VMware Smart Assurance UI Installation and Configuration Guide

VMware Smart Assurance 10.0

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2019 VMware, Inc. All rights reserved. Copyright and trademark information.

Contents

1 Overview 5

- General Requirements 5
- Linux Requirements 5
- Related documentation 6

2 Installing DCF 7

- Install DCF using Console Mode 7
- Install DCF using Graphical Mode 9
- Install DCF in Silent Mode 10

3 Installing Eventstore 12

- Install Eventstore using Console Mode 12
- Install Eventstore using Graphical Mode 16
- Install Eventstore in Silent Mode 20

4 Installing cAPI 23

- Install cAPI using Console Mode 23
- Install cAPI using Graphical Mode 26
- Install cAPI in Silent Mode 28

5 Installing Smarts-UI 30

- Install Smarts-UI using Console Mode 30
- Install Smarts-UI using Graphical Mode 32
- Install Smarts-UI in Silent Mode 34

6 Performing Uninstallation 36

7 Configuration and Authentication of Components 39

- Elasticsearch Authentication 39
- Enabling HTTPS in Elastic Search 41
- Redis Cluster Authentication 42
- Kafka SASL_PLAIN Authentication Configuration 42
- Kafka SASL_SSL Authentication Configuration 44
- cAPI-vIDM Configuration and Authentication 47
- VIDM Authentication with Notification GUI 49
- Create Remote Access Token for SpringBoot App for VIDM Authentication 50
- Export VIDM Certficate 50
- vROps Integration 50

Enabling HTTPS in SAM 51

8 Troubleshooting 54

When Live Notifications are not Appearing to UI 54

When Service Unavailable Error Appears 55

When Cluster is Down 55

When Connections cannot be Established with Smarts Tomcat Service 55

When Connections cannot be Established with Smarts Presentation service 56

When "Result window is too large, from + size must be less than or equal to: [10000]" Message Appears 56

When Request Timeout Message Appears 56

When Controller Service Fails to Start in DCF 57

Overview

1

This chapter describes compatibility of the components Eventstore, cAPI, SmartsUI, and DCF with each other and their installation tasks.

This chapter includes the following topics:

- General Requirements
- Linux Requirements
- Related documentation

General Requirements

These requirements are for a minimal deployment. In a production environment, the requirements vary depending on the provisioned load, and you must include careful planning and sizing before beginning the deployment.

The environment must meet the following requirements:

1. 64 bit operating system (Linux).
2. Forward and Reverse IP and DNS lookups must work on each server.

Note The following sections use Linux commands and directories as examples.

Linux Requirements

The environment must meet the following requirements. Make an adjustment to the host before continuing.

- RHEL 7.5, 7.6
- RHEL 6.9, 6.10
- The graphical desktop environment is required (optional).

Related documentation

The following VMware publications provide additional information:

- *VMware K4M Installation and Administration Guide.*
- *VMware K4M KPI Designer User Guide.*
- *VMware K4M User Guide.*
- *VMware Smart Assurance Web Portal User Guide.*
- *VMware Smart Assurance Integration Guide.*
- *VMware Smart Assurance UI Platform User and Configuration Guide.*
- *vRealize Operations Management Pack for Smart Assurance Adapter Guide.*

Installing DCF

2

This chapter includes the following topics:

- Install DCF using Console Mode
- Install DCF using Graphical Mode
- Install DCF in Silent Mode

Install DCF using Console Mode

DCF can be installed on the platform of supported Linux hosts. This procedure specifically uses the Linux installation procedure as an example.

Prerequisites

Fulfill the following prerequisites before starting the installation:

1 Installation server must have bash installed.

2 Installation server must have zip installed.

3 Installation server must have installed curl utility.

4 MongoDB must be already installed along with first MongoDB user.

5 When you install DCF on a Linux Platform, assign executable permissions to the installation script.

6 Ensure that you have a login with root privileges to run the installer.

7 Download the installation file from support.vmware.com and place it in a temporary location on the server.

Procedure

1 Login server as root.

2 Type "`./release-1.0.0.<build_number>.bin -i console`" to run the installer in the console-based installer mode, press **Enter**.

The introduction command prompt screen appears.

3 Press **Enter** to continue.

License agreement appears.

4 PRESS ANY KEY TO CONTINUE TO READ LICENSE AGREEMENT OR PRESS '0' to ADVANCE TO END. Press **Enter**.

5 Press ‘Y’ + ‘Enter’ to accept the license agreement.

6 Installer prompts to choose an install folder. Press **Enter** to accept the default or enter a non-existing folder location for the install folder.

   This is the location where DCF will be installed.

   Note If Install folder already contains DCF folder, installer cancels the installation and exits.

7 Installer prompts to enter the Controller port. Press **Enter** to choose the default port.

   DCF-CONTROLLER service will start in this port. Port number must be between 1 to 65535. If wrong port number is entered, installer throws a validation error and redirects to re-enter the Port details.

8 Enter the **Controller user name** when installer prompts. Press **Enter** to choose the default user name.

9 Enter **Controller Passwor**d and confirm the password when installer prompts.

   Note The password must not leave blank. You must enter the password.

   These user name and password is required to authenticate REST calls.

   If passwords are mismatched, installer throws a validation error and redirects to re-enter the password at step 9.

10 Installer prompts to enter **MongoDB URI**. Press **Enter** to choose the default URI.

11 Installer prompts to enter the **MongoDB User Name**. Press **Enter** to choose the default user name.

12 Installer prompts to enter **MongoDB Password**, enter the **Password** and **Confirm** Password when prompts for confirmation. The password must not left blank.

   Note Make sure these user name and password are same as the password created during MongoDB setup. If passwords are mis matched, installer throws a validation error and redirects to re-enter the password at step 12.

13 Press **Enter** to continue when pre-install summary is displayed.

   Installation continues.

   Note Installer triggers rollback action on any kind of failure. Except `DCF_Logs` all files and folders will be uninstalled. Errors can be seen inside “`DCF_Logs/INSTALL_ERR.log`”.

14 Press **Enter** to exit the installer when Install completed message displays.

What to do next

After successful DCF installation, Install **VMware Smarts Notification Collector** to pull all the events from Smarts Presentation SAM and publish the same to KAFKA for consumption.

Install DCF using Graphical Mode

This installation procedure describes the steps of DCF installation in the Graphical Interface.

Prerequisites

1 Ensure that you have a login with root privileges to run the installer.

2 Download the installation file from support.vmware.com and place it in a temporary location on the server.

Procedure

1 Login to the server as root.

2 Type "`./release-1.0.0.<build_number>.bin -i gui`" to run the installer in the graphical installer mode, press **Enter**.

Installer introduction appears.

3 Click **Next** to continue.

License agreement appears.

4 Select the checkbox "**I agree to the terms of the License agreement**" and click **Next**.

Installer prompts to choose an install folder.

5 Click **Next** to accept the default or choose a location for the install folder.

This is the location where DCF will be installed.

Note If Install folder already contains DCF folder, Installer cancels the installation and exits.

6 Installer prompts to enter the Controller port. Press **Enter** to choose the default port.

This is the port on which DCF-CONTROLLER service will start. Port number must be between 1 to 65535. If wrong port number is entered, Installer throws a validation error and redirects to re-enter the Port details.

7 The installer prompts to enter the **Controller user name**. Click **Next** to choose the default user name.

Installer Prompts for Controller Password.

8 Enter **Controller Password** and Confirm the Password when Installer prompts.

Note Password must not leave blank. You must enter the password. These user name and password is required to authenticate REST calls.

If passwords are not matched, installer throws a validation error and redirects to re-enter the password at step 8.

9 Installer prompts to enter **MongoDB URI**. Click **Next** to choose the default URI.

10 Installer prompts to enter the **MongoDB User Name**. Click **Next** to choose the default user name.

11 Installer prompts to enter MongoDB Password, enter the Password and Confirm Password when installer prompts for confirmation. The password must not be left blank.

Note Make sure these user name and password are same as the password created during MongoDB setup. If passwords do not match, installer throws a validation error and redirects to re-enter the password at step 11.

12 Click **Next** to continue when pre-install summary is displayed.

Note Installer triggers rollback action on any kind of failure. Except DCF_Logs all files and folders will be uninstalled. Errors can be seen inside “DCF_Logs/INSTALL_ERR.log”.

13 Click **Done** to exit the installer when Install Completed message displays.

DCF installation is completed.

What to do next

After successful DCF installation, Install **VMware Smarts Notification Collector** to pull all the events from Smarts Presentation SAM and publish the same to KAFKA for consumption.

Install DCF in Silent Mode

A DCF silent installation is an installation procedure that continues without user interaction.

Table 2-1. Variables Properties and Description

Property	Description
Replay feature output	This file was built by the Replay feature of InstallAnywhere. It contains variables that were set by Panels, Consoles or Custom Code.
USER_INSTALL_DIR	Choose Install Folder, =/opt/DCF.
CTRL_URI_1=8443	Controller Details, Controller Port.
CTRL_UN	Controller Username.
CTRL_PWD	Controller Password.
MDB_URI	MongoDB Details. MongoDB URL. MDB_URI=127.0.0.1:27017.
MDB_UN	MongoDB Username.
MDB_PWD	MongoDB Password.

Prerequisites

Create a configuration file for the installer to execute the installation. To create configuration file:

1 Copy the sample configuration file from the distribution (`installer.properties`) to a directory on the server where you are installing DCF.

2 Use any editor (vi/vim) to modify this file.

3 Define each of the properties in this file for server type, according to Table Variables Properties and Description. Save the changes to the file.

Procedure

1 Login to server as root.

2 Type "`./release-1.0.0.<build_number>.bin -i silent -f installer.properties`" to run the installer in the silent installer mode, press **Enter**.

> **Note** Any user interaction is not required for this installer. Once it completes, a message displays indicating that installation is completed, and you are returned to the shell prompt. Logs are available at `<DCF_INSTALL_DIRECTORY>/DCF_Logs.`

What to do next

After successful DCF installation, Install **VMware Smarts Notification Collector** to pull all the events from Smarts Presentation SAM and publish the same to KAFKA for consumption.

