



Operations Bridge Analytics

Software Version: 3.01

Hardening Guide

Document Release Date: April 2017

Software Release Date: April 2017



Hewlett Packard
Enterprise

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© 2016 - 2017 Hewlett Packard Enterprise Development LP

Trademark Notices

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

AMD, the AMD Arrow symbol and ATI are trademarks of Advanced Micro Devices, Inc.

Citrix® and XenDesktop® are registered trademarks of Citrix Systems, Inc. and/or one more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

Google™ and Google Maps™ are trademarks of Google Inc.

Intel®, Itanium®, Pentium®, and Intel® Xeon® are trademarks of Intel Corporation in the U.S. and other countries.

iPad® and iPhone® are trademarks of Apple Inc.

Java is a registered trademark of Oracle and/or its affiliates.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft®, Windows®, Lync®, Windows NT®, Windows® XP, Windows Vista® and Windows Server® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

NVIDIA® is a trademark and/or registered trademark of NVIDIA Corporation in the U.S. and other countries.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

Red Hat® is a registered trademark of Red Hat, Inc. in the United States and other countries.

SAP® is the trademark or registered trademark of SAP SE in Germany and in several other countries.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

To check for recent updates or to verify that you are using the most recent edition of a document, go to: <https://softwaresupport.hpe.com/>.

This site requires that you register for an HPE Passport and to sign in. To register for an HPE Passport ID, click **Register** on the HPE Software Support site or click **Create an Account** on the HPE Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HPE sales representative for details.

Support

Visit the HPE Software Support site at: <https://softwaresupport.hpe.com/>.

Most of the support areas require that you register as an HPE Passport user and to sign in. Many also require a support contract. To register for an HPE Passport ID, click **Register** on the HPE Support site or click **Create an Account** on the HPE Passport login page.

To find more information about access levels, go to: <https://softwaresupport.hpe.com/web/softwaresupport/access-levels>.

HPE Software Solutions Now accesses the Solution and Integration Portal website. This site enables you to explore HPE product solutions to meet your business needs, includes a full list of integrations between HPE products, as well as a listing of ITIL processes. The URL for this website is <https://softwaresupport.hpe.com/km/KM01702731>.

Contents

Chapter 1: Introduction	5
Environment Variables Used in this Document	5
System Architecture	7
Chapter 2: Distributed Operations Bridge Analytics Security	
Hardening	8
Encrypting Operations Bridge Analytics	8
Other Security Considerations	8
Chapter 3: SSL for Operations Bridge Analytics Components	10
SSL for Servers and Collectors	10
Configuring SSL for the OBA Servers and Collectors	10
Configuring SSL Communication to the OBA Server and Collector with a Certificate Authority (CA) Signed Certificate	11
Configuring SSL Communication to the OBA Server and Collector with a Self-Signed Certificate	17
Editing the SSL Configuration for the OBA Server or Collector	22
Disabling the SSL Configuration for the OBA Server or Collector	24
Managing the Keystore and Truststore for the OBA Server and Collector	26
Two-Way SSL for Accessing ArcSight Logger	28
SSL for Communication Between Vertica and OBA	31
Enabling SSL Communications between the Operations Bridge Analytics Server and Vertica	31
Disabling SSL Communications between the Operations Bridge Analytics Server and Vertica	39
Enabling SSL Communications between the Operations Bridge Analytics Collector Host and Vertica	42
Disabling SSL Communications between the Operations Bridge Analytics Collector Host and Vertica	43
Adjusting Operations Bridge Analytics for RC4 Cipher Security Changes	44
SSL for the SMTP Server Used for OBA Alerts	45
Chapter 4: HTTP and HTTPS	46

Configuring the HTTP and HTTPS Port for the Operations Bridge Analytics Collector Host	46
Configuring the HTTP and HTTPS User Name and Password for the Operations Bridge Analytics Collector Host	47
Chapter 5: Single Sign On	48
Configuring and Enabling Single Sign-on to Access Operations Bridge Analytics	48
Disabling Single Sign-on to Access Operations Bridge Analytics	50
Chapter 6: LDAP Authentication	52
Configuring LDAP Authentication for Operations Bridge Analytics	52
Configuring SSL for LDAP Server Authentication	52
Chapter 7: PKI	54
Configuring User Authentication using Public Key Infrastructure (PKI) to Access Operations Bridge Analytics	54
Disabling User Authentication using Public (PKI) to Access Operations Bridge Analytics	57
Editing User Authentication using Public (PKI) to Access Operations Bridge Analytics	57
Chapter 8: Resetting User Passwords	59
Chapter 9: Changing the Port Used by the Operations Bridge Analytics Console	60
Chapter 10: Securing Data Among Tenants	61
Send documentation feedback	62

Chapter 1: Introduction

This guide contains information about how to configure Operations Bridge Analytics including the following major topics:

- Hardening
- Maintenance

Note: This manual includes examples that show script usage, command line usage, command line syntax, and file editing. If you copy and paste any examples from this manual, carefully review the results of your paste before running a command or saving a file.

