disaster recovery enabled are designed to use two sites: active and standby. After SAS Visual Investigator is deployed, the active site contains the full software stack (SAS Viya and SAS Visual Investigator). The standby site contains a similar set of machines and services. The stateful services (PostgreSQL, Consul, RabbitMQ, CAS, and Elasticsearch) are deployed and running. Data replication occurs for the PostgreSQL database and Consul KV stores. Stateless services (also referred to as microservices) are deployed to the Cloud Foundry Runtime Environment in a stopped state, and are also configured to leverage the currently selected standby microservices. Because the microservices are stopped, the SAS Visual Investigator web interface is not accessible to the standby site.

Performing the steps in this chapter up to this point installs the active site. This section describes the steps that are required to install the standby site. It assumes that the active site has been installed.

**Prepare the Standby Site**

1 Switch to the standby site.

```
sas site set standby-site-name
```

2 Select the JSON template for the standby site.

```
sas conf set vsphere-multi
```
3 Save the configuration file with a new configuration filename that is meaningful in your environment.
   
   ```bash
   sas conf save standby-site-configuration-file-name
   ```

   Here is the command output:
   
   ```
   Saved configuration file: filename
   ```

4 Set the new configuration file as the configuration file for the environment to use.
   
   ```bash
   sas conf set standby-site-configuration-file-name
   ```

   Here is the command output:
   
   ```
   Now using configuration: filename
   ```

5 Establish the replication pattern from the active site to the standby site.
   
   ```bash
   sas replicate set active-site-name to standby-site-name
   sas site import keys active-site-name
   ```

6 Save the configuration.
   
   ```bash
   sas conf save
   ```

7 Synchronize the active site's configuration data with the remote location.
   
   ```bash
   sas site sync -v
   ```

   The data is synchronized to the `sites` directory. The `-v` flag is optional and is used to show all the files that are synchronized

---

**Install the Standby Site**

1 If you are not already on the standby site, switch to it.
   
   ```bash
   sas site set standby-site-name
   ```

2 Change the configuration to the file created for the standby site.
   
   ```bash
   sas conf set standby-site-configuration-file-name
   ```

3 Authenticate Cloud Foundry.
   
   ```bash
   sas cf auth
   ```

4 Verify that the IP addresses are correct.
   
   ```bash
   sas show info
   ```

5 Since the standby site must use the same keys as the active site, import those keys to the standby site.
   
   ```bash
   sas site import keys active-site-name
   sas conf save
   sas site sync
   ```

6 Deploy the files.
   
   ```bash
   sas deploy files
   ```

7 Deploy the stateful services.
   
   ```bash
   sas deploy services
   ```

8 Deploy the stateless applications and microservices.
   
   ```bash
   sas deploy apps
   ```

9 Display information about the installed applications.
   
   ```bash
   sas show info
   ```
Post-installation Tasks

Configure Your Environment with SAS Environment Manager

When the deployment process has completed, use SAS Environment Manager to set up an LDAP identity provider.

Sign In as the sasboot User

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

1. To display information about your deployment, run the following command:
   ```
sas show info
   ```
   The output will display the URL for SAS Environment Manager.

2. Sign in to SAS Environment Manager using the URL provided with the sasboot credentials.
   ```
   http://deployment-host.deployment-domain/SASEnvironmentManager
   ```

3. 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

You must configure the connection to your identity provider before your users can access SAS Environment Manager and SAS Visual Investigator. 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 more information about properties, see “sas.identities.providers.ldap” in SAS Viya Administration: Configuration Properties.
1. Select the from the side menu.

2. On the Environment page, 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:
   - 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.

   - Click **Save**.

4. In the `sas.identities.providers.ldap.group` section, click 📋. In the New Configuration window, do the following:
   - 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.

   - Click **Save**.

5. In the `sas.identities.providers.ldap.connection` section, click 📋. In the New Configuration window, do the following:
   - 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.

   - Click **Save**.

6. From the SAS Environment Manager side menu, select **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.

---

**Configure the Connection to the Mail Service**

Complete these steps while you are signed in as the sasboot user.