Installing Eventstore

3

This chapter includes the following topics:

- Install Eventstore using Console Mode
- Install Eventstore using Graphical Mode
- Install Eventstore in Silent Mode

Install Eventstore using Console Mode

You can install the Eventstore on the platform of supported Linux hosts. One server can support only one instance of Eventstore installation.

Prerequisites

Fulfill the following prerequisites before starting the installation:

1. Installation server must have java version 1.8+ installed.
2. Installation server must support bash, sed and curl utility.
3. Elastic Search - version 6.4.2 must be installed.
   a. User name and password authentication must be enabled for Elastic Search.
   b. Minimum 3 node Elastic Search Cluster is required for high availability.
4. Redis - version 5.0.2 must be installed and running.
   a. Password Authentication must be enabled for Redis.
   b. For Redis minimum 6 node (3 Master, 3 Salve) cluster is required which can be deployed over 3 machines.
5. Kafka - version 2.0.0 must be installed and running.
   a. SASL/PlainText based authentication must be enabled in kafka.
   b. A topic must be created with 1 partition.
   c. Zookeeper must be running.
   d. Minimum 3 node Kafka Broker is required for high availability. In Cluster mode, it is recommended to create a topic with 1 partition and 3 replication factor.

   e Optional: Enabling SSL (encryption) using SASL/SSL mechanism between Kafka Broker and Clients with 1-way authentication is also supported.

6 Smarts Presentation SAM must be already running.

   a EDAA must be enabled and smarts tomcat service must be running.

   b Optional: Enabling HTTPS in EDAA is also supported.

7 Copy the **eventstore-install.bin** installer to any directory on the server where Eventstore can be installed.

8 Ensure that you have a login with root privileges to run the installer.

9 Download the installation file from support.vmware.com and place it in a temporary location on the server.

Procedure

1 Login to the server as root.

2 Type `bash eventstore-install.bin -i console` to run the installer in the console-based installer mode and hit **Enter**.

   The command prompt screen appears.

3 Press **Enter**.

   Installer introduction continues.

4 Press **Enter** to accept the default location when Installer prompts to choose an Install folder or provide the desired location.

   This is the location where you can find Eventstore is installed.

5 If the Install folder already contains Eventstore folder, installer prompts for the below selections.

   - Enter **1** to override the already installed folder and Press **Enter** to continue.
   - or Enter **2** to choose a new installation directory and Press **Enter** to continue.
   - or Enter **3** to cancel the installation and Press **Enter.**

6 Press Enter to continue when installer prompts to enter the Eventstore port.

   This is the port in where Eventstore service starts. Port number must be between 1 to 65535. If wrong port number is entered, Installer will throw a validation error and redirect to re-enter the Port details. Default port is 8080.

7 The installer prompts to choose the protocol for communication:

- Choose option **1** for https communication and Press **Enter** to continue.

  or

- Choose option **2** for http communication Press **Enter** to continue.

Note 1. Default is http. For “https” you must ensure that “esdb.crt” file is available in “/opt/ssl”. For configuring https in Elastic Search refer section Enabling HTTPS in Elastic Search.

Note 2. The certificate file esdb.crt must contain certificates from all elastic search instances in a cluster.

8 Installer prompts for Elastic Search Configurations.

- Enter the Elastic search IP or FQDN or Hostname in the format <IP-ADDRESS/FQDN/HOSTNAME>:<PORT>. In case of cluster enter the comma separated IP or FQDN or Hostname address.
- Type the **Elastic Search Username** and press **Enter** to continue.

(To enable ES authentication refer Elasticsearch Authentication).

9 Enter the **Elastic Search Password** when prompted and confirm **Elastic Search Password** when prompted for confirmation.

If Passwords are mismatched, installer throws a validation error and redirect to re-enter the password. Verify if any fields are blank to avoid the installer validation error and redirection of step 8.

Also verify if the first IP/fqdn/hostname address of Elastic Search entered, is reachable from Installation server. Otherwise, installer will throw a connectivity error, and redirect to at the beginning of step 8.

10 Provide **Redis IP Address** and press **Enter** to continue when installer prompts to enter Redis configuration.

In case of Redis cluster enter the Comma separated IP in the format

<IP-ADDRESS>:<PORT>

Default is 127.0.0.1:6379

(For redis authentication refer Redis Cluster Authentication).

Note 1. Eventstore supports only Redis Cluster with 3 Redis Master instance. A single non-cluster redis instance is not supported.

Note 2. Verify if you have entered the IP address in a correct format. Otherwise, installer throws a validation error and redirects to this step again.

11 Enter **Redis Password** and confirm **Redis Password** again when installer prompts. Press **Enter** to continue.

Note Installer throws a validation error and redirect to the beginning of step 11 if the passwords are mismatching.

12 Installer prompts to enter the Kafka SASL configuration. You can choose SASL_PLAINTEXT or SASL_SSL for Kafka communication.

SASL_PLAINTEXT: User name and Password authentication without encryption of data.

SASL_SSL: User name and Password authentication with SSL encryption.

For SSL encrypted communication ensure that " kafka.crt " file is available in "/opt/ssl". Default is SASL_SSL.

- Choose **1** for SASL_PLAINTEXT, press **Enter** to continue.

  (For Enabling Kafka authentication using SASL/PLAINTEXT, refer Kafka Kafka SASL_PLAIN Authentication Configuration).

  or

- Choose **2** for SASL_SSL Enter the KAKFA TOPIC, press **Enter** to continue.

  (For Enabling Kafka authentication with SSL Encryption using SASL/SSL, refer Kafka SASL_SSL Authentication Configuration).

13 Installer prompts to enter the kafka configuration:

a Enter **KAKFA ADDRESS**.

Kafka IP/fqdn/hostname address must be in the format <IP-ADDRESS/FQDN/HOSTNAME>:<PORT>.

For Kafka cluster enter the comma separated address.

b Enter **KAKFA TOPIC.** Default is sam_notification.

Note The topic must be already created with 1 partition only.

c Enter **KAFKA Username**, press **Enter** to continue.

14 Enter the **Kafka Password** and Confirm **Kafka Password** when Installer prompts for confirmation.

If Passwords are mismatched, installer throws a validation error and redirect to the beginning of step 14.

15 Installer prompts for the choice of communication protocol https and default (http)

- Enter **1** for https and press Enter to continue. For **https,** ensure that “**sam.crt**” is available in “/opt/ssl”.

  To import the SAM certificate refer Enabling HTTPS in SAM.

  or

- Enter **2** for **http** and press **Enter** to continue. Http is default.

16 Enter the presentation **SAM configuration details** when Installer prompts. Enter the IP/fqdn/hostname address for SAM in the format <IP-ADDRESS/FQDN/HOSTNAME>:<PORT>).Press **Enter** to continue.

   If any input fields are empty, installer throws a validation error and redirects to the beginning of this step 16.

   Note In SAM, Port 8080 is enabled in http mode and Port 8443 is enabled in https mode.

17 Press **Enter** to continue when Pre install summary is displayed.

   Installation continues.

18 Press **Enter** to exit the installer.

   Install Completed message is displayed.

What to do next

After successful EventStore installation, install 3 elastic search plugins on all elastic search instances in the cluster by following these steps:

1 Copy the plugins directory containing "ChainingSupport-6.4.2.zip, elasticsearch-arrayformat-6.4.2.zip and elasticsearch-userprofile-6.4.2.zip" from "<EventStore_INSTALL_DIR>/evenstore/plugins/" to the <PLUGIN-DIRECTORY> where Elastic Search is running. Here <PLUGIN-DIRECTORY> can be any directory.

2 After copying run the following command to install each plugin:

```
1. /path/to/elasticsearch/bin/elasticsearch-plugin install file:///<PLUGIN
DIRECTORY>/
plugins/ChainingSupport-6.4.2.zip
2. /path/to/elasticsearch/bin/elasticsearch-plugin install file:///<PLUGIN
DIRECTORY>/
plugins/elasticsearch-arrayformat-6.4.2.zip
3. /path/to/elasticsearch/bin/elasticsearch-plugin install file:///<PLUGIN
DIRECTORY>/
plugins/elasticsearch-userprofile-6.4.2.zip
```

3 After installing all the plugins restart the **Elastic Search Service** on all cluster nodes.

Install Eventstore using Graphical Mode

This installation procedure describes the steps of Eventstore installation in the Graphical Interface. One server can support only one instance of Eventstore installation.

Prerequisites

- Ensure that you have a login with root privileges to run the installer.
- Download the installation file from support.vmware.com and place it in a temporary location on the server.

Procedure

1. Log in to the server as root.

   Logged in with root privileges.

2. Type bash `eventstore-install.bin -i gui` to run the installer in the graphical installer mode, and press **Enter**.

   Installer introduction appears.

3. Click **Next.**

   Installer introduction continues.

4. Installer prompts to choose an install folder, click **Next** to continue with the Default folder.

   Default is /opt/eventstore.

5. If the install folder already contains eventstore folder you can choose appropriate options from any of the following:

   - Click **Yes** to override the already installed folder.

     or

   - Click **No** to choose a new installation directory.

     or

   - Click **Cancel** to cancel the installation.

6. Click **Next** to continue when installer prompts to enter the eventstore port .

   This is the port in which eventstore service starts. Port number must be between 1 to 65535. If wrong port number is entered, installer will throw a validation error and redirect to re-enter the Port details. Default port is 8080.

7. The Installer prompts you to choose any of the below protocol for communication.

   - Click “https” radio button for https communication and click **Next** to continue.

     or

   - Click “http” radio button for http communication and click **Next** to continue.

     Note 1. For “https” communication ensure that “esdb.crt” file is available in “/opt/ssl”. (For configuring https in elastic search refer Enabling HTTPS in Elastic Search).

     Note 2. The certificate file esdb.crt should contain certificates from all elastic search instances in a cluster.

8. Installer prompts for Elastic Search Configurations:

   a. Enter the Elastic search IP or FQDN or Hostname in the format <IP-ADDRESS/FQDN/HOSTNAME>:<PORT>. In case of cluster enter the comma separated IP or FQDN or Hostname address.

b Type the **Elastic Search Username** and click **Next** to continue. (To enable ES authentication refer Elasticsearch Authentication).