Environment Variables Used in this Document

This document refers to the following environment variables and other useful directories when explaining installation and configuration instructions for the Operations Bridge Analytics Software, including the Operations Bridge Analytics Server and the Operations Bridge Analytics Collector host. The environment variables are set automatically for the opsa user who can use all Operations Bridge Analytics functionality and has access to data at the tenant level.

Table 1: Environment Variables

Variable Name	Path	Operations Bridge Analytics Server or Operations Bridge Analytics Collector Host
OPSA_HOME	/opt/HP/opsa	Operations Bridge Analytics Server and Collector hosts
JAVA_HOME	/opt/HP/opsa/jdk	Operations Bridge Analytics Server and Collector hosts

Table 2: Other Useful Directories

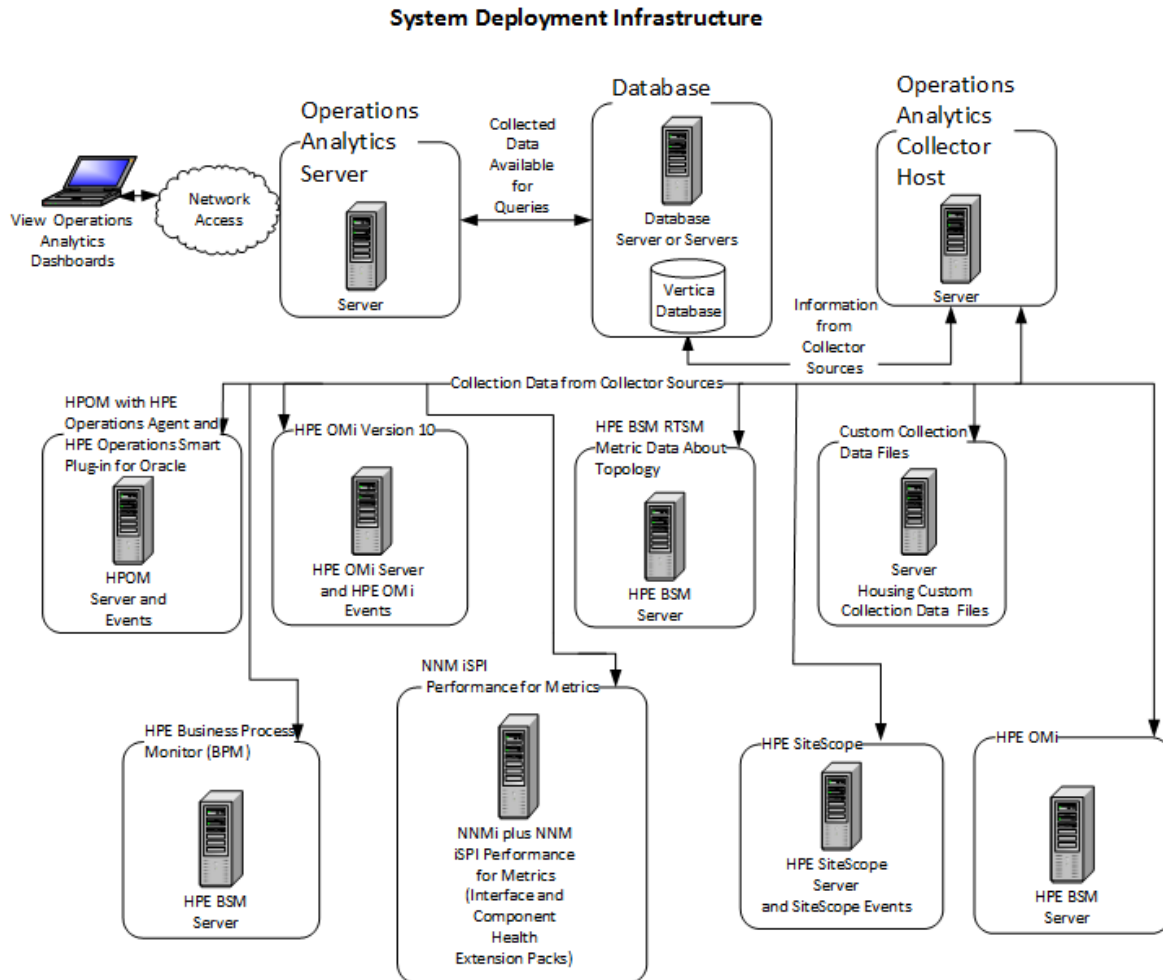
Folder Name	Path	Operations Bridge Analytics Server or Operations Bridge Analytics Collector Host
JBOSS Home Directory	/opt/HP/opsa/jboss	Operations Bridge Analytics Server
JDK Folder	/opt/HP/opsa/jdk	Operations Bridge Analytics Server and Collector hosts