1. Select the from the side menu.
On the Environment page, select **Basic Services** from the list, and then select **Mail service** from the list of services.

In the **sas.mail** section, click 💻. In the Edit Configuration window, follow these steps:

- 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.
- Click **Save**.

(Optional) To enable the health check for the mail service, perform the following steps.

- Select the 📊 from the side menu 📊.
- On the Environment page, select **Basic Services** from the list, and then select **Mail service** from the list of services.
- In the **management.health.mail** section, click 📊.
- Turn the enabled toggle to **on**.
- 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 that 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. 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** Because 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:
Sign in as one of the SAS Administrators that you set up in “Set Up Administrative Users” on page 23.

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.
2. On the Environment 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 and Onboard Initial Tenant

1. Edit the tenant JSON template by running the following command:
   
   ```
   sas conf edit templates tenant-ID
   ```

2. Specify the tenant properties. Here is an example of an edited JSON file:
   
   ```
   
   # Selection: tenants > tenant-id
   
   (  
     # Title: Tenant identifier
     # Description:
     #    The identifier for a tenant
     # Required
     # Type: string
     "tenant_id": "",

     # Title: Tenant name
     # Description:
     #    The name for a tenant
     # Required
     # Type: string
     "name": "",
   ```
# Title: Tenant admin user name
# Description:
#   The name of the admin user for the tenant
# Required
# Type: string
"admin_user": "",

# Title: Tenant admin user password
# Description:
#   The password for the tenant admin user
# Required
# Type: string
"admin_password": "",

# Title: IP Address for the PgPool Instance
# Description:
#   IP Address for the PgPool Instance
# Required
# Type: string
# Format: ip-address
"pgpool_ip_address": "1.1.1.1",

# Title: Tenant PostgreSQL super user name
# Description:
#   The name of the PostgreSQL user for the tenant database
# Required
# Type: string
"pg_super_user": "",

# Title: Tenant PostgreSQL super user password
# Description:
#   The PostgreSQL super user password for the tenant database
# Required
# Type: string
"pg_super_password": "",

# Title: Tenant PostgreSQL user name
# Description:
#   The name of the PostgreSQL user for the tenant database
# Required
# Type: string
"pg_username": "",

# Title: Tenant PostgreSQL password
# Description:
#   The PostgreSQL password for the tenant database
# Required
# Type: string
"pg_password": "",

# Title: CAS Mode
# Description:
#   The Mode that the CAS server will run in either SMP or MPP
# Required
# Type: string
# Examples:
# Title: Storage Class
# Description:
# The Kubernetes storage class name
# Required
# Type: string
"cas_storage_class": "cas-storage",

# Title: Persistent Volume Claim Size
# Description:
# The Kubernetes persistent volume claim size
# Required
# Type: string
"cas_volume_size": "2Gi",

# Title: Number of CAS Workers
# Description:
# The number of CAS workers
# Type: integer
"cas_workers": 0
}

3 Save the file.

4 If you have a PostgreSQL user ID and password, establish the tenant PostgreSQL user ID in PgPool. To configure each user within each PgPool instance:

a To configure the PgPool instance:
   cd /home/sas/site-name/services/postgres_ha
   bosh deployment manifest_two_pgpools.yml
   bosh -d manifest_two_pgpools.yml ssh

b Choose a PGPool instance:
   sudo pg_md5 --username 'new-tenant-user-ID' --md5auth --prompt
   Password: new-tenant-password
   exit

5 To verify that all Consul services and applications have a passing status:
   sas show details

6 Create the tenant database role:
   sas create tenant database role tenant-ID
   
   Here is an example where acme is the tenant name:
   sas create tenant database role acme

7 Create the tenant database:
   sas create tenant database tenant-ID

8 Create the tenant CAS instance:
   sas create cas cluster tenant-ID

   Verify that the cluster is active:
   sas get cas cluster tenant-ID
Note: It can sometimes take 1–2 minutes before the status changes to “running.”