9 Enter the **Elastic Search Password** when installer prompted and click **Next** to continue.

Password confirmation prompt appears.

10 Enter **Elastic Search Password** again when prompts for confirmation and click **Next** to continue.

Installer throws a validation error and redirects to the beginning of step 9 if the password mismatches. Verify if any fields are blank to avoid the installer validation error and redirects to step 8.

Also verify if the first IP/fqdn/hostname address of Elastic Search entered, is reachable from Installation server. Otherwise, installer will throw a connectivity error, and redirects to the beginning of step 8.

11 Enter **Redis IP address** when installer prompts for Redis configurations and click **Next** to continue.

For Redis cluster enter the Comma separated IP in the format <IP-ADDRESS>:<PORT> Default is 127.0.0.1:6379 (For redis authentication refer Redis Cluster Authentication).

Note 1. Eventstore supports only Redis Cluster with 3 Redis Master instance. A single non-cluster redis instance is not supported.

Note 2. Verify if you have entered the IP address in a correct format. Otherwise, installer throws a validation error and redirects to this step again.

12 Enter the **Redis Password** when installer prompts and click **Next** to continue.

Installer prompts for password confirmation.

13 Enter **Redis Password** when prompts for confirmation and click **Next** to continue.

Installer throws a validation error and redirects to the beginning of step 12 if the passwords are mismatched.

14 Installer prompts to enter Kafka SASL Configuration. You can choose SASL_PLAINTEXT or SASL_SSL for Kafka communication.

SASL_PLAINTEXT: User name and Password authentication without encryption of data.

SASL_SSL: User name and Password authentication with SSL encryption.

For SSL encrypted communication ensure that " kafka.crt " file is available in "/opt/ssl". Default is SASL_SSL.

a Click **SASL_PLAINTEXT** radio button for SASL_PLAINTEXT, click **Next** to continue.

(For Enabling Kafka authentication using SASL/PLAINTEXT, refer Kafka SASL_PLAIN Authentication Configuration).

or

b Click **SASL_SSL** radio button for SASL_SSL, click **Next** to continue.

(For Enabling Kafka authentication with SSL Encryption using SASL/SSL, refer Kafka SASL_SSL Authentication Configuration).

15 Installer prompts to enter the kafka configuration.

a Enter **KAKFA ADDRESS.** Kafka IP/fqdn/hostname address must be in the format <IP-ADDRESS/FQDN/HOSTNAME>:<PORT>. For Kafka cluster enter the comma separated address.

b Enter **KAKFA TOPIC**. Default is sam_notification.

Note The topic must be already created with 1 partition only.

c Enter **KAFKA Username**, click **Next** to continue.

Note Installer throws a validation error if any input fields are empty and redirects to the beginning of this step 15.

16 Enter the **KAFKA Password** when installer prompts and click **Next** to continue.

Installer prompts for password confirmation.

17 Enter **KAFKA Password** again when prompts for confirmation and click **Next** to continue.

Installer throws a validation error and redirects to the beginning of step 12 if the passwords are mismatched.

18 Installer prompts to choose the communication protocol for presentation SAM. Default is http.

- Click **https** radio button for https communication and Click **Next** to continue.

  For https, ensure that “sam.crt” is available in `/opt/ssl`. To import the SAM certificate refer Enabling HTTPS in SAM.

  or

- Click **http** radio button for http communication and Click **Next** to continue.

19 Enter the presentation **SAM configuration details** when Installer prompts. Enter the IP/fqdn/hostname address for SAM in the format <IP-ADDRESS/FQDN/HOSTNAME>:<PORT>). Click **Next** to continue.

Installer throws a validation error if any input fields are empty and redirects to the beginning of this step 19.

Note In SAM Port 8080 is enabled in http mode and Port 8443 is enabled in https mode.

20 Click **Next** to continue when Pre install summary is displayed.

installation continues.

21 Click **Done** to exit the Installer.

Install Completed message is displayed.

What to do next

After successful EventStore installation, install 3 elastic search plugins on all elastic search instances in the cluster by following these steps:

1 Copy the plugins directory containing "ChainingSupport-6.4.2.zip, elasticsearch-arrayformat-6.4.2.zip and elasticsearch-userprofile-6.4.2.zip" from "<EventStore_INSTALL_DIR>/evenstore/plugins/" to < PLUGIN-DIRECTORY > where Elastic Search is running.

   Here <PLUGIN-DIRECTORY> can be any directory.

2 After copying Run the following command to install each plugin:

```
1. /path/to/elasticsearch/bin/elasticsearch-plugin install file:///<PLUGIN
DIRECTORY>/
plugins/ChainingSupport-6.4.2.zip
2. /path/to/elasticsearch/bin/elasticsearch-plugin install file:///<PLUGIN
DIRECTORY>/
plugins/elasticsearch-arrayformat-6.4.2.zip
3. /path/to/elasticsearch/bin/elasticsearch-plugin install file:///<PLUGIN
DIRECTORY>/
plugins/elasticsearch-userprofile-6.4.2.zip
```

3 After installing all the plugins Restart the **Elastic Search Service** on all cluster nodes.

Install Eventstore in Silent Mode

A silent installation is an installation procedure that continues without user interaction. It requires no user intervention from start to finish. This installation is performed using a user-modifiable response file, which enables you to easily duplicate the installation on many computer systems.

Table 3-1. Variables Property and Description

Property	Description
USER_INSTALL_DIR	Install directory for eventstore.
ES_PROTOCOL	Choose the protocol (http/https) for Elastic Search communication. For https communication ensure that "esdb.crt" certificate is available on "/opt/ssl". For https set ES_PROTOCOL to " https". For http set ES_PROTOCOL to " http ".
ES_CERT_FILE	If https is enabled for ES then set the CERT FILE location else leave it blank. For example, ES_CERT_FILE=/opt/ssl/esdb.crt.
EVENTSTORE_PORT_NO	Event Store Port. Enter the port number in which you want to start the Event Store.
ES_ADDRESS	Elastic search IP/fqdn/hostname address in the format <IP-ADDRESS/FQDN/HOSTNAME>:<PORT> For Elastic search cluster, enter the comma separated address.
ES_USER_NAME	Elastic search user name.
ES_PASSWORD	Elastic Search Password.

Table 3-1. Variables Property and Description (Continued)

Property	Description
REDIS_IP_ADDRESS	REDIS IP ADDRESS. Example: 127.0.0.1:6379 For Redis cluster, enter the comma separated IP in the format <IP-ADDRESS>:<PORT>.
REDIS_PASSWORD	Redis Password.
KAFKA_SASL_PROTOCOL	Kafka SASL Configuration. For SSL encrypted communication, ensure that " kafka.crt" file is available in "/opt/ssl". Set KAFKA_SASL_PROTOCOL to SASL_PLAINTEXT or SASL_SSL. SASL_PLAINTEXT : User name and Password authentication without encryption of data. SASL_SSL: User name and Password authentication with SSL encryption. Example: KAFKA_SASL_PROTOCOL=SASL_SSL
KAFKA_ADDRESS	KAFKA IP ADDRESS. For Kafka cluster, enter the comma separated IP/fqdn/hostname in the format <IP-ADDRESS/FQDN/HOSTNAME>:<PORT>.
KAFKA_TOPIC	KAFKA Topic. Example: KAFKA_TOPIC =sam_notification.
KAFKA_USER_NAME	KAFKA User Name.
KAFKA_PASSWORD	Kafka Password.
SAM_PROTOCOL	Choose the protocol (http/https) for SAM communication. For https communication, ensure that " sam.crt" certificate is available on "/opt/ssl". For https set SAM_PROTOCOL to " https". For http set SAM_PROTOCOL to " http ".
SAM_CERT_FILE	If https is enabled for SAM then set the CERT FILE location else leave it blank. Example: SAM_CERT_FILE =/opt/ssl/sam.crt.
SAM_ADDRESS	SAM IP ADDRESS. Enter the the IP/fqdn/hosname address in the format <IP-ADDRESS/FQDN/HOSTNAME>:<PORT>.

Prerequisites

Create a configuration file for the installer to execute the installation. To create configuration file:

1 Copy the sample configuration file from the distribution `eventstore-installer.properties` to a directory on the server where you are installing eventstore.

2 Use any editor (vi/vim) to modify this file.

3 Define each of the properties in this file, according to Table - Variables Property and Description.

4 Save the changes to the file.

Procedure

1 Login to the server as root.

2 Type bash `eventstore-install.bin -f <response file location> -i silent` and press **Enter**.

Note Any user interaction is not required for this installer. Once it completes, a message displays indicating that installation is completed, and you are returned to the shell prompt. If the installer is unable to complete the installation, an error message is saved in the

[Product directory]/eventstore_logs.

What to do next

After successful EventStore installation, install 3 elastic search plugins on all elastic search instances in the cluster by following these steps:

1 Copy the plugins directory containing "ChainingSupport-6.4.2.zip, elasticsearch-arrayformat-6.4.2.zip and elasticsearch-userprofile-6.4.2.zip" from "<EventStore_INSTALL_DIR>/evenstore/plugins/" to < PLUGIN-DIRECTORY > where Elastic Search is running.

   Here <PLUGIN-DIRECTORY> can be any directory.

2 After copying Run the following command to install each plugin:

```
1. /path/to/elasticsearch/bin/elasticsearch-plugin install file:///<PLUGIN DIRECTORY>/
plugins/ChainingSupport-6.4.2.zip
2. /path/to/elasticsearch/bin/elasticsearch-plugin install file:///<PLUGIN DIRECTORY>/
plugins/elasticsearch-arrayformat-6.4.2.zip
3. /path/to/elasticsearch/bin/elasticsearch-plugin install file:///<PLUGIN DIRECTORY>/
plugins/elasticsearch-userprofile-6.4.2.zip
```

3 After installing all the plugins Restart the Elastic Search Service on all cluster nodes.

Installing cAPI

4

This chapter includes the following topics:

- Install cAPI using Console Mode
- Install cAPI using Graphical Mode
- Install cAPI in Silent Mode

Install cAPI using Console Mode

You can install cAPI on supported Linux Platform. Console mode provides a text-based method for invoking the installation program. This mode is intended for Linux platforms with non-graphics consoles.