Table 2: Other Useful Directories, continued

Folder Name	Path	Operations Bridge Analytics Server or Operations Bridge Analytics Collector Host
scripts Folder	/opt/HP/opsa/scripts	Operations Bridge Analytics Server and Collector hosts
conf Folder	/opt/HP/opsa/conf	Operations Bridge Analytics Server and Collector hosts
data Folder	/opt/HP/opsa/data	Operations Bridge Analytics Server and Collector hosts
log Folder	/opt/HP/opsa/log	Operations Bridge Analytics Server and Collector hosts
lib Folder	/opt/HP/opsa/lib	Operations Bridge Analytics Server and Collector hosts
bin Folder	/opt/HP/opsa/bin	Operations Bridge Analytics Server and Collector hosts
Vertica Database Installation Folder	/opt/vertica	Operations Bridge Analytics Server and Collector hosts have the Vertica client installed in this folder

System Architecture

Review the information shown in the following diagram to begin understanding the data sources used by Operations Bridge Analytics and how they are configured together to better plan your Operations Bridge Analytics installation.



Chapter 2: Distributed Operations Bridge Analytics Security Hardening

The following information is a summary of the security hardening recommendations for Operations Bridge Analytics.


Note: The hardening instructions shown in this section are optional. Complete the instructions in this section if you are interested in securing your Operations Bridge Analytics installation.

Encrypting Operations Bridge Analytics

Each Operations Bridge Analytics Server uses a separate encryption key to provide secure data for each Operations Bridge Analytics deployment.

Operations Bridge Analytics provides the `opsa-key-manager.sh` script. If you want to modify the encryption password and salt for an Operations Bridge Analytics installation, do the following from the Operations Bridge Analytics Server:

1. Run the `opsa-key-manager.sh` script as a user with super-admin credentials.
2. When prompted, follow the instructions shown by the `opsa-key-manager.sh` script.
3. After the `opsa-key-manager.sh` script completes, Operations Bridge Analytics has a new encryption key and salt.

See the `opsa-key-manager.sh` reference page (or the Linux man page), for more information. To view Operations Bridge Analytics reference pages, select  > **Reference Pages** in the Operations Bridge Analytics console,

Other Security Considerations

Below are some other security items to consider:

- If you have multiple tenants, make sure that you use different Operations Bridge Analytics Collector hosts for each tenant to ensure data separation for each tenant (which is an architectural

requirement).

- When selecting credentials to connect to the OMi database, it is recommended that you select a user with minimal credentials for reading the required information. Selecting a more powerful user could present a security vulnerability.

Chapter 3: SSL for Operations Bridge Analytics Components

This section provides information about securing the communication between OBA components. If you choose to configure SSL, it is recommended that you secure all OBA connections, and not just individual components.

This section includes:

- ["SSL for Servers and Collectors" below](#)
- ["Two-Way SSL for Accessing ArcSight Logger" on page 28](#)
- ["SSL for Communication Between Vertica and OBA" on page 31](#)
- ["SSL for the SMTP Server Used for OBA Alerts" on page 45](#)

SSL for Servers and Collectors

This section includes:

- ["Configuring SSL for the OBA Servers and Collectors" below](#)
- ["Editing the SSL Configuration for the OBA Server or Collector" on page 22](#)
- ["Disabling the SSL Configuration for the OBA Server or Collector" on page 24](#)
- ["Managing the Keystore and Truststore for the OBA Server and Collector" on page 26](#)

Configuring SSL for the OBA Servers and Collectors

One-way SSL provides secure communication between the client and the Operations Bridge Analytics Server and the Collector host. During an SSL session creation, the server sends a digital certificate (self-signed or CA signed) containing information about the server. This information, such as domain, organization, and location, helps the client verify the server's identity. SSL is disabled by default.