9 Onboard the initial tenant:

```bash
sas onboard tenant tenant-ID
```

10 Check the status of the initial tenant by running one of the following commands:

```bash
sas tenant status -t tenant-ID --detail
sas tenant status --all --detail
```

11 (Optional) Start all of your additional deployment instances:

```bash
cf scale app-name -i n
```

where you specify \( n \) as the number of instances that should be running after the command has completed.
Validating the Deployment

Verify RabbitMQ

To verify that RabbitMQ has been deployed correctly, open a browser and go to the following address:

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

If the RabbitMQ logon window appears, then RabbitMQ is functioning as expected.

Verify PostgreSQL

Note: This section is applicable only if your order contains PostgreSQL. If it does not, skip this section.

1 Run the following command:

   /opt/sas/viya/home/bin/sas-bootstrap-config kv read "config/application/postgres/password"

2 Note the output of the command. It is the password for the dbmsowner.

3 Connect to the database:

   Note: Multiple lines are used to improve readability. However, in your environment, make sure that you enter the command on a single line.

   /opt/sas/viya/home/bin/psql -h IP-address-for-PostgreSQL-database -p port-number-for Postgresql-database -d SharedServices -U dbmsowner postgres

4 When prompted, enter the password that you noted in step 2:

   Password for user dbmsowner:

5 If PostgreSQL is deployed appropriately, you should receive a response like this:

   psql (9.4.9)
   Type "help" for help
   postgres=#

6 To exit the prompt, type \q and press Enter.
Validate Elasticsearch

To determine the health of the deployed Elasticsearch, run the following command:

```bash
sudo curl -XGET https://IP-address-for-Elasticsearch-master-node:9200/_cluster/health?pretty=true
--cert /opt/sas/viya/config/etc/SASSecurityCertificateFramework/tls/certs/consul/default/consul.pem
--key /opt/sas/viya/config/etc/SASSecurityCertificateFramework/private/consul/default/consul.key
```

Typical output follows:

```json
{
  "cluster_name" : "testcluster",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 2,
  "number_of_data_nodes" : 3,
  ...
}
```

If the value of status is **green**, the cluster is fully functional. For additional information about Elasticsearch cluster health, refer to [https://www.elastic.co/guide/en/elasticsearch/reference/current/cluster-health.html](https://www.elastic.co/guide/en/elasticsearch/reference/current/cluster-health.html).

Note: For deployments with only one data node, the value of status should be **yellow** to indicate that the cluster is functional.

---

Validate Consul

To validate the installation of Consul:

1. Open a web browser and enter the URL for Consul.
2. To determine the correct URL for Consul, run the following command:

```bash
sas show info
```

The following output is displayed:

```
SAS Visual Investigator: Info

Product:
  Name                  : SAS Visual Investigator
  Version               : 10.4.0.3177.0
  Build Date            : 2018-07-09.094255

Configuration:
  JSON Configuration    : test
  Org                   : test
  Space                 : test
  Host                  : test

URLs:
```
Consul : http://10.10.10.01:8500
RabbitMQ : http://10.10.10.02:15672

IP Addresses:
  CAS Controller : 10.10.10.04
  CAS Worker : 0
  Consul : 10.10.10.01

Elastic Search
  Master Nodes : 10.10.10.05
  Client Nodes : 10.10.10.06
  Data Nodes : 2

Cache Locator : 10.10.10.07
Cache Server : 10.10.10.08
RabbitMQ : 10.10.10.02 10.10.10.03
PostgreSQL : 10.10.10.09:9432

From the preceding output, select the URL for Consul. In this example, the URL is http://10.10.10.01:8500.
Completing the Deployment

Further Documentation

You can access *SAS Visual Investigator 10.4: Administrator’s Guide* from within the SAS Visual Investigator application or from the SAS Visual Investigator documentation page. To access the secure SAS Visual Investigator 10.4 documentation, you must have an access key. The documentation page explains how to contact SAS Technical Support to request the access key.
Managing Your Software

Upgrade SAS Visual Investigator

Important: This section contains several references to SAS Visual Investigator: Administrator’s Guide. To access the secure SAS Visual Investigator documentation, you must have an access key. A message on the SAS Visual Investigator documentation page explains that licensed customers can contact SAS Technical Support to request the access key. SAS recommends that you obtain the access key before completing the tasks in this section.