Prerequisites

Fulfill the following prerequisites before starting the installation:

1 Ensure Event store is installed already.

2 Ensure that minimum 3 node elastic search cluster is already installed.

3 Ensure java version 1.8+ is already installed.

4 Ensure bash and curl utility are already installed and installation server is compatible with "`sed`" command.

5 Create Client Id and Shared Secret in VIDM for cAPI.

   Refer the cAPI-vIDM Configuration and Authentication.

6 Copy the "`cAPI-install.bin` " installer to any directory on the server where cAPI will be installed.

7 Ensure that you have a login with root privileges to run the installer.

8 Download the installation file from support.vmware.com and place it in a temporary location on the server.

Procedure

1 Login to the server as root.

   Logged in with root privileges.

2 Type `bash cAPI-install.bin -i console` to run the installer in the console-based installer mode, press **Enter**.

   Installer introduction appears.

3 Press **Enter** to continue.

   Installer Prompts to choose an install folder.

4 Press **Enter** to continue.

   This is the location where cAPI will be installed. Default is /opt/cAPI.

5 If install folder already contains cAPI folder, choose from the following options

   - Enter **1** to override the already installed folder.

     or

   - Enter **2** to choose a new installation directory.

     or

   - Enter **3** to cancel the installation.

6 Installer prompts for cAPI configuration.

   a Enter **cAPI ADMIN port**. Default port 9901.

   b Enter **cAPI Listener port**. Default port 10000.

   c Press **Enter** to continue.

   Note The port number must be between 1 to 65535. Otherwise, installer throws validation error and redirects to this step to re-enter the port details.

7 Installer prompts to enter the cAPI configuration.

   a Enter **VIDM HOST NAME**. Default is identitymanager.eng.vmware.com.

   b Enter the **VIDM IP ADDRESS**. Default is 127.0.0.1

   c Enter the **VIDM PORT**. Default port is 443.

   d Press **Enter** to continue.

   Note If the IP address is wrong or the Port is invalid, installer throws validation error and redirects to the beginning of this step to enter the configurations.

8 Choose the Elastic Search https Configuration when installer prompts. Default is http.

   - Choose **1** for https and Press **Enter** to continue.

     or

- Choose **2** for http and Press **Enter** to continue.

Note 1. For https communication in Elastic search ensure that "esdb.crt" file is available in "/opt/ssl". For configuring https refer Enabling HTTPS in Elastic Search.

Note 2. The certificate file esdb.crt should contain certificates from all elastic search instances in a cluster.

9 Installer prompts for Elastic Search configurations.

a Enter the Elastic search IP/fqdn/hostname in the format <IP-ADDRESS/FQDN/HOSTNAME>:<PORT>. In case of cluster, enter the comma separated IP/fqdn/hostname address.

b Enter Elastic Search **User name** and press **Enter** to continue.

To enable ES authentication, refer Elasticsearch Authentication.

Note Installer throws validation error and redirects to the beginning of this step to enter the configurations if any input fields are left blank.

10 Enter the **Elastic Search Password** when installer prompts, press **Enter** to continue.

Installer prompts for password confirmation.

11 Press **Enter** to continue.

If the passwords are mismatched, installer throws a validation error and redirects to re-enter the password at step 10.

12 Enter EventStore configuration when installer prompts.

a Enter **Event Store IP Address**. Default is 127.0.0.1.

b Enter **Event Store Port**. Default is 8080.

c Press **Enter** to continue.

Note If the IP address is wrong or the Port is invalid, installer throws validation error and redirects to the beginning of this step to enter the configurations.

13 Installer prompts to enter the Client Registration configuration.

a Provide **Client ID**. Default is capi_client.

b Provide **Secret** and press **Enter** to continue.

Note Client ID and Secret is a one-time configuration of an Oauth2 client that supports password grant on VIDM.

Refer cAPI-vIDM Configuration and Authentication for configuration details.

Installer throws an error and redirects to the beginning of this step to enter the configurations if any input filed left blank.

14 Press **Enter** to continue the installation when installer shows the pre-install summary.

   Installation continues.

15 Press **Enter** to exit the installer when installer shows the installation is completed.

   cAPI is installed.

Install cAPI using Graphical Mode

This installation procedure describes the steps of cAPI installation in the Graphical Interface.

Prerequisites

- Ensure that you have a login with root privileges to run the installer.
- Download the installation file from support.vmware.com and place it in a temporary location on the server.

Procedure

1 Log in to the server as root.

   Logged in with root privileges.

2 Type `bash cAPI-install.bin -i gui` to run the installer in the graphical mode, press **Enter**.

   Introduction to the installer appears.

3 Click **Next** to continue.

   Installer prompts to choose an install folder.

4 Click **Choose.**

   This is the location where cAPI will be installed. Default is /opt/cAPI.

5 Click **Next** to continue.

   Installer checks if any cAPI folder existing inside install folder.

6 If install folder already contains cAPI folder, choose from the following options:

   - Click **Yes** to override the already installed folder.
   - Click **N**o to choose a new Installation directory.
   - Click **Cancel** to cancel the Installation.

7 Installer prompts for cAPI configuration.

   a Enter **cAPI ADMIN port**. Default port 9901.

   b Enter **cAPI Listener port**. Default port 10000.

c Click **Next** to continue.

Note The port number must be between 1 to 65535. Otherwise, installer throws validation error and redirects to this step to re-enter the port details.

8 Installer prompts to enter the cAPI configuration.

a Enter **VIDM HOST NAME**. Default is identitymanager.eng.vmware.com.

b Enter the **VIDM IP ADDRESS**. Default is 127.0.0.1.

c Enter the **VIDM PORT**. Default port number is 443.

d Click **Next** to continue.

Note If the IP address is wrong or the Port is invalid, installer throws validation error and redirects to the beginning of this step to enter the configurations.

9 Choose the Elastic Search https Configuration when installer prompts. Default is http.

- Click **https** radio button for https communication and Click **Next** to continue.

  or

- Click **http** radio button for http communication and Click **Next** to continue.

Note 1. For https communication in Elastic search ensure that "esdb.crt" file is available in "/opt/ssl". For configuring https refer Enabling HTTPS in Elastic Search.

Note 2. The certificate file esdb.crt should contain certificates from all elastic search instances in a cluster.

10 Installer prompts for Elastic Search configurations.

a Enter the Elastic search IP/fqdn/hostname in the format <IP-ADDRESS/FQDN/HOSTNAME>:<PORT>. In case of cluster enter the comma separated IP/fqdn/hostname address.

b Enter Elastic Search **User name** and click **Next** to continue.

To enable ES authentication refer the Elasticsearch Authentication.

Note Installer throws validation error and redirects to the beginning of this step to enter the configurations if any input filed left blank.

11 Enter the **Elastic Search Password** when installer prompts, click **Next** to continue.

Installer prompts for password confirmation.

12 Confirm **Elastic Search Password** when installer prompts for confirmation, click **Next** to continue.

If the passwords are mismatched, installer throws a validation error and redirects to re-enter the password at step 11.

13 Enter EventStore configuration when installer prompts.

   a Enter **Event store IP address**. Default is 127.0.0.1.

   b Enter **Event store port**. Default is 8080.

   c Click **Next** to continue.

   If the IP address is wrong or the Port is invalid, installer throws validation error and redirects to the beginning of this step to enter the configurations.

14 Installer prompts to enter the Client Registration configuration.

   a Provide Client ID. Default is capi_client.

   b Provide **Secret** and click **Next** to continue.

   Note Client ID and Secret is a one-time configuration of an Oauth2 client that supports password grant on VIDM. Refer cAPI-vIDM Configuration and Authentication for configuration details.

   Installer throws an error and redirects to the beginning of this step to enter the configurations if any input filed is left blank.

15 Click **Install** to continue the installation when displays pre-install summary.

   Installation continues.

16 Click **Done** to exit the installer.

   Installer displays installation is completed.

Install cAPI in Silent Mode

A silent installation is an installation procedure that continues without user interaction. It requires no user intervention from start to finish. This installation is performed using a user-modifiable response file, which enables you to easily duplicate the installation on many computer systems.

Table 4-1. Variables Property and Description

Property	Description
USER_INSTALL_DIR	Install directory for cAPI.
ADMIN_PORT	Admin Port: cAPI admin port.
LISTENER_PORT	Listener Port: cAPI client port, where cAPI listens incoming request.
VIDM_HOST_NAME	VIDM Host Name. example: identitymanager.eng.vmware.com.
VIDM_IP_ADDRESS	VIDM IP Address (example: 127.0.0.1)
VIDM_PORT	VIDM Port.
ES_PROTO	Choose the protocol for communication. For https communication ensure that "esdb.crt" certificate is available on "/opt/ssl". For https set ES_PROTO to "https". For http set ES_PROTO to "http".

Table 4-1. Variables Property and Description (Continued)

Property	Description
ES_ADDRESS	Elastic Search IP Address. For Elastic search cluster, please use the comma separated IP/fqdn/hostname in the format: <IP-ADDRESS/FQDN/HOSTNAME>:<PORT>.
ES_USER_NAME	Elastic Search User Name.
ES_PASSWORD	Elastic Search Password.
EVENTSTORE_IP_ADDRESS	EventStore IP Address.
EVENTSTORE_PORT	EventStore Port.
CLIENT_ID	Client ID. **Note** Client registration configuration. ClientID and Secret is onetime configuration of an Oauth2 client that supports password grant on vIDM.
SECRET	Secret.

Prerequisites

Create a configuration file for the installer to execute the installation. To create configuration file:

1 Copy the sample configuration file from the distribution `cAPI-installer.properties` to a directory on the server where you are installing cAPI.

2 Use any editor (vi/vim) to modify this file.

3 Define each of the properties in this file, according to Table - Variables Property and Description.

4 Save the changes to the file.

Procedure

1 Log in to the server as root.

2 Type `bash cAPI-install.bin -f <response file location> -i silent` and press **Enter**.

Note Any user interaction is not required for this installer. Once it completes, a message displays indicating that installation is completed, and you are returned to the shell prompt. If the installer is unable to complete the installation, an error message is saved in the [Product directory]/cAPI_logs.