HPE recommends that customers enable SSL communication for those environments where security is a concern. SSL should be enabled for both the OBA server and the collectors.

The workflow is as follows:

1. If the collector is registered, unregister the collector from the server
2. Enable SSL communication to the server
3. Enable SSL communication to the collector
4. Reregister the collector using SSL

If you are using a certificate authority (CA) signed certificate, perform the workflow starting with ["Configuring SSL Communication to the OBA Server and Collector with a Certificate Authority \(CA\) Signed Certificate "](#) below. If your environment contains multiple servers, you must issue a new certificate for each server, not one certificate for all servers. On each server, import the certificate issued for the server and import the CA's root certificate to the trust store on each server.

If you are using a self-signed certificate, perform the workflow starting with ["Configuring SSL Communication to the OBA Server and Collector with a Self-Signed Certificate"](#) on page 17.

Configuring SSL Communication to the OBA Server and Collector with a Certificate Authority (CA) Signed Certificate

If you set up SSL connection for the OBA server(s), you must also set up SSL connection for the OBA collector(s). For environments with more than one server, you must issue a different certificate for each of your servers, and import the CA's root certificate into the truststore on each server. This must be repeated for each OBA server and each OBA collector.

1. **Unregister the collector.** If OBA is already configured with collections (the collector is already registered) you must unregister all collections either by using the OBA interface or the command line. Run the following command as the `opsa` user to unregister the collector from the OBA server:

```
/opt/HP/opsa/bin/opsa-collection-config.sh -unregister -collectorhost  
<collector IP address> -port 9443 -username <tenant admin username> -password  
<password for tenant admin username>
```

Run the following command to check that the collector was unregistered successfully:

```
/opt/HP/opsa/bin/opsa-collection-config.sh -list -allversions -collectorhosts -  
port 9443 -username <tenant admin username> -password <password for tenant  
admin username>
```

2. **Configure SSL communication to the OBA server.** Complete the following steps to enable

SSL communication to the OBA server using a CA signed certificate:

- a. Before enabling SSL to the Operations Bridge Analytics Server, complete this step on the Operations Bridge Analytics Server to create a user in JBoss **Management Realm**.

Do the following:

- i. Run the `$OPSA_HOME/jboss/bin/add-user.sh` script as the `opsa` user.
- ii. For the first question, answer **"a" - Management User (mgmt-users.properties)**, then follow the instructions.

Note: You will need to provide the JBoss management realm credentials when enabling SSL later in these instructions.

- iii. When queried about the group to which the user should belong, accept the default settings. When queried if the user will be used for one AS process to connect to another AS process, select No. If the script prompts you to add the JBOSS secret, you can safely ignore this. OBA does not use this secret.
- b. As the `opsa` user, change the directory to `/opt/HP/opsa` and run the `$OPSA_HOME/bin/opsa-server-manager.sh` script on the Operations Bridge Analytics Server. See the `opsa-server-manager.sh` reference page (or the Linux man page), for more information.

Note: This script must be run out of the `$OPSA_HOME` directory.

Make the following selections in the resulting flow of options:

- i. Select option **2: Configure SSL**.
 - ii. Select option **1: Generate self signed certificate for OPSA** to generate a selfsign key pair.
 - iii. If you have more than one server, select option **7: Change key alias to be used for SSL communication** to ensure the alias for all servers is different (this is required when importing into other products, like OMi).
 - iv. Select option **2: Generate certificate signing request** to generate a certificate request for a signed CA certificate. Choose the `opsa_server` alias and save the certificate to `/tmp/opsa_server_crf.csr`.
- c. After creating the request file, sign the Certificate Request on your CA. Download the certificate chain on based 64 encoded format (`p7b` extension) and copy the file to the Operations Bridge Analytics server in the `/tmp` folder.
 - d. Select option **3: Import CA signed certificate to OPSA keystore**. Specify the absolute path

- to the certificate.
- e. Download the root CA certificate from your CA and copy the file to the OBA server in the /tmp folder.
 - f. Select option **4: Import trusted certificate to OPSA truststore**. Enter the exact path to the root CA certificate that you downloaded.
 - g. Select option **8: Enable/Disable SSL**. You will need to enter the JBoss **Management Realm** user and password you created in the first step. The `opsa-server-manager.sh` script prompts you for the certificate alias to be used for SSL communication. Enter the `opsa_server` alias from the list of key aliases in the OPSA keystore.
 - h. Select the option **13: Go back to main menu**.
 - i. Select option **7: Exit**.
 - j. Restart all OBA processes by calling `sudo /opt/HP/opsa/bin/opsa restart`.