Back Up the Deployment and Remove Applications

Before performing an upgrade on a SAS Visual Investigator 10.3 deployment, you should make backups of persisted data to facilitate performing a rollback if it becomes necessary. Persisted data includes BOSH services data as well as deployment configuration data.

1. Confirm that you are working with a SAS Visual Investigator 10.3 system.

   ```
   sas show info
   ```

   The results should include 10.3.1.xxxx in the Version field.

   ```
   SAS Visual Investigator : Info
   |
   | Product                          |
   | Name                : SAS Visual Investigator |
   | Version:            : 10.3.1.xxxx            |
   | Build Date:         : 2018-2-7.xxxxxxxx      |
   ```

2. Confirm that the services and applications pass their health checks.

   ```
   sas show details
   ```

   The results should show all the services as **Success** or **Agent alive and reachable**. The applications should be listed as **UP**.

3. Confirm that the instances are healthy, which is indicated by the status **RUNNING**.
sas show instances

4 Save the configuration.
   sas conf save
   sas site sync

5 Back up PostgreSQL. See Back Up the SAS Infrastructure Data Server in SAS Visual Investigator 10.4: Administrator’s Guide.

6 Back up Consul.
   cd site-directory
   sas consul backup

   For more information see Back Up the SAS Configuration Server in SAS Visual Investigator 10.4: Administrator’s Guide.

7 Remove the applications.
   cd site-directory/apps
   sas cf auth
   ./remove.sh

8 Exit the container.
   sas util exit

**Upgrade the Container**

1 Run the bin installer in upgrade mode.
   
   bash visualinvestigator_10.4.xxx_lax.bin --update

   This command makes a backup of the current installation and places it at install-directory/.backup/timestamp. It also overlays persistent data from the following SAS Visual Investigator 10.3 deployment directories into the new deployment.
   
   - /home/sas/*
   - /home/sas/.sas

2 Start the SAS Visual Investigator container.
   ./sas/bin/start

3 Add files outside the original container to the same location in the new container. For example, in the JSON configuration, the entry .directors.director-name.certificate_path might be stored locally within the container. If so, then re-add the certificate to this path.

4 Mount points that are manually created outside the deployment process must be created again. For example, if the entry .deployments.sas.log_dir is specified in the JSON configuration file, and it is an NFS mount point, you would need to upgrade the file/etc/fstab in order to persist this mount point.

**Perform Data Transformations**

Because the deployment container contains code from the new release, but still contains old configuration data, the configuration data must be upgraded.

1 Set the site name.
   
   sas site set site-name
2  Set the configuration.
   \texttt{sas conf set configuration-name}

3  Upgrade the configuration.
   \texttt{sas conf edit --update}

   The \textit{vi} editor starts and its pointer automatically moves to lines containing \# Upgrade:. Use the \textit{vi} commands \texttt{n} (next) and \texttt{p} (previous) to move between \# Upgrade: locations in the file. Make your changes at each location and exit the \textit{vi} editor with \texttt{:wq}.

4  Review the changes.
   \texttt{sas conf diff}

   The process reviews multiple files:
   \begin{itemize}
     \item \_active/_configuration.json — the union of all configuration data, including system properties such as releases and stemcells as well as user-modifiable properties. Commented-out properties are not shown.
     \item \_active/dynamic/file.json — only the properties that the user can modify. Commented-out properties are shown.
     \item \_active/fixed/*.json — only the system properties. No comments are present.
   \end{itemize}

   Within a file, use the Up Arrow Key and the Down Arrow key to move between differences. To change files, press Ctrl+T.

5  Save your changes.
   \texttt{sas conf save}

\textbf{Back Up the Elasticsearch Indices}

1  Authenticate the Elasticsearch indices.
   \texttt{sas cf auth}

2  Back up the Elasticsearch indices.
   \texttt{sas site backup indices --insecure}

   The indices are stored at the mount point that is specified by the deployment configuration.

