SAS® Visual Investigator 10.2.2 on the Cloud: Deployment Guide

SAS® Visual Investigator 10.2.2 on the Cloud: Deployment Guide

Copyright © 2017, SAS Institute Inc., Cary, NC, USA

All Rights Reserved. Produced in the United States of America.

For a hard copy book: No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, or otherwise, without the prior written permission of the publisher, SAS Institute Inc.

For a web download or e-book: Your use of this publication shall be governed by the terms established by the vendor at the time you acquire this publication.

The scanning, uploading, and distribution of this book via the Internet or any other means without the permission of the publisher is illegal and punishable by law. Please purchase only authorized electronic editions and do not participate in or encourage electronic piracy of copyrighted materials. Your support of others’ rights is appreciated.

U.S. Government License Rights; Restricted Rights: The Software and its documentation is commercial computer software developed at private expense and is provided with RESTRICTED RIGHTS to the United States Government. Use, duplication, or disclosure of the Software by the United States Government is subject to the license terms of this Agreement pursuant to, as applicable, FAR 12.212, DFAR 227.7202-1(a), DFAR 227.7202-3(a), and DFAR 227.7202-4, and, to the extent required under U.S. federal law, the minimum restricted rights as set out in FAR 52.227-19 (DEC 2007). If FAR 52.227-19 is applicable, this provision serves as notice under clause (c) thereof and no other notice is required to be affixed to the Software or documentation. The Government’s rights in Software and documentation shall be only those set forth in this Agreement.

SAS Institute Inc., SAS Campus Drive, Cary, NC 27513-2414

August 2017

SAS® and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration.

Other brand and product names are trademarks of their respective companies.

10.2.2-P1:dplyvi0dd
Contents

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

Chapter 2 / System Requirements for SAS Visual Investigator .................. 3
  Cloud Platform Software Requirements ................................. 3
  Virtual Machine Operating System and Software Requirements ........ 4
  Security Requirements .................................................... 4
  Client Requirements .......................................................... 5

Chapter 3 / Pre-installation Tasks ......................................................... 7
  Complete the Configuration Worksheet .................... 7
  Enable Required Ports ............................................... 7

Chapter 4 / Installing SAS Visual Investigator on SAS Viya ................... 9
  Prepare the Installation Tools ........................................ 9
  Prepare the Installation Environment ...................... 12
  Install SAS Visual Investigator ............................. 19

Chapter 5 / Manual Configuration ..................................................... 21
  Configure and Onboard Initial Tenant ...................... 21

Chapter 6 / Validating the Deployment ............................................... 23
  Validate Elasticsearch ................................................. 23
  Validate Consul ................................................................. 23
  Verify RabbitMQ .............................................................. 24
  Verify PostgreSQL .......................................................... 24

Chapter 7 / Next Steps ........................................................................ 27
  Further Documentation ................................................ 27

Chapter 8 / Appendix A: Troubleshooting .......................................... 29
  BOSH ............................................................................ 29
  Cloud Foundry Run Time ............................................ 32
Introduction

About This Guide

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

- 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, Cloud Foundry, and vSphere or OpenStack, depending on your environment.
- Unless another situation is specifically cited, the information in this guide pertains to the software that you ordered.

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.
- vSphere and OpenStack are the supported IaaS environments.
- 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 services and the microservices.

SAS provides unique files to support and customize your deployment.

- The SAS Visual Investigator services and applications are packaged as a container. You will access the container from a binary installer file that you download from SAS.
- SAS provides the Cloud Foundry Deployment Information worksheet in XLS format that you will complete for vSphere or OpenStack, depending on your environment.
What Gets Deployed

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

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

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 for SAS Visual Investigator

Cloud Platform Software Requirements

Cloud Foundry Requirements

BOSH Director

Other Required Software

Supported Data Sources

Virtual Machine Operating System and Software Requirements

Security Requirements

User Accounts

Authentication

Client Requirements

Web Browser Requirements

Cloud Foundry Requirements

SAS Visual Investigator supports Cloud Foundry versions 246 through 254 on OpenStack or VMware vSphere.