Note: Your configuration changes will not occur unless the server is restarted. If you receive an error, follow the instructions in the error messages.

3. **Configure SSL communication to the OBA collector.** Complete the following steps to enable SSL communication to the OBA collector using a CA signed certificate:
 - a. As the `opsa` user, change the directory to `/opt/HP/opsa` and run the `$OPSA_HOME/bin/opsa-collector-manager.sh` script on the Operations Bridge Analytics Collector host. See the `opsa-collector-manager.sh` reference page (or the Linux man page), for more information.

Note: This script must be run out of the `$OPSA_HOME` directory.

Make the following selections in the resulting flow of options:

- i. Select option **1: Configure SSL**.
 - ii. Select option **1: Generate a self signed certificate for OPSA**.
 - iii. If you have more than one collector, select option **7: Change key alias to be used for SSL communication** to ensure the alias for all collectors is different (this is required when importing into other products, like OMi).
 - iv. Select option **2: Generate a certificate signing request**. Choose the `opsa_server` alias. Save the certificate to `/tmp/opsa_collector_crf.csr`.
- b. After creating the request file, sign the Certificate Request on your CA. Download the certificate chain on based 64 encoded format (p7b extension). Copy this file to the Operations

Bridge Analytics server in the /tmp folder.

- c. Select option **3: Import CA signed certificate to OPSA keystore**. Specify the absolute path to the certificate.
- d. Download the root CA certificate from your CA and copy the file to the OBA server in the /tmp folder.
- e. Select option **4: Import trusted certificate to OPSA truststore**. Enter the exact path to the root CA certificate that you downloaded.
- f. Select option **8: Enable/Disable SSL**. You will need to enter the JBoss **Management Realm** user and password you created in the first step. The `opsa_collector_manager.sh` script prompts you for the certificate alias to be used for SSL communication. Enter the `opsa_server` alias from the list of key aliases in the OPSA keystore.
- g. Select option **13: Go back to main menu**.
- h. Select option **5: Exit**.
- i. Restart all OBA processes by calling `sudo /opt/HP/opsa/bin/opsa restart`.

Note: Your configuration changes will not occur unless the collector is restarted. If you receive an error, follow the instructions in the error messages.

4. Reregister the OBA collector.

- a. Run the following command as the "opsa" user on the OBA server to register the OBA collector with the SSL command:

```
/opt/HP/opsa/bin/opsa-collection-config.sh -register -collectorhost  
<collector IP address> -port 9443 -username <tenant admin username> -  
password <password for tenant admin username> -ssl
```

- b. Reregister all collections that you unregistered in step 1.
5. *Optional.* Select the **Import trusted certificate to OPSA server truststore** option to import trusted certificates (if any). For example, you can add HPE ArcSight Logger's server certificate to the Operations Bridge Analytics truststore file.

Note: You must complete this certificate import on both the Operations Bridge Analytics Server (for the rawlog query) and the Operations Bridge Analytics Collector host (for the structured log query). Follow these steps:

- a. Log on to the Logger console, then click **System Admin**.
- b. Select the **SSL Server Certificate** option under **security** on the left side of the screen.

- c. Click the View Certificate button at the bottom of the screen.
 - d. After the dialog box opens, copy the certificate text and save it to a file on both the Operations Bridge Analytics Collector host and on the Operations Bridge Analytics Server.
 - e. Complete this step on both the Operations Bridge Analytics Collector host and on the Operations Bridge Analytics Server to import the certificate.
6. *OMi integration only. Import the OMi certificate into OBA.*
- a. On an OMi data processing server, export the certificates by running the following command:

```
ovcert -exporttrusted -file omi.cer
```
 - b. Copy the file to all of the OBA collectors.
 - c. As the `opsa` user on each collector, change the directory to `/opt/HP/opsa` and run the `$OPSA_HOME/bin/opsa-collector-manager.sh` script on the Operations Bridge Analytics Collector host. See the *opsa-collector-manager.sh* reference page (or the Linux man page), for more information.

Note: This script must be run out of the `$OPSA_HOME` directory.

- d. Make the following selections in the resulting flow of options:
 - i. Select option 1: **Configure SSL**.
 - ii. Select option 4: **Import trusted certificate to OPSA truststore**. Specify the file exported in the previous steps, for example `/tmp/omi/cer`. If prompted to run a procedure manually, execute it in another shell.
 - iii. Select option 13: **Go back to main menu**.
 - iv. Select option 7: **Exit**.
 - v. Restart all OBA processes by calling `sudo /opt/HP/opsa/bin/opsa restart`.