\textbf{Upgrade Stemcells and Releases}

1  Authenticate to Cloud Foundry and BOSH.
   \texttt{sas cf auth}

2  Since the site directory will be regenerated from the new configuration data, you should consider saving the existing site directory for comparison purposes.
   \texttt{mv -/site-directory -/site-directory.orig}

3  Generate the deployment files.
   \texttt{sas deploy files}

4  Generate the tenant files.
   \texttt{sas make tenant tenant-name.properties}

5  Confirm that you are working with a SAS Visual Investigator 10.4 system.
The results should include 10.4.xxxx in the Version field.

Confirm that the services are running.

The results should show all the services as Success or Agent alive and reachable.

Deploy the new stemcells.

Deploy the release.

Upgrade Services and Applications

1. Deploy Consul:
   - sas consul delete network port
   - cd site-directory/services/consul_ha
   - bosh -n -d manifest.yml deploy
   - sas consul update

2. Deploy CAS:
   - cd site-directory/services/cas
   - ./deploy

3. Deploy PostgreSQL.
   a. Change to the PostgreSQL directory.
      - cd site-directory/services/postgres_ha
   b. Unmount the persistent storage by running the following code to make a secure connection to each PostgreSQL instance, and then run the unmount command.
      - bosh deployment manifest_two_postgresql_databases.yml
      - Label="$(sas conf select .deployments.sas.label)"
      - for Instance in $(bosh instances 2>/dev/null | grep $Label | awk '{print $2}'); do
        - bosh ssh "$Instance" "sudo su - root bash -c 'if mountpoint -q /var/vcap/store; then umount -l /var/vcap/store; fi'"
      - done

      Note: For improved readability, the bosh ssh command in the preceding code occupies three lines. However, make sure that you enter the command on a single line.

   c. Deploy the upgrade.
      - bosh -n -d ./manifest_two_postgresql_databases.yml ./deploy
      - bosh -n -d ./manifest_two_pgpool.yml ./deploy

   d. Verify the mount points that have been remounted.
      - for Instance in $(bosh instances 2>/dev/null | grep $Label | awk '{print $2}'); do
        - bosh ssh "$Instance" "sudo su - root bash -c 'mountpoint /var/vcap/store'"
      - done

4. Deploy the cache service.
cd site-directory/services/cache
./deploy

5 Deploy Elasticsearch.

   cd site-directory/services/elasticsearch
   ./deploy

6 Deploy RabbitMQ.

   cd site-directory/services/rabbitmq_ha
   ./deploy

7 Deploy a CAS tenant.

   cd site-directory/tenants
   for TenantDeploy in */cas/deploy.sh; do
       $TenantDeploy
   done

8 If you are updating a system that contains Visual Analytics, an additional property needs to be added to Consul. Run the following command:

   sas consul add
   /config/reportrenderer/sas.reportrenderer.properties.custom.baseUrl value

   The value should be the non-TLS base route, which is specified in the following form: http://<deployment-label>.Host.Domain. An example is http://dc62.v62r1.sas.com.

9 Deploy the applications.

   sas deploy apps

---

**Roll Back a Failed Upgrade**

1 Restore the Elasticsearch indices.

   sas site restore indices

2 Remove all applications and exit the deployment container.

   cd site-directory/apps
   ./remove.sh
   sas util exit

3 Archive the current deployment container.

   cd installation-directory
   Timestamp="$(date "+%Y-%m-%d.%H%M%S")"
   mkdir -p .backups/$Timestamp
   mv * .backups/$Timestamp

4 Restore the previous deployment container.

   cd installation-directory
   Previous=".backups/timestamp-of-version-10.3-backup"
   mv "$Previous/" .