For additional information about the supported run-time environment and stemcells, see https://support.sas.com/en/documentation/third-party-software-reference/viya/support-for-operating-systems.html#cf.

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 1.3262.26.0 or later is required.

Other Required Software

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

- HashiCorp Consul – Included to enable service discovery and configuration.
- RabbitMQ – Included to provide an open-source, standards-based platform for SAS components and applications to send and receive messages.
- Elasticsearch – Included to provide search capability.
Apache Geode – Used for session caching.

**Supported Data Sources**
The following database is supported for use by SAS Visual Investigator:
- PostgreSQL

The following data stores are supported:
- PostgreSQL 9.4
- Oracle 12c

**Virtual Machine Operating System and Software Requirements**
The VM instance that is used to install SAS Visual Investigator has the following requirements:
- Red Hat Enterprise Linux or CentOS 7.2 must be installed.
- The systemd-nspawn component must be installed.
- 20 GB of free space must be available.

**Security Requirements**

**User Accounts**
The user account that is used to perform the deployment 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 you start the deployment, a user that will fulfill the role of this viadmin account must exist as a valid LDAP user.

The administrator creates groups for users as well as a group for administrators by importing a spreadsheet. The spreadsheet is tenant-specific and enables the administrator to make updates to users and groups. Here is the location of the template spreadsheet, named svi-user-management.xls:

`/home/sas/apps/`

**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. The deployment process configures LDAP settings automatically.

Before SAS Visual Investigator is deployed, perform the following tasks:

1. Make sure that SAS Visual Investigator users are able to authenticate to your LDAP provider.
2. (Optional) Set up tenants in LDAP. Use the documentation that is appropriate for your LDAP implementation.
After the deployment has completed, the designated administrator logs on to the administration application as the viadmin user. Then, valid LDAP user accounts can be imported from the spreadsheet, as discussed previously.

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/support-for-web-browsers.html.
Pre-installation Tasks

Complete the Configuration Worksheet

To prepare for deployment, you must complete the Cloud Foundry Deployment Information worksheet in XLS format for vSphere or OpenStack, depending on your environment. Then, during installation, you must manually enter this information in a configuration file.

To complete and customize your deployment, specify the information by associating required and optional keys with the appropriate values.

- For each key, specify a value in the Value column, where a value does not already pre-exist.
- Do not specify any values for passwords. They are entered on-site.
- Blank lines have been inserted to improve readability and to show a separation between sections of the configuration file.
- JSON header lines are included to provide information about the section.

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></td>
<td>443 (external)</td>
<td></td>
</tr>
<tr>
<td>default Erlang Port Mapper Daemon (epmd)</td>
<td>4369</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>Process</td>
<td>Required Port</td>
<td>Notes</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------------</td>
<td>----------------------------------------------------------------------</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>default SAS Messaging Broker AMQP client access port</td>
<td>5672</td>
<td></td>
</tr>
<tr>
<td>SAS Configuration Server</td>
<td>8300–8309, 8500</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>8500</td>
<td>Used by clients to make REST HTTP calls to CAS, as with the Python REST interface.</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>default SAS Messaging Broker management web console port</td>
<td>15672</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>default SAS Messaging Broker clustering port</td>
<td>25672</td>
<td></td>
</tr>
<tr>
<td>Apache Geode</td>
<td>40404</td>
<td></td>
</tr>
</tbody>
</table>
Installing SAS Visual Investigator on SAS Viya

Prepare the Installation Tools

Overview
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

Overview
Set the Configuration File
Edit the Configuration File
Save the Configuration File
Authenticate to Cloud Foundry and BOSH
Upload the BOSH Stemcells
Upload the BOSH Releases
Create the Files for Deployment
Preparing to Examine the Files
Examine the Files Related to BOSH
Examine the Files Related to Cloud Foundry
Using Logs

Install SAS Visual Investigator

Overview
Install the Stateful Services to BOSH
Install the Stateless Applications and Microservices

Prepare the Installation Tools

Overview
You must prepare the installation tools before you can install SAS Visual Investigator. Preparation consists of the following tasks:

- Download the binary installer.
- Unzip the downloaded file.
- Extract the binary file.
Start the container.