Installing Smarts-UI

5

This chapter includes the following topics:

- Install Smarts-UI using Console Mode
- Install Smarts-UI using Graphical Mode
- Install Smarts-UI in Silent Mode

Install Smarts-UI using Console Mode

You can install Smarts-UI on supported Linux Platform. This procedure describes Smarts-UI installation in Console Mode.

Prerequisites

Fulfill the following prerequisites before starting the installation:

1 Ensure Eventstore and cAPI are already installed on the Installation server.

2 Ensure java version 1.8+ is already installed on the Installation server .

3 Ensure bash is already installed on the Installation server.

4 Ensure bash and curl utility are already installed and installation server is compatible with "`sed`" command.

5 SE Linux must be disabled in installation server.

6 Create Client Id and Shared Secret in VIDM for smarts-ui installation. Refer VIDM Authentication with Notification GUI.

7 Copy the "`smartsui-install.bin`" installer to any directory on the server where smarts-ui will be installed.

8 KPI should be installed and running. For KPI installation refer to VMware-K4M-1.0.0.0-Installation-and-Administration-Guide.

9 Installation server must have httpd and mod-ssl installed.

10 When you install Smart-UI on a Linux Platform, assign executable permissions to the installation script.

11 Ensure that you have a login with root privileges to run the installer.

12 Download the installation file from support.vmware.com and place it in a temporary location on the server.

Procedure

1 Login the server as root.

2 Type `bash smartsui-install.bin -i console` to run the installer in the console-based installer mode, press **Enter**.

   Introduction to the installer appears.

3 Press **Enter** to continue.

   Installer prompts to choose an install folder.

4 Press **Enter** to continue.

   This is the location where smarts-ui will be installed. Default is /opt/ smarts-ui.

5 If install folder already contains smarts-ui folder, choose from the following options.

   - Enter **1** to override the already installed folder.

     or

   - Enter **2** to choose a new Installation directory.

     or

   - Enter **3** to cancel the Installation.

6 Installer prompts for VIDM configuration.

   a Enter the **client ID**.

   b Enter the **Shared Secret.**

   c Enter **VIDM Host Name**. Default is identitymanager.eng.vmware.com.

   d Enter the **Auth application Port**. Default port is 8082.This is the port where auth application will start.

   e Press **Enter** to continue.

   Note Installer throws validation error and redirects to the beginning of this step to enter the configurations if any input filed left blank.

   For VIDM configuration, refer VIDM Authentication with Notification GUI.

7 Installer prompts to enter the cAPI configuration. Enter cAPI IP Address in the format <IP-ADDRESS:PORT> and Press **Enter** to continue.

   Default value for this fields is 127.0.0.1:10000 The port number is cAPI listener port provided during cAPI Installation. If the input is in wrong format, installer throws validation error and redirects to the beginning of this step to enter the configurations.

8 Enter ssl.conf directory and Press **Enter** to continue when installer prompts to choose the ssl.conf folder location.

   Default value is /etc/httpd/conf.d. If ssl.conf is not existing on the directory, Installer throws an error and redirects to the beginning of step 8 to re-enter the configuration.

9 Provide KPI REST API URL when prompts and press **Enter** to continue.

   Default value is 127.0.0.1:8083. This is the address where KPI is running.

   Note Installer throws validation error and redirects to the beginning of this step to enter IP Address if IP Address input filed left blank.

10 Press **Enter** to continue the installation when installer shows the pre-install summary.

   Installer continues the installation.

11 Press **Enter** to exit the installer when installer shows the installation is completed.

What to do next

After successful Smart-UI installation, follow the steps provided in Export VIDM Certficate section to export and import VIDM certificates.

Install Smarts-UI using Graphical Mode

This installation procedure describes the procedure of Smarts-UI installation in the Graphical Interface.

Prerequisites

1 Ensure that you have a login with root privileges to run the installer.

2 Download the installation file from support.vmware.com and place it in a temporary location on the server.

Procedure

1 Login to the server as root.

2 Type `bash smartsui-install.bin -i` to gui to run the installer graphical mode, press **Enter**.

3 Click **Next** to continue when introduction to the installer appears.

   Installer prompts to choose an install folder.

4 Choose a location and click **Next** to continue.

   This is the location where smarts-ui will be installed. Default is /opt/ smarts-ui.

5 If install folder already contains smarts-ui folder, choose from the following options:

   - Click **Yes** to override the already installed folder.

     or

- Click **No** to choose a new Installation directory.

  or

- Click **Cancel** to cancel the Installation.

6 Installer prompts for VIDM configuration.

   a Enter the **Client ID**.

   b Enter the **Shared Secret**.

   c Enter **VIDM Host Name**. Default is identitymanager.eng.vmware.com.

   d Enter the **Auth application Port**. Default port is 8082.This is the port where auth application starts.

   e Click **Next** to continue.

   For VIDM configuration refer vidm.docx.

   Installer throws validation error and redirects to the beginning of this step to enter the configurations if any input filed left blank.

7 Installer prompts to enter the **cAPI configuration**.Enter cAPI IP Address in the format <IP-ADDRESS:PORT> and click **Next** to continue.

   Default value for this fields is 127.0.0.1:10000. The port number is cAPI listener port provided during cAPI Installation.

   If the input is in wrong format, installer throws validation error and redirects to the beginning of this step to enter the configurations.

8 Choose ssl.conf directory and click **Next** to continue when installer prompts to choose the ssl.conf folder location.

   Default value is /etc/httpd/conf.d

   Note If ssl.conf is not existing on the directory, installer throws an error and redirects to the beginning of step 8 to re-enter the configuration.

9 Provide **KPI REST API URL** when prompts and click **Next** to continue.

   Default value is 127.0.0.1:8083.This is the address where KPI is running.

   Installer throws validation error and redirects to the beginning of this step to enter IP Address if IP Address input filed left blank.

10 Click **Install** to continue the installation when installer shows the pre-install summary.

   Installation continues.

11 Click **Done** to exit the installer when installer displays as completed.

   Installation is completed.

What to do next

After successful Smart-UI installation, follow the steps provided in Export VIDM Certficate section to export and import VIDM certificates.

Install Smarts-UI in Silent Mode

A silent installation is an installation procedure that continues without user interaction. It requires no user intervention from start to finish. This installation is performed using a user-modifiable response file, which enables you to easily duplicate the installation on many computer systems.

Table 5-1. Variables Property and Description

Property	Description
USER_INSTALL_DIR	Install directory for smarts-ui.
CLIENT_ID	Client ID. **Note** Use the created remote access token for Auth App for VIDM Authentication. Get the values of client ID, shared secret and VIDM host name from VIDM authentication server.
SECRET	Shared Secret.
VIDM_HOST_NAME	VIDM Host Name.
AUTH_PORT	Auth Application Port. **Note** Port where Auth application will start.
CAPI_IP_ADDRESS	cAPI IP Address. **Note** Enter the cAPI address in the format <IP:PORT> Example: 127.0.0.1:10000.
SSL_CONF_DIR	Enter the ssl.conf location folder. For example, /etc/httpd/conf.d
KPI_REST_API_URL	KPI REST API URL. **Note** Enter the KPI REST API URL in the format <IP-ADDRESS:PORT>. For example, 127.0.0.1:8083.

Prerequisites

Create a configuration file for the installer to execute the installation. To create configuration file:

1 Copy the sample configuration file from the distribution (smartsui-installer.properties) to a directory on the server where you are installing smarts-ui.

2 Use any editor (vi/vim) to modify this file.

3 Define each of the properties in this file, according to the Table - Variables Property and Description. Save the changes to the file.

Procedure

1 Log in to the server as root.

2 Type `bash smartsui-install.bin -f <response file location> -i silent`, press **Enter**.

Note Any user interaction is not required for this installer. Once it completes, a message displays indicating that installation is completed, and you are returned to the shell prompt. If the installer is unable to complete the installation, an error message is saved in the [Product directory]/smarts-ui_logs.

What to do next

After successful Smart-UI installation, follow the steps provided in Export VIDM Certficate section to export and import VIDM certificates.

Performing Uninstallation

6

This chapter describes the Uninstallation procedure of the components Eventstore, cAPI, Smarts-UI and DCF in different modes like Console Mode, GUI Mode and Silent mode. Following topics are included here:

- Uninstallation of Eventstore in Console Mode, GUI Mode and Silent Mode.
- Uninstallation of cAPI in Console Mode, GUI Mode and Silent Mode.
- Uninstallation of Smarts-UI in Console Mode, GUI Mode and Silent Mode..
- Uninstallation of DCF in Console Mode, GUI Mode and Silent Mode.

Table 6-1. Uninstallation of the Components

Component Name	Uninstallation Method	Uninstallation Procedure
EventStore	Console Mode	1 Login to server as root. 2 Execute `<USER_INSTALL_DIR>/uninstaller/eventstore/eventstore_uninstaller -i console` Here USER_INSTALL_DIR denotes the location where Eventstore is installed. 3 Installer displays information about uninstaller, press **Enter** to continue. 4 Uninstaller exits after uninstalling all the installed files.
	GUI Mode	1 Login to server as root. 2 Execute `<USER_INSTALL_DIR>/uninstaller/eventstore/eventstore_uninstaller -i gui` Here USER_INSTALL_DIR denotes the location where eventstore is installed. 3 Installer displays information about uninstaller, click **Uninstall** to continue. 4 Click **Done** to exit the uninstaller.
	Silent Mode	1 Login to server as root. 2 Type `bash <USER_INSTALL_DIR>/uninstaller/eventstore/eventstore_uninstaller -i silent` Where <USER_INSTALL_DIR> is the place where eventstore is installed.