5 Start the SAS Visual Investigator container.

   ./sas/bin/start

6 Set the site and configuration.
sas site set site-name
sas conf set configuration-name

7 Authenticate Bosh and Cloud Foundry.
   sas cf auth

8 Deploy the previous stemcells.
   sas bosh upload stemcells

9 Deploy previous releases.
   sas deploy releases

10 Restore the Consul key/value pairs.
    cd site-directory/services/consul_ha
    bosh -n -d manifest.yml deploy
    sas consul restore -f backup-file-name

11 Restore the CAS service.
    cd site-directory/services/cas
    ./deploy.sh

12 Connect to the restored PostgreSQL database.
    bosh -n -d manifest_two_postgresql_databases.yml deploy
    bosh -n -d manifest_two_pgpools.yml deploy

13 Restore the cache service.
    cd site-directory/services/cache
    ./deploy.sh

14 The Elasticsearch indices should be restored while you are still in the 10.4 deployment container. In that deployment container, run the following commands:
    cd site-directory/services/cache
    ./deploy.sh

15 Restore the RabbitMQ service.
    cd site-directory/services/rabbitmq_ha
    ./deploy.sh

16 Restart the applications.
   sas deploy apps
Uninstalling SAS Viya

Uninstall SAS Viya

Follow these steps to uninstall your software. The steps also apply to deployments that include disaster recovery software.

1. **Check the current status.**
   
   ```
   cd ~
   sas show status
   ```

2. **Remove the services and applications.** If you deployed using disaster recovery, repeat these commands for the active and standby sites.
   
   ```
   sas site set site-name
   sas conf set site-configuration-file
   sas cf auth.
   ./site-name/remove.sh
   ```

   **Note:** These commands will not remove any tenant-specific CAS servers. To remove tenant-specific CAS servers, also run the `remove.sh` script in each tenant CAS directory using the following command.

   ```
   ./site-name/tenants/tenant-name/services/cas/remove.sh
   ```

3. **Verify that the environment is clean.**
   
   ```
   sas show status
   ```
   
   If the results of this command show no BOSH deployments and no Cloud Foundry apps, then the environment is clean.

4. **Remove all orphaned BOSH artifacts.**
   
   ```
   bosh -e environment-alias clean-up --all
   ```

5. **Remove the log files.** If you deployed using disaster recovery, repeat this command for the active and standby sites.
   
   ```
   sudo rm -f /log/cf-org/cf-space/label/*.txt
   ```

6. **Exit the container.**
   
   ```
   sas util exit
   ```

7. **Ensure that the container has been removed.**
   
   ```
   cd ~
   sudo rm -rf sas
   ```
Delete any persistent data by removing any files under the `/postgres` and `/elasticsearch` directories.

```sh
sudo rm -rf /persistent-file-mount/postgres/names/*
```

```sh
sudo rm -rf /persistent-file-mount/elasticsearch/names/*
```

**Note:** Do not remove the directory `/names`, but instead remove the files in the directory. Removing the directory itself will cause future PostgreSQL and Elasticsearch deployments to fail.
Appendix A: Troubleshooting

BOSH

Virtual Machine Is Not Created
The most common problem with a BOSH deployment of a stateful service is the failure to create the Virtual Machine (VM). Generally, the solution is to remove the failed service and then to redeploy again. Follow the procedure:

- Change to the directory of the failed service.
- Run the remove.sh script in the directory to remove any traces of the deployment from the BOSH director.
- Run the deploy.sh script in the directory to redeploy the service.

During the attempted deployment, the RabbitMQ deployment fails and a message is displayed. Here is an example:

Error 400007: 'rabbitmq/0 (8e792c02-47c5-495c-9c06-c7b7542bd775)' is not running after update.
Review logs for failed jobs: runrabbit

To determine the state of the deployment, run the following command:

bosh vms host-rabbitmq-deployment=ha

where host is the value of the label key in the configuration file. For this example, the test host is used.

After running the command, the output might look like this:

bosh vms test-rabbitmq-ha
RSA 1024 bit CA certificates are loaded due to old openssl compatibility
Acting as user 'admin' on deployment 'test-rabbitmq-ha' on 'test'

Director task 10206

Task 10206 done

No VMs
To clean up residual information in the Bosh director's database, change to the following directory:

```
cd services rabbitmq_ha
```

To ensure that you are in the correct directory, run the command:

```
pwd
```

**WARNINGS:**

- The remove.sh script uses options that prevent interaction. Therefore, the command continues processing.
- There is a remove.sh script in each of the directories. Make sure that you are in the correct directory or you might remove everything instead of just the deployment that failed. Each of the remove.sh scripts removes the service or the call for each of the remove.sh scripts in any subdirectories that are in the directory in which it resides. For example, if you are in the `services` directory, the remove.sh script removes all of the services. If you are in the `/home/sas` directory, the remove.sh script removes everything. If you are in the `/home/services/rabbitmq` directory, the remove.sh script removes only the RabbitMQ deployment.