Sign on to the container.

**Download the Binary Installer File**

You start by downloading the binary installer file to a physical machine or a virtual machine (VM) in 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_2_2__xxx__lax.zip
```

Note: `xxx` represents three digits that are provided automatically. Note this value for use in subsequent commands in this section.

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

Here are typical results:

```bash
--2016-06-20 14:53:04--  http://10.120.16.120/visualinvestigator__10_2_2__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_2_2__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_2_2__xxx__lax.zip' saved [5508425807/5508425807]
```

**Unzip the Downloaded File**

Unzip the downloaded file using the `unzip` utility:

```bash
unzip visualinvestigator__10_2_2__xxx__lax.zip
```

**Extract the Binary File**

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

```bash
bash visualinvestigator__10_2_2__xxx__lax.bin
```

Here is an excerpt of the results:

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

The binary installer deploys to the installing user’s home directory and its subdirectories:

- **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.
Failed to create directory /home/test/sas/image//sys/fs/selinux: No such file or directory
Failed to create directory /home/test/sas/image//sys/fs/selinux: No such file or directory
Press ^] three times within 1s to kill container.
systemd 219 running in system mode. (+PAM +AUDIT +SELINUX +IMA -APPARMOR +SMACK +SYSSVINIT +AUDIT +TMP +LIBCRYPTSETUP +GCRYPT +GNUTLS +ACL +XZ -LZ4 -SECCOMP +BLKID +ELFUTILS +KMOD +IDN)
Detected virtualization systemd-nspawn.
Detected architecture x86-64.
Welcome to CentOS Linux 7 (Core)!

Because the container attempts to alter the state of the host operating system, the following error message might be displayed. You can safely ignore the message:

```
Failed to create directory /home/test/sas/image//sys/fs/selinux: No such file or directory
Failed to create directory /home/test/sas/image//sys/fs/selinux: No such file or directory
[FAILED] Failed to start LSB: Bring up/down networking.
See 'systemctl status network.service' for details.
```

Sign On to the Container

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

   CentOS Linux 7 (Core)
   Kernel 3.10.0-229.el7.x86_64 on an x86_64

   sfr47066 login:

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

   SAS 15:04:47 !1 [-]

   The prompt now includes the string, SAS, 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 type of 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 file 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 are typical results:

```
Product
  Name : SAS Visual Investigator
  Version: 10.1.216
  Build Date: 20160916.1051
```

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

Overview

Before you can deploy SAS Visual Investigator, follow these pre-deployment steps:

- Collect information about the environment.
- Set, edit, and save the configuration file.
- Authenticate the sas user to Cloud Foundry and BOSH.
- Upload BOSH stemcells.
- Upload releases.
- Generate files from configuration data for deployment.

The information in the Microsoft Excel spreadsheet CF_Deployment_Questionnaire.xlsx needs to be collected. See [http://support.sas.com/documentation/prod-p/visgator/index.html](http://support.sas.com/documentation/prod-p/visgator/index.html). Then, during installation, you must manually enter this information in a configuration file.

Once the information is collected, enter the following command to list the available SAS Visual Investigator configuration files.

```
sas conf list
```

Here are the results:

```
The following configurations are available:

  template_openstack
  template_vsphere
```

To use a configuration, use the command:

```
sas conf use <configurationName>
```
Current configuration: unset

Set the Configuration File

1. 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 use template_xxxxx`

   where `xxxxx` is either `vsphere` or `openstack`.

   Here is an example of the output:

   Now using configuration: `template_xxxxx`

2. Save the template configuration file with a new configuration filename that is meaningful in your environment. The configuration file `test` is used in this example.

   `sas conf save test`

   This produces the following output:

   Saved configuration file: `test`

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

   `sas conf use test`

   This produces the following output:

   Now using configuration: `test`

Edit the Configuration File

Once the template is ready to use, edit the configuration file and enter the information from the spreadsheet. See http://support.sas.com/documentation/prod-p/visgator/index.html. Then, during installation, you must manually enter this information in a configuration file.

Note: SAS has configured the vim utility to check JSON syntax for this purpose. You will be notified of any JSON errors when you exit the utility if the file contains invalid JSON syntax.

Here is an example of the configuration file before editing:
After you enter the information into the table from Appendix A or the spreadsheet, copy your entries into the configuration file.

1. Copy your entries into the configuration file and ensure that your entries do not contain Rich Text markup. It must contain only ASCII 7 data. Every entry in Appendix A or the spreadsheet corresponds to an entry in the configuration file.

2. Save the configuration file.

Here is an example of the configuration file after editing:
Save the Configuration File

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

```bash
classic conf save test
```

This produces the following output:

```
Saved configuration file: test
```

This command does not change the active configuration file. Instead, it saves a copy of it to a saved configuration directory. You can see your configuration name now by running the command:

```bash
classic conf list
```

This produces the following output:

```
The following configurations are available:
```

Note: The location of this configuration file that is in use is a temporary location and can easily be overwritten by another configuration file. SAS recommends that you save the configuration file that has been edited.
To use a configuration, use the command:

```bash
sas conf use <configurationName>
```

Current configuration: test

**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 host bastion box 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:

```bash
sas cf auth
```

This produces the following output:

```plaintext
Authentication for user: sas
Current target is https://0.0.0.0:25555 (ocfdir)

API endpoint:   https://api.sas.sas.sas.com (API version: 2.48.0)
User:           test
Org:            test
Space:          test
```

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 directory and run-time sections of the configuration file. Correct them for your installation and try again.

**CAUTION!** Do not attempt to proceed beyond this point if you do not have a working connection to both BOSH and Cloud Foundry.

**Upload the BOSH Stemcells**

Once connectivity is established to the BOSH environment, 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:

   ```bash
   bosh stemcells
   ```

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

   ```plaintext
   Name="bosh-openstack-kvm-centos-7-go_agent"
   Version="3421.11"
   ```

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

   ```bash
   sas bosh upload stemcells
   ```

   Two stemcells are delivered: one each for OpenStack and vSphere.
To ensure that the correct stemcells are loaded, even if there are existing stemcells, run the following command:

```bash
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:

```bash
sas deploy releases
```

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

- Cloud Analytic Server (CAS)
- Elasticsearch 2.3.3
- PostgreSQL 9.4
- Consul
- RabbitMQ
- PGPool
- Apache Geode

**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. If these files have already been generated, then remove them from the container first by running the following commands:

```bash
cd ~/
rm -rf *
```

**Note:** **Warning:** User needs to confirm that they are in the users home directory and not in the root directory when issuing the command listed above.

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 are deployed into Cloud Foundry. Then it performs the token substitution on the various files that are required for deploying the solution.

When file system 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.

**Note:** Be sure to remove the files that were generated before running the command `sas deploy files` again.
Preparing 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 home 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/services directory in the container.

To examine the manifest files:

1. Change to the /home/sas/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:

- director_uuid – make sure this matches what was entered in the configuration file.
- Validate 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/services directory.

2. Run the following command to display the vim editor: `vi */*.sh`. This displays the vim editor in the window.

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 archive.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 filled in. If you discover any entries like this, return to the configuration file and make sure that all required entries are filled in. 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/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 filled in. If you discover any entries like this, return to the configuration file and make sure that all required entries are filled in. 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 redirect it to a logging server is the standard means of providing access to application logs. The rsyslog logging service has been added to the services 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**

**Overview**

Installing SAS Visual Investigator consists of the following tasks:

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

**Install the Stateful Services to BOSH**

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

```
  sas deploy services
```

When installations are complete, test the applications to ensure that the installation is working as expected. For more information, see “Validating the Deployment” on page 23.