Table 6-1. Uninstallation of the Components (Continued)

Component Name	Uninstallation Method	Uninstallation Procedure
cAPI	Console Mode	1 Login to server as root. 2 Execute `<USER_INSTALL_DIR>/uninstaller/cAPI/cAPI_uninstaller -i console` Here USER_INSTALL_DIR denotes the location where cAPI is installed. 3 Installer displays information about uninstaller, press **Enter** to continue. 4 Installer exits after uninstallation of all the installed files.
	GUI Mode	1 Login to server as root. 2 Execute `<USER_INSTALL_DIR>/uninstaller/cAPI/cAPI_uninstaller -i gui` Here USER_INSTALL_DIR denotes the location where cAPI is installed. 3 Installer displays information about uninstaller, click **Uninstall** to continue. 4 Click **Done** to exit the uninstaller.
	Silent Mode	1 Login to server as root. 2 Type `bash <USER_INSTALL_DIR>/uninstaller/cAPI/cAPI_uninstaller -i silent` Where <USER_INSTALL_DIR> is the place where cAPI is installed.
Smarts-UI	Console Mode	1 Login to server as rot. 2 Execute `<USER_INSTALL_DIR>/uninstaller/smarts-ui/smarts-ui_uninstaller -i console` Here USER_INSTALL_DIR denotes the location where smarts-ui is installed. 3 Installer displays information about uninstaller, press **Enter** to continue. 4 Uninstaller exits after uninstalling all the installed files.
	GUI Mode	1 Login to server as root. 2 Execute `<USER_INSTALL_DIR>/uninstaller/smarts-ui/ smarts-ui _uninstaller -i gui` Here USER_INSTALL_DIR denotes the location where smarts-ui is installed. 3 Installer displays information about uninstaller, click **Uninstall** to continue. 4 Click **Done** to exit the uninstaller.
	Silent Mode	1 Login to server as root. 2 Type bash `<USER_INSTALL_DIR>/uninstaller/smarts-ui/smarts-ui_uninstaller -i silent` Where <USER_INSTALL_DIR> is the place where smarts-ui is installed.
DCF	Console Mode	1 Login to server as root. 2 Change directory to the DCF uninstall directory within DCF location: `cd <DCF_INSTALL_DIRECTORY>/Uninstaller` 3 Execute `./uninstall -i console` Logs are available at <DCF_INSTALL_DIRECTORY>/DCF_Logs.

Table 6-1. Uninstallation of the Components (Continued)

Component Name	Uninstallation Method	Uninstallation Procedure
	GUI Mode	1 Login to server as root. 2 Change directory to the DCF uninstall directory within DCF location: `cd <DCF_INSTALL_DIRECTORY>/Uninstaller` 3 Execute `./uninstall -i gui` 4 The uninstall DCF window appears, click **Uninstall** to continue. 5 The DCF uninstallation proceeds and uninstall complete window appears, click **Done** to exit. Logs are available at <DCF_INSTALL_DIRECTORY>/DCF_Logs.
	Silent Mode	1 Login to server as root. 2 Change directory to the DCF uninstall directory within DCF location: `cd <DCF_INSTALL_DIRECTORY>/Uninstaller` 3 Execute `./uninstall –i silent` Logs are available at <DCF_INSTALL_DIRECTORY>/DCF_Logs.

Note 1. Post uninstallation browse for /tmp directory and perform cleanup for the DCF collector related files.

Example: [root@wp-qa-090 tmp]# rm -rf velocloud-sdwan-collect-1.1/

Note 2. Post uninstallation verify if /tmp/sqlite.db is deleted. If not, delete the file.

Configuration and Authentication of Components

7

This chapter includes the following topics:

- Elasticsearch Authentication
- Enabling HTTPS in Elastic Search
- Redis Cluster Authentication
- Kafka SASL_PLAIN Authentication Configuration
- Kafka SASL_SSL Authentication Configuration
- cAPI-vIDM Configuration and Authentication
- VIDM Authentication with Notification GUI
- Create Remote Access Token for SpringBoot App for VIDM Authentication
- Export VIDM Certficate
- vROps Integration
- Enabling HTTPS in SAM

Elasticsearch Authentication

Authentication to ElasticSearch using the custom readonlyrest plugin.

To add the user follow the below steps:

Prerequisites

Download Readonlyrest Plugin, to download:

1 Go to https://readonlyrest.com/download

2 Select Product **Elasticsearch plugin (Free).**

3 Elastic Stack Version **6.4.2**

4 Send to email **email-id**.

5 Click **Get It Now**

6 Download link is sent to the mentioned email.

Installing readonlyrest plugin:

`/path to elastic search/bin/elasticsearch-plugin install`

`file:///path to readonlyrest-<version>.zip`

Example: `/usr/share/elasticsearch/bin/elasticsearch-plugin install file:///root/readonlyrest-1.16.28_es6.4.2..zip`

Procedure

1 Change directory to /etc/elasticsearch.

2 Edit **readonlyrest.yml**

3 Add the following in the file:

- name: **<Description for the User>**

auth_key_unix: **<Username>:<Hashed_Password>**

4 Restart **Elasticsearch**.

Sample User (Test/Test):

```
readonlyrest:
  access_control_rules:
  - name: Accept GET,POST requests from user
     Auth_key_unix: Test:
$6$rounds=65635$koKSfnyc$4iZfsoA9mxZYcRMSXUylDa2T/mPWnh/WWNqI7lM.
2hdXCIx5cVJY0Ni5NrBUXPc5F8xSVYGvs7ORVzAoyJeXq/
```

For Hashing of password:

`./encryptpassword.py <password>`

Creating encryptpassword.py file:

1 Go to https://github.com/beshu-tech/readonlyrest-docs/blob/master/elasticsearch.md#rules

2 Copy and write the code to file using the command:

```
vi encryptpassword.py
```

Paste the code and save the file using :**wq**.

3 Change the permission on the file **encryptpassword.py**

```
chmod 755 encryptpassword.py
```

4 Execute **encryptpassword.py**.

```
./encryptpassword.py <password>
```

Note Authentication must be enabled in each elastic search instance in the cluster.

Enabling HTTPS in Elastic Search

Learn how to enable HTTPS in Elastic Search.

Procedure

1 Create Elastic Search Keystore file using below command:

a
```
cd /etc/elasticsearch
```

b
```
<JRE_HOME>/bin/keytool -genkeypair -keystore keystore.jks -dname "CN=<FQDN>, OU=<Org Unit>,
O=<Org Name>, L=<City>, ST=<State>, C=<Country>" -keypass readonlyrest -storepass readonlyrest
-keyalg RSA -alias <alias name> -storetype PKCS12 -ext SAN=dns:<FQDN>,ip:<IP Address>
```

2 To enable ReadonlyREST's SSL stack, open **elasticsearch.yml** and add the below line:

```
http.type: ssl_netty4
```

3 In **readonlyrest.yml** add the following settings:

```
ssl:
keystore_file: "keystore.jks"
keystore_pass: readonlyrest
key_pass: readonlyrest
```

The keystore should be stored in the same directory as **elasticsearch.yml** and **readonlyrest.yml**.

4 Restart Elastic Search.

5 Repeat steps 1-4 for each instance of Elastic Search in the Cluster.

6 Export certificate from the keystore for each Elastic Search instance using below command:

a
```
cd /etc/elasticsearch
```

b
```
<JRE_HOME>/bin/keytool -export -keystore /etc/elasticsearch/keystore.jks -storepass
readonlyrest -alias <alias name> -rfc > /root/esdb.crt
```

7 Create `/opt/ssl` directory in the installation server.

8 Copy esdb.crt file from each Elastic Search instance to installation server under /opt/ssl directory.

Note The `/opt/ssl/esdb.crt` file in the installation server must contain consolidated certificates of all Elastic Search instances in the cluster.

Redis Cluster Authentication

Redis Authentication is enabled for Eventstore mainly to make it secure and to reduce the vulnerability. The topic consists of:

- Post Installation of Redis Enabling the Authentication.
- Create Redis Cluster without replication and with authentication.
- Adding slave to master.

Procedure

1 Post Installation of Redis type the below commands to enable the Authentication:

```
vi /path/to/redis.conf
replace 'requirepass <password>' with your password
replace 'masterauth <password>' with your password
```

Note Perform above config changes in all Redis instances and restart all Redis instances.

2 Create Redis cluster without replication with authentication.

Example: For a 3 node cluster with 3 masters, below is the command:

```
./redis-cli --cluster create <redis-server-ip-1>:<port> <redis-server-ip-2>:<port> <redis-server-ip-3>:<port> -a <password>
```

3 Add the slave to master, below is the command:

```
./ redis-cli --cluster add-node <redis-slave> <redis-master> --cluster-slave -a <password>
```

Note Execute above command to associate slave node with each master node.

Kafka SASL_PLAIN Authentication Configuration

This section describes the configuration of Kafka SASL_PLAIN authentication.

Procedure

1 Add/Update the below files in /KAKA_HOME/config directory.

a **server.properties**

```
security.inter.broker.protocol=SASL_PLAINTEXT
sasl.mechanism.inter.broker.protocol=PLAIN
sasl.enabled.mechanisms=PLAIN
authorizer.class.name=kafka.security.auth.SimpleAclAuthorizer
```

```
allow.everyone.if.no.acl.found=true
auto.create.topics.enable=true
listeners=SASL_PLAINTEXT://<IP Address>:9092
advertised.listeners=SASL_PLAINTEXT://<IP Address>:9092
```

b **zookeeper.properties**

```
authProvider.1=org.apache.zookeeper.server.auth.SASLAuthenticationProvider
requireClientAuthScheme=sasl
jaasLoginRenew=3600000
```

c **consumer.properties**

```
security.protocol=SASL_PLAINTEXT
sasl.mechanism=PLAIN
```

d **zookeeper_jaas.conf**

```
Server {
org.apache.zookeeper.server.auth.DigestLoginModule required
   user_super="zookeeper"
   user_admin="admin-secret";
};
```

e **kafka_server_jaas.conf**

```
KafkaServer {
org.apache.kafka.common.security.plain.PlainLoginModule required
username="admin"
password="admin-secret"
user_admin="admin-secret";
};
Client {
org.apache.zookeeper.server.auth.DigestLoginModule required
username="admin"
password="admin-secret";
};
```

2 Add the zookeeper_jaas.conf file to the environment variable KAFKA_OPTS before starting zookeeper.

```
$ export KAFKA_OPTS="-
Djava.security.auth.login.config=/KAFKA_HOME/config/zookeeper_jaas.conf"
$ bin/zookeeper-server-start.sh -daemon config/zookeeper.properties
```

3 Add the kafka_server_jaas.conf file to the environment variable KAFKA_OPTS before starting kafka server.

```
$ export KAFKA_OPTS="-
Djava.security.auth.login.config=/KAFKA_HOME/config/kafka_server_jaas.conf"
$ bin/kafka-server-start.sh -daemon config/server.properties
```

4 Configuring the producer.

producer.properties

```
security.protocol=SASL_PLAINTEXT
sasl.mechanism=PLAIN
bootstrap.servers=localhost:9092
compression.type=none
```

5 kafka_client_jaas.conf.