In the `/home/services/rabbitmq` directory, run the command:

```
./remove.sh
```

Here is typical output:

```
RSA 1024 bit CA certificates are loaded due to old openssl compatibility
Acting as user 'admin' on deployment 'test-rabbitmq-deployment' on 'test'

You are going to delete deployment 'test-rabbitmq-deployment'.

THIS IS A VERY DESTRUCTIVE OPERATION AND IT CANNOT BE UNDONE!

Director task 40322
  Started deleting instances > rabbitmq/0 (43aab57f-b71c-419b-95c3-9b151cf9a5). Done (00:00:51)

  Started deleting properties
  Started deleting properties > Destroying deployment. Done (00:00:00)

Task 40322 done

Started 2016-01-01 00:49:34 UTC
Finished 2016-01-01 00:50:25 UTC
Duration 00:00:51

Deleted deployment 'test-rabbitmq-deployment'
```

The warning message **THIS IS A VERY DESTRUCTIVE OPERATION AND IT CANNOT BE UNDONE!** is present for all BOSH delete deployment commands. There are flags in the remove.sh script that prevent interaction but the message is always displayed.

You must check these additional items in the manifest.yml file and the configuration JSON file:

- The watch time must be 30000-1800000 or higher.
- Canary watch time must be 30000-1800000 or higher.
- The number of workers must be increased.

If only one VM failed in a set of deployments like Elasticsearch, it might not be desirable to remove the VMs and then redeploy them. In this situation, use the following command:

```
bosh delete deployment test-elasticsearch-deployment-client
```
In this case, you are prompted to continue with the deployment.

```
bosh delete deployment test-elasticsearch-deployment-client
RSA 1024 bit CA certificates are loaded due to old openssl compatibility
Acting as user 'admin' on deployment 'test-elasticsearch-deployment-client' on 'test'
```

You are going to delete deployment 'test-elasticsearch-deployment-client'.

**THIS IS A VERY DESTRUCTIVE OPERATION AND IT CANNOT BE UNDONE!**

Are you sure? (type 'yes' to continue):

Be sure to enter **yes**. BOSH continues with the deletion of the deployment.

If you enter **y** or any other character, the following message is displayed:

```
Canceled deleting deployment
```

### BOSH Deployment Fails to Remove a Canceled Deployment

A deployment was started and then canceled using Ctrl+C in the terminal session in which the deployment was running. When canceled using Ctrl+C, you can issue the command `bosh tasks` and then use the `bosh cancel task` command to cancel unwanted tasks. Further cleanup can be done by running the `remove.sh` script. An attempt to remove the canceled deployment using the `remove.sh` script might result in the following message:

```
./remove.sh
RSA 1024 bit CA certificates are loaded due to old openssl compatibility
Deployment set to '/home/sas/services/consul/manifest.yml'
RSA 1024 bit CA certificates are loaded due to old openssl compatibility
Acting as user 'admin' on deployment 'test-consul' on 'test'
```

You are going to delete deployment 'test-consul-deployment'.

**THIS IS A VERY DESTRUCTIVE OPERATION AND IT CANNOT BE UNDONE!**

```
Director task 49064
Error 100: Redis lock lock:deployment:test-consul-deployment is acquired by another thread
```

Task 49064 error

For a more detailed error report, run: `bosh task 49064 --debug`

Error 100 is caused by a lock in the director’s Redis data store that prevents the removal of the deployment. To remove the deployment, wait approximately 10 minutes for the lock to clear and then run the `remove.sh` script again.
Cloud Foundry Run Time

UI Displays with No Tabs and No Access to the Administration UI

In this case, the initial problem is that the UI comes up but there are no tabs and no access to the Administrative UI.