**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 29

**Install the Stateless Applications and Microservices**

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

   ```
   1. 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.

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 Run the following command to display the status of a stateful service or application:
sas show details

Here is an excerpt of typical output:

Service Status
pass cas-acme-default (Success)
pass cas-license-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)
...
Configure and Onboard Initial Tenant

1 Locate the `tenant.properties` template in the home directory of the container.

2 Make a copy of the template, naming the new file with the actual name of the initial tenant that will be created.
   
   For example, if you are creating a tenant named acme, you could copy the template file as the new tenant file.
   
   ```
   cp tenant.properties acme.properties
   ```

3 Use the text editor to modify the newly named template file. For example, if the name of the tenant file is `acme.properties` then you could open the file to edit it using the following command.

   ```
   vi acme.properties
   ```

4 Enter the tenant properties. Here is an example showing the edited template.

   ```bash
   #!/bin/bash
   
   # This is a template file for tenant on-boarding.
   # Copy this file to a new filename and change the properties below.
   
   # ===== TENANT NAME
   
   # Description:
   #   This is your tenant name.
   #   Tenant names must begin with a lowercase letter and
   #   may be followed by additional lowercase letters or digits.
   # 
   # Enter your Tenant name here:
   svi_TENANT_ID="acme"
   
   # ===== CAS CONTROLLER IP ADDRESS
   
   # Description:
   #   This is the CAS Controller IP address for your tenant.
   #   This is NOT the same IP address as that of the base CAS Controller
   #   that is used for licensing.
   # 
   # Enter the IP address of your CAS Controller here:
   ```
svi_SERVICE_CAS_CONTROLLER_IP="10.10.10.36"

# ===== CAS WORKER IP ADDRESSES
#
# Description:
# These are the CAS Worker IP addresses for your tenant.
# These are NOT the same IP addresses as that of the base CAS workers.
# An empty array is valid.
#
# Enter the IP addresses of your CAS Workers here:
svi_SERVICE_CAS_WORKER_IP=( "10.10.0.37" )

# ===== TENANT USERNAME
#
# Description:
# This is the first user added for the new tenant.
# The tenant first user is a username that can be authenticated
# using the configured LDAP type.
# This username may be different for each deployed tenant.
#
# Enter the tenant username:
svi_TENANT_USERNAME="demo"

5 Save the changes.

6 To verify that all Consul services and applications have a passing status, run the following command:
   sas show details

7 (Optional) Scale the deployment by running the following command:
   cf scale app-name -i n
   where you specify n as the number of instances that should be running when the command completes.
   Note: During onboarding, as a default the applications authorization, identities and tenant should have twice
   as many instances running:

8 Make the initial tenant by running the following command:
   sas make tenant tenant-name.properties
   For example, if your tenant name is acme, then the command would be as follows:
   sas make tenant acme.properties

9 Initialize the first tenant by running the following command:
   sas deploy tenant -i

10 Deploy the initial tenant by running the following command:
   sas deploy tenant tenant-name

11 Check the status of the initial tenant by running the following commands:
   sas show tenant status tenant-name
Validating the Deployment

Validate Elasticsearch

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

```
curl -XGET 'http://IP-address-for-Elasticsearch-master-node:9200/_cluster/health?pretty=true'
```

Typical output follows:

```
{
  "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.

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:

```
sas show info
```

The following output is displayed:

```
SAS Visual Investigator: Info
```

Product:
Name : SAS Visual Investigator
From the preceding output, select the URL for Consul. In this example, the URL is http://10.10.10.01:8500.