Note Console operations [for testing purpose only].

```
KafkaClient {
org.apache.kafka.common.security.plain.PlainLoginModule required
username="admin"
password="admin-secret";
};
Client {
  org.apache.zookeeper.server.auth.DigestLoginModule required
  username="admin"
  password="admin-secret";
};
$ export KAFKA_OPTS="-
Djava.security.auth.login.config=/KAFKA_HOME/config/kafka_client_jaas.conf"
$ ./bin/kafka-console-consumer.sh --
topic test-topic --from-beginning --
consumer.config=config/consumer.properties --bootstrap-server=localhost:9092
$ export KAFKA_OPTS="-
Djava.security.auth.login.config=/KAFKA_HOME/config/kafka_client_jaas.conf"
$ ./bin/kafka-console-producer.sh --broker-list localhost:9092 --topic test-topic
--producer.config=config/producer.properties
```

Kafka SASL_SSL Authentication Configuration

This section describes the configuration of Kafka SASL_SSL authentication.

Procedure

1 Add/Update the below files in /KAKA_HOME/config directory.

a **server.properties**

```
listeners=SASL_SSL://<ip-address>:9092
advertised.listeners=SASL_SSL://<ip-address>:9092

sasl.enabled.mechanisms=PLAIN
sasl.mechanism.inter.broker.protocol=PLAIN
security.inter.broker.protocol=SASL_PLAINTEXT
ssl.endpoint.identification.algorithm=HTTPS

authorizer.class.name=kafka.security.auth.SimpleAclAuthorizer

allow.everyone.if.no.acl.found=true

auto.create.topics.enable=false

ssl.keystore.location=/KAFKA_HOME/config/server.keystore.jks
ssl.keystore.password=<password>
ssl.key.password=<password>
ssl.truststore.location=/KAFKA_HOME/config/server.truststore.jks
ssl.truststore.password=<password>

ssl.client.auth=required
ssl.enabled.protocols=TLSv1.2,TLSv1.1,TLSv1
ssl.keystore.type=JKS
ssl.truststore.type=JKS
ssl.secure.random.implementation=SHA1PRNG
```

b **zookeeper.properties**

```
authProvider.1=org.apache.zookeeper.server.auth.SASLAuthenticationProvider
requireClientAuthScheme=sasl
```

c **consumer.properties**

```
sasl.mechanism=PLAIN
security.protocol=SASL_SSL
sasl.jaas.config=org.apache.kafka.common.security.plain.PlainLoginModule required \
   username="admin" \
   password="admin-secret";

ssl.truststore.location=/KAFKA_HOME/config/client.truststore.jks
ssl.truststore.password=<password>
```

d Generating SSL certificates.

Create the certificates in /KAFKA_HOME/config

```
keytool -keystore server.keystore.jks -alias <alias> -validity 365 -genkey -keyalg RSA -ext
SAN=DNS:<hostname>,DNS:<fqdn>,DNS:localhost,IP:<IP-ADDRESS>,IP:127.0.0.1

openssl req -new -x509 -keyout ca-key -out ca-cert -days 365 -subj '/CN=<fqdn>'   -extensions
san   -config <(echo '[req]'; echo 'distinguished_name=req'; echo '[san]'; echo
'subjectAltName = DNS:localhost, IP:127.0.0.1, DNS:<hostname>, IP:<ip-address>')

keytool -keystore server.truststore.jks -alias CARoot -import -file ca-cert

keytool -keystore client.truststore.jks -alias CARoot -import -file ca-cert

keytool -keystore server.keystore.jks -alias <fqdn> -certreq -file cert-file -ext
SAN=DNS:<hostname>,DNS:localhost,IP:<ip-address >,IP:127.0.0.1

openssl x509 -req  -extfile <(printf "subjectAltName = DNS:localhost, IP:127.0.0.1,
DNS:<fqdn>, IP:<ip-address>") -CA ca-cert -CAkey ca-key -in cert-file -out cert-signed -days
365 -CAcreateserial -passin pass:<password>

keytool -keystore server.keystore.jks -alias CARoot -import -file ca-cert

keytool -keystore server.keystore.jks -alias <alias> -import -file cert-signed.
```

e **zookeeper_jaas.conf**

```
Server {
        org.apache.zookeeper.server.auth.DigestLoginModule required
        user_super="admin-secret"
        user_kafka="kafka-secret";
 };
```

f **kafka_server_jaas.conf**

```
KafkaServer {
    org.apache.kafka.common.security.plain.PlainLoginModule required
    username="admin"
    password="admin-secret"
    user_admin="admin-secret";
 };

Client {
    org.apache.zookeeper.server.auth.DigestLoginModule required
    username="kafka"
    password="kafka-secret";
 };
```

2 Add the **zookeeper_jaas.conf** file to the environment variable **KAFKA_OPTS** before starting zookeeper.

```
$ export KAFKA_OPTS="-Djava.security.auth.login.config=/KAFKA_HOME/config/zookeeper_jaas.conf"
$ bin/zookeeper-server-start.sh -daemon config/zookeeper.properties
```

3 Add the **kafka_server_jaas.conf** file to the environment variable **KAFKA_OPTS** before starting kafka server.

```
$ export KAFKA_OPTS="-Djava.security.auth.login.config=/KAFKA_HOME/config/kafka_server_jaas.conf"
bin/kafka-server-start.sh -daemon config/server.properties
```

4 Configuring the producer

a **producer.properties**

```
sasl.mechanism=PLAIN
security.protocol=SASL_SSL
sasl.jaas.config=org.apache.kafka.common.security.plain.PlainLoginModule required \
   username="admin" \
   password="admin-secret";
ssl.truststore.location=/KAFKA_HOME/config/client.truststore.jks
ssl.truststore.password=<password>
```

5 **kafka_client_jaas.conf**

Note Console operations [for testing purpose only]

```
KafkaClient {
  org.apache.kafka.common.security.plain.PlainLoginModule required
  username="admin"
  password="admin-secret";
};
Client {
org.apache.zookeeper.server.auth.DigestLoginModule required
  username="kafka"
  password="kafka-secret";
};
$ export KAFKA_OPTS="-Djava.security.auth.login.config=/KAFKA_HOME/config/kafka_client_jaas.conf"
$ ./bin/kafka-console-consumer.sh --bootstrap-server <fqdn/hostname/ip-address>:9092 --topic
test_topic --from-beginning --consumer.config config/consumer.properties

$ export KAFKA_OPTS="-Djava.security.auth.login.config=/KAFKA_HOME/config/kafka_client_jaas.conf"
$ ./bin/kafka-console-producer.sh  --broker-list <fqdn/hostname/ip-address>:9092 --topic
test_topic  --producer.config config/producer.properties
```

cAPI-vIDM Configuration and Authentication

This is a onetime configuration of an Oauth2 client that supports password grant on vIDM. To configure Client on vIDM

Procedure

1 Use below API to create a password grant Oauth2 client.

`Rest URL: https://<VIDM FQDN>/SAAS/jersey/manager/api/oauth2clients`

`Method: POST`

```
Headers:
Accept: application/vnd.vmware.horizon.manager.oauth2client+json
Content-Type: application/vnd.vmware.horizon.manager.oauth2client+json
Authorization: "Basic " + base64Encode(Admin User + ":" + Admin Password)
Eg: Basic YWRtaW46Vk13YXJlMSE=
Payload:
{
"clientId":"capi_client",
"secret":"YJJ4afCPWH5DZQH85XOu423qIBRcirRQctsDRPiaOlOWWwuN",
"scope":"email profile user admin",
"authGrantTypes":"password",
"tokenType":"Bearer",
"tokenLength":23,
"accessTokenTTL":360,
"refreshTokenTTL":43200,
"rememberAs":null,
"resourceUuid":"00000000-0000-0000-0000-000000000000",
"displayUserGrant":false,
"internalSystemClient":false,
"activationToken":null,
"strData":"{\"credentialCheckType\":\"ActiveDirectoryPassword\"}"
}
Response:
Status: 201
Body:
{
"clientId": "capi_client",
"secret": "YJJ4afCPWH5DZQH85XOu423qIBRcirRQctsDRPiaOlOWWwuN",
"scope": "email profile user admin",
"authGrantTypes": "password",
"redirectUri": null,
"tokenType": "Bearer",
```

```
"tokenLength": 32,
"accessTokenTTL": 360,
"refreshTokenTTL": 43200,
"refreshTokenIdleTTL": null,
"rememberAs": null,
"resourceUuid": "00000000-0000-0000-0000-000000000000",
"displayUserGrant": false,
"internalSystemClient": false,
"activationToken": null,
"strData": "{\"credentialCheckType\":\"ActiveDirectoryPassword\"}",
"inheritanceAllowed": false,
"returnFailureResponse": false,
"_links": {
"self": {
"href": "/SAAS/jersey/manager/api/oauth2clients/example_browser_cli_clientid"
}
}
}
```


2 Replace `<VIDM_Authorization_Header>` with the below string in the **envoy.yaml** file:

```
Authorization is constructed of "Basic " + base64Encode(clientId + ":" + secret)
= base64Encode(OAuth2Client_aaAdminClient:OAuth2Client_aaAdminClientSecret)
```

VIDM Authentication with Notification GUI

This section describes the Configuration of VIDM Authentication with Notification GUI .

Procedure

1 Configure VIDM with a Remote app Access.

2 During installation of the GUI/Auth service, it prompts for Client ID, Shared Secret and VIDM hostname based on the remote access token created.

Note In any case server is not registered with DNS make entries on /etc/hosts file for all the needed servers and on clients.

Export VIDM certificate and import to java certs on the server where Smarts-UI is installed.

Create Remote Access Token for SpringBoot App for VIDM Authentication

This section describes how to create remote access token for SpringBoot App for VIDM Authentication.