To check the status of all of the components in Consul, run the following command;

```
sas show details
  pass cas-controller (Success)
  pass cas-worker@192.168.5.141 (Success)
  pass cas-worker@192.168.5.142 (Success)
  pass consul_container (Agent alive and reachable)
  pass elasticsearch (TCP connect 10.10.10.05:9200: Success. ElasticSearch cluster green.)
  pass postgres (Success)
  pass rabbitmq (Success)
```

App Status

```
pass audit (UP)
pass authorization (UP)
pass casManagement (UP)
pass datahub (UP)
pass entityResolution (UP)
pass feature (UP)
pass files (UP)
pass identities (UP)
pass networkAnalytics (UP)
pass SASLogon (UP)
pass SASVisualInvestigator (UP)
pass svi-ai (UP)
warn svi-alert (DOWN)
pass svi-core (UP)
pass svi-sand (UP)
pass svi-transport (UP)
```

This displays svi-alert as a warn and the status would be (DOWN).

Most problems in the run-time deployments are linked to failures in the BOSH services. If only one service is failing (such as the svi-alert service), check the log for that service by running the command:

```
cf logs <host>-svi-alert --recent
```

Where host is the value of the label key in the configuration file. For our example, the test host is used.

```
cf logs test-svi-alert --recent
```

This displays the log data that is in the Loggregator buffer. If a store and display log service is set up, then you can use that to see the log data. When reviewing the log, you might see error messages that look like this:

```
  Datahub error: stored object not created
```

This points to a problem in the svi-datahub application. Examining the svi-datahub log, the following is displayed:
The key is the Access is denied message and the pointer to the feature service svi-feature. Examining the svi-feature log, you see the following error:

cf logs test-svi-feature --recent
2016-09-04T22:49:13.12-0400 [APP/0] OUT debug=0x88bfc1e5:TKCASA_GEN_LICENSE_NOT_LOADED.

This main problem is that the CAS server cannot find the license file, which is preventing both CAS and SAS Visual Investigator from being operational.

To fix this problem, correct the nfs_mounts section of the JSON configuration file. The incorrect mount point for the license file had been entered so that you need to renter the mount point.

Here was the original entry:

```
"cas_controller": [
  {
    "fs_spec": "test.some.server.com:/files/license",
    "fs_file": "/opt/cas/cloud"
  }
],
```

The new entry would look like this:

```
"cas_controller": [
  {
    "fs_spec": "test.some.server.com:/files/license",
    "fs_file": "/opt/cas/license"
  }
],
```

Once the network file system mount is corrected, check the application status and verify that all of the applications are up and running before continuing the deployment process.

**Tenant State Has Not Changed to Onboarded**

The following message might be displayed during onboarding.

Tenant your-tenant-name's state is ...onboarding.........
To onboard the client:

1. Run the following command to restart datahub:
   ```
   cf restart xx-svi-datahub
   ```

2. (Optional) Ensure that the tenant has been initialized:
   ```
   cd ~/tenants/your-tenant-name/scripts/bin/tenant ./add-tenant-admin.sh -p cf -t your-tenant-name
   ```

3. Load the users:
   ```
   cd ~/tenants/your-tenant-name/scripts/bin/tenant ./add-users-cf.sh -p cf -t your-tenant-name
   ```
   
   **Note:** The users are not LDAP users.

If all processes are complete without errors, you can load the user management spreadsheet.

### svi-feature and svi-network-analytics Fail to Start

Check to ensure that the license is read.

1. Change to the directory for the CAS license controller:
   ```
   cd ~/services/cas
   ```

2. To list all VMs for a deployment, run the following command:
   ```
   bosh -e env -d deployment name vms
   ```

3. To connect to any of the VMs, run the following command:
   ```
   bosh -e environment-alias-or-name -d deployment name ssh vm-name
   ```

4. Change to the `/tmp` directory.
   ```
   cd /tmp
   ```

5. Run the `cat` command on the `init.info` file:
   ```
   cat init.info
   ```
   To locate an error with the NFS mount for the CAS license, search for the phrase "Mounting NFS...".

6. On the BOSH virtual machine, change to the `/opt/cas/license` directory.
   ```
   cd /opt/cas/license
   ```
   If the license file is present, check the expiration date to determine whether it has expired.