**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:
/opt/sas/viya/home/bin/psql -h IP-address-for-PostgreSQL-database -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.
Next Steps

Further Documentation

You can access *SAS Visual Investigator 10.2.2: 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 10.2.2 documentation, you must have an access key. The documentation page explains how to contact SAS Technical Support to request the access key.
Appendix A: Troubleshooting

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
```

where `host` is the value of the deployments.sas.host 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-deployment
RSA 1024 bit CA certificates are loaded due to old openssl compatibility
Acting as user 'admin' on deployment 'test-rabbitmq-deployment' 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:

```bash
cd services/rabbitmq
```

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

```bash
pwd
```

```
/home/sas/services/rabbitmq
```

**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:

```bash
./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 (43aabb57f-b71c-419b-95c3-9b151cfc99a5). 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.
- Increase the number of workers.
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 the 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 a 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-deployment' 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 deployments.sas.host 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:

```
2016-09-05T22:45:08.98-0400 [APP/0] OUT 2016-09-05 02:45:08.988 ERROR 13 --- [nio-8080-exec-7]
  c.s.f.t.c.h.DatahubHealthIndicator : anonymousUser [27fa5841-1091-4d28-9faa-916782e21e22]
  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:

```
cf logs test-svi-datahub --recent
  "Access is denied"
2016-09-04T22:47:02.76-0400 [APP/0] OUT
     (FeatureAuthorizationAspect.java:76)
```

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 reenter the mount point.

Here was the original entry:

```
"cas_controller":
  [
    
    # Description:
    # The mount that specifies the location of the SAS license file.
    # Notes: One mandatory mount point for the SAS license file is required.
    # The entry in the fs_file value MUST be "/opt/cas/license".
    # This is required in order for CAS to locate the SAS license file.
    # The file must be renamed to setin90.sas.
    "fs_spec":                    "test.some.server.com:/files/license",
    "fs_file":                    "/opt/cas/cloud"
  ],
```

The new entry would look like this:

```
"cas_controller":
  [
    
    # Description:
    # The mount that specifies the location of the SAS license file.
    # Notes: One mandatory mount point for the SAS license file is required.
    # The entry in the fs_file value MUST be "/opt/cas/license".
    # This is required in order for CAS to locate the SAS license file.
    # The file must be renamed to setin90.sas.
    "fs_spec":                    "test.some.server.com:/files/license",
    "fs_file":                    "/opt/cas/license"
  ],
```

Once the network file system mount is corrected, you can do the deployment.

**Tenant State Has Not Changed to Onboarded**

The following message might be displayed during onboarding.
Tenant your-tenant-name's state is ..onboarding.............

-- Wed Jul 19 09:21:09 EST 2017: (u=sas): Command-line override (yes) to: [onboarding]
Tenant state hasn't changed to onboarded (round 1). Proceed anyway?

To onboard the client:

1. Run the following command to restart datahub:
   ```bash
cf restart xx-svi-datahub
   ```
2. (Optional) Ensure that the tenant has been initialized:
   ```bash
cd ~/tenants/your-tenant-name/scripts/bin/tenant ./add-tenant-admin.sh -p cf -t your-tenant-name
   ```
3. Load the users:
   ```bash
   Note: The users are not LDAP users.
   cd ~/tenants/your-tenant-name/scripts/bin/tenant ./add-users-cf.sh -p cf -t your-tenant-name
   ```

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:
   ```bash
cd ~/services/cas
   ```
2. Run the following commands:
   ```bash
   bosh deployment manifest-controller.yml
   bosh ssh
   ```
3. Change to the `/tmp` directory.
   ```bash
cd /tmp
   ```
4. Run the cat command on the init.info file:
   ```bash
cat init.info
   ```

To locate an error with the NFS mount for the CAS license, search for the phrase "Mounting NFS...".

5. On the BOSH virtual machine, change to the `/opt/cas/license` directory.
   ```bash
cd /opt/cas/license
   ```

If the license file is present, check the expiration date to determine whether it has expired.

**Destroy Tenant Command Fails on Drop of the Database**

Run the following SQL code using the pgadmin tool, or submit the following SQL using the psql script.

```sql
REVOKE CONNECT ON DATABASE tenant_name FROM PUBLIC, dbmsowner;
SELECT
    pg_terminate_backend(pid)
FROM
    pg_stat_activity
WHERE
    -- don't kill my own connection!
    pid <> pg_backend_pid()
    -- don't kill the connections to other databases
```
AND datname = 'tenant_name';