Procedure

1 Launch **VIDM admin console** > **Catalog** >**Settings** > **Remote App Access** > click **Create Client**.

2 Provide a client id in the form of **“auth.gui.notification.log.view.<server ip identifier>**.

3 Click **Generate Shared Secret.**

4 Provide re-direct URI as the **<http://<Smart UI Server FQDN>/login/vmware>**.

5 Select check box **OpenID**.

If not registered with DNS, add the GUI server ip to the vidm /etc/hosts and vidm and GUI on your client server where browser will be launched.

Export VIDM Certficate

Procedure to export VIDM certificate using Openssl and import to Smarts-UI server

Procedure

1 Login to VIDM Server and execute following command to export certificate:

a
```
openssl s_client –connect <VIDM_FQDN>:<VIDM Port> </dev/null 2>/dev/null|
openssl x509 –outform PEM ><certfilename>.pem
```

b Copy <certfilename>.pem to Smart-UI Server.

2 Login to Smarts-UI server and execute below command to import VIDM certificate to java certs.

a
```
<JAVA_HOME>/jre/bin/keytool –importcert –file <certfilename>.pem – keystore
<JAVA_HOME>/jre/lib/security/cacerts –alias "<alias_name>"
```

3 Restart the **auth service**.

```
service auth restart
```

vROps Integration

Perform SMARTS Management pack installation from the vROps Administration page.

Procedure

1 After installation of the Management pack the files are located at location

/usr/lib/vmware-vcops/user/plugins/inbound/<SmartAssuranceAdapter>/conf/dashboards/:

- Network-Adapters.json

- network-adapter-perf-param.json
- top-n-adapter-util.json
- Network-Device-Details.json
- **notifications.html**
- top-n-cpu-util.json
- dashboard.json
- top-n-adapter-errors.json
- top-n-mem-util.json

2 vROps admin need to edit the notifications.html to point to the Notification log view GUI server.

3 Import the file **notifications.html** using the below command.

```
#cd /usr/lib/vmware-vcops/tools/opscli
```

```
#$VMWARE_PYTHON_BIN ops-cli.py file import txtwidget /usr/lib/vmware-
vcops/user/plugins/inbound/SmartAssurance/conf/dashboards/notifications.html
```

Note If the notifications.html file was already imported, remove it before adding again.

Launch the vROps GUI, click **Dashboards** and click **Notifications Log View** Launch **Dashboard** on the left hand side. Now click **Launch Notification Log View** button on the ride hand side to launch Smarts-UI webpage on a separate tab.

Enabling HTTPS in SAM

This section describes how to generate and set up SSL in SAM.

Linux: Generating the SAM Tomcat server keystore file and certificate

Learn how to create the Tomcat server keystore file and certificate.

Procedure

- Issue the command to generate the keystore file.

  For example: run this command for the SAM host if it has a Fully Qualified Domain Name (FQDN):

```
<<Base_Dir>>/SAM/smarts/jre/bin/keytool -genkey -alias
tomcat -keyalg RSA
To specify a different location or filename, add the -keystore parameter
followed by the complete pathname to the keystore file. For example,
<<Base_Dir>>/SAM/smarts/jre/bin/keytool -genkey -alias
tomcat -keyalg RSA
-keystore <<Base_Dir>>/SAM/smarts/.keystore -ext SAN=ip:<y.y.y.y>
```

  - Enter **Changeit** for keystore password.
  - When asked for your first and last name, enter the fully qualified name of the machine.

    For example: `itops-dev-204.lss.emc.com.`
  - Answer the other questions and type **yes** when asked for confirmation.

This creates a keystore file inside `<<Base_Dir>>/SAM/smarts folder` with name **.keystore.**

What to do next

Export the cert.

```
<<Base_Dir>>/SAM/smarts/jre/bin/keytool -export -keystore
<<Base_Dir>>/SAM/smarts/.keystore -storepass changeit -alias tomcat -rfc
> /root/sam.crt
```

Note Copy `/root/sam.crt` to `/opt/ssl` in Eventstore server machine.

Linux: Editing the SAM server.xml file and runcmd_env.sh

Procedure

1. Add SM_TOMCAT_SERVER=https://<smarts-tomcat-server-host>:8443 in <<Base_Dir>>/SAM/smart/local/conf/runcmd_env.sh file
2. Edit the server.xml file so that SAM Tomcat server can understand which secure port and protocol to use.
3. Add following lines in `<<Base_Dir>>/SAM/smarts/tomcat/conf/server.xml`

```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
keystoreFile="<<Base_Dir>>/SAM/smarts/.keystore" keystorePass="changeit"
clientAuth="false" sslEnabledProtocols="TLSv1.2" />

<Connector protocol="org.apache.coyote.http11.Http11Protocol" port="8443"
maxThreads="150" scheme="https" secure="true"
```

```
keystoreFile="<<Base_Dir>>/SAM/smarts/.keystore" keystorePass="changeit"
clientAuth="false" sslProtocol="TLS" />

<Connector protocol="org.apache.coyote.http11.Http11NioProtocol" port="8443"
maxThreads="150" scheme="https" secure="true"
keystoreFile="<<Base_Dir>>/SAM/smarts/.keystore" keystorePass="changeit"
clientAuth="false" sslProtocol="TLS" />
```

What to do next

Restart Tomcat and Presentation SAM service.

Troubleshooting

8

This article helps to find the solutions to the issues you may observe in Smart Assurance UI.

This chapter includes the following topics:

- When Live Notifications are not Appearing to UI
- When Service Unavailable Error Appears
- When Cluster is Down
- When Connections cannot be Established with Smarts Tomcat Service
- When Connections cannot be Established with Smarts Presentation service
- When "Result window is too large, from + size must be less than or equal to: [10000]" Message Appears
- When Request Timeout Message Appears
- When Controller Service Fails to Start in DCF

When Live Notifications are not Appearing to UI

If Live Notification are not appearing to UI, perform these steps:

Procedure

1. Check the Kafka Broker Cluster status.

   If Kafka Cluster is down, then start all the kafka broker in the cluster.

2. Check Smarts Notifs Events Collector Manager is running using below command from `<DCF Install Dir>/bin`.

   ```
   ./manage-modules.sh service status event-processing-manager <instance name>
   ```

   If not running, start the service using below command from `<DCF Install Dir>/bin`

   ```
   ./manage-modules.sh service start event-processing-manager < instance name>
   ```

3. Check EventStore service is running using below command.

   ```
   service eventstore status.
   ```

If not running, start the service using below command:

`service eventstore start`.

When Service Unavailable Error Appears

Follow these troubleshooting steps if service unavailable error appears in UI:

Procedure

1. Verify Eventstore, cAPI and Auth services are running.
2. Verify connection to KPI is working.
3. Verify Elastic Search Cluster is up & running.

When Cluster is Down

If the Cluster Down error appears in UI, perform these steps:

Procedure

1. Verify Redis Cache Cluster is up and running.
2. Ensure all 3 Master services are running.

When Connections cannot be Established with Smarts Tomcat Service

Perform these steps to troubleshoot the issue connections cannot be established with Smarts Tomcat Service:

Procedure

1. Login to the machine where Smarts Presentation SAM is installed and check the status of tomcat service.
2. Verify if the Smarts Tomcat Service is available and running.

   Ensure the service is listening on port 8080(HTTP) or 8443(HTTPS).
3. If the Smarts Tomcat Service is running and listening on port 8080(HTTP) or 8443(HTTPS), execute below command on the machine where EPS(eventstore) is installed. Ensure the command executes successfully.

   a `For HTTP, curl http://<SAM IP:8080>/smarts-edaa/msa/INCHARGE-SA-PRES/instances/ICS_User::ICS-User-admin/relationships/MemberOf?alt=json`.

b For HTTPS, `curl --cacert <SAM Cert file> https://<SAM IP:8443>/smarts-edaa/msa/INCHARGE-SA-PRES/instances/ICS_User::ICS-User-admin/relationships/MemberOf?alt=json`.

Note Make sure latest version of curl is installed in the machine.

When Connections cannot be Established with Smarts Presentation service

Perform these steps when Connections cannot be established with the Smarts Presentation service issue observed.

Procedure

1. Login to the machine where Smarts Presentation SAM is installed and check the status of presentation SAM service.
2. Verify if the Smarts Presentation service is available and running.
3. Smarts Presentation service is available and running, ensure no firewalls are running between the machine where presentation SAM and Eventstore is installed.
4. Ensure that you have given correct Smarts Presentation SAM and port details during installation if no firewalls are running between the machine where presentation SAM and Eventstore is installed.

When "Result window is too large, from + size must be less than or equal to: [10000]" Message Appears

The message "Result window is too large, from + size must be less than or equal to: [10000]" is displayed in UI when the user tries to access Notifications greater than 10,000.

Perform these troubleshooting steps for this error:

Procedure

1. Increase the limit by setting the property "indexMaxResultWindow" to a value greater than 10,000 using eps refresh api.

   It can impact the read query performance and can lead to high memory consumption.
2. Use more refined filters to reduce the response list size.

When Request Timeout Message Appears

If "Request Timeout has happened. Please increase the timeout period” or “Gateway Timeout" message appears when you take any actions on Notifications, perform these troubleshooting steps:

Procedure

1. Use "/eps/refresh" api to increase default sam request timeout. Sample payload for changing the time.

   ```
   {
   "doc": {
   "sam-requestTimeout": "300s"
   }
   }
   ```

2. Restart Eventstore service.
3. Configure higher timeout period in cAPI configuration(<<cAPI_Homedir>>/cAPI/config/envoy.yml) file as:

   ```
   - match: { prefix: "/eps" }
   route: { cluster: eps_cluster, timeout: 60s }
   ```

4. Restart cAPI service.

When Controller Service Fails to Start in DCF

This section describe how to troubleshoot if Controller Service fails to start in DCF.

Procedure

- Check the permission of the file `/sys/fs/cgroup/systemd/system.slice/apg-services.service/tasks`

  If it is not apg:apg, execute the following command:

  ```
  chown apg:apg /sys/fs/cgroup/systemd/system.slice/apg-services.service/tasks
  ```