Note: Your configuration changes will not occur unless the collector is restarted. If you receive an error, follow the instructions in the error messages.

7. *OMi integration only. Import the OBA certificate into OMi.*
- a. On all OBA servers, export the OBA server certificate:
 - i. As the `opsa` user, change the directory to `/opt/HP/opsa` and run the `$OPSA_HOME/bin/opsa-server-manager.sh` script on the Operations Bridge Analytics Server. See the *opsa-server-manager.sh* reference page (or the Linux man page), for

more information.

Note: This script must be run out of the \$OPSA_HOME directory.

Make the following selections in the resulting flow of options:

- A. Select option **2: Configure SSL**.
 - B. Select option **5: Export certificate from OPSA keystore**. Enter the `opsa_server` alias from the list of key aliases in the OPSA keystore. Store the file, for example as `/tmp/opsa_server.cer`.
 - C. Select option **13: Go back to main menu**.
 - D. Select option **7: Exit**.
- b. Copy the exported OBA server certificates to one of the OMi gateway servers.
 - c. Import all the OBA server certificates to OMi:
 - i. On one of the OMi gateway servers, run the following command for all OBA server certificates:

```
<OMi_HOME>\bin\opr-cert-mgmt.[bat|sh] -import opsa_server <path>
```

For more information on the `opr-cert-mgmt` tool, see the *OMi Extensibility Guide*.
 - d. Export the OBA collector certificates by doing the following on all OBA collectors:
 - i. As the `opsa` user, change the directory to `/opt/HP/opsa` and run the `$OPSA_HOME/bin/opsa-collector-manager.sh` script on the Operations Bridge Analytics Collector host. See the *opsa-collector-manager.sh* reference page (or the Linux man page), for more information.
 - ii. Select option **1: Configure SSL**.
 - iii. Select option **5: Export certificate from OPSA keystore**. Enter the `opsa_collector` alias from the list of key aliases in the OPSA keystore. Store the file, for example as `/tmp/opsa_collector.cer`.
 - iv. Select option **13: Go back to main menu**.
 - v. Select option **5: Exit**.
 - vi. Convert the certificate to PEM format by running the following commands:

```
-keytool -import -alias opsa_server -file <file exported in previous step> -keystore /tmp/test.keystore -storepass 123456  
-keytool -exportcert -alias opsa_server -file <collector certificate> -rfc -keystore /tmp/test.keystore -storepass 123456
```

- vii. Copy the converted collector certificate to one OMi data processing server and import the certificate:

```
ovcert -importtrusted -file <copied certificate file>
```

OMi automatically distributes the certificate to all OMi data processing and gateway servers.

- e. Restart OMi on all servers to distribute the trust(s) to all of the servers' truststores.

Configuring SSL Communication to the OBA Server and Collector with a Self-Signed Certificate

To set up SSL communication to the OBA server and collector using a self-signed certificate, perform the following steps:

1. **Unregister the collector.** If OBA is already configured with collections (the collector is already registered) you must unregister all collections either by using the OBA interface or the command line. Run the following command as the `opsa` user to unregister the collector from the OBA server:

```
/opt/HP/opsa/bin/opsa-collection-config.sh -unregister -collectorhost
<collector IP address> -port 9443 -username <tenant admin username> -password
<password for tenant admin username>
```

Run the following command to check that the collector was unregistered successfully:

```
/opt/HP/opsa/bin/opsa-collection-config.sh -list -allversions -collectorhosts -
port 9443 -username <tenant admin username> -password <password for tenant
admin username>
```

2. **Configure SSL communication to the OBA server.** Complete the following steps as the `opsa` user to enable SSL communication to the OBA server using a self signed certificate:

- a. Before enabling SSL to the Operations Bridge Analytics Server, complete this step on the Operations Bridge Analytics Server to create a user in JBoss **Management Realm**.

Do the following:

- i. Run the `$OPSA_HOME/jboss/bin/add-user.sh` script.
- ii. For the first question, answer **"a" - Management User (mgmt-users.properties)**, then follow the instructions.
- iii. When queried about the group to which the user should belong, accept the default

settings. When queried if the user will be used for one AS process to connect to another AS process, select No. If the script prompts you to add the JBOSS secret, you can safely ignore this. OBA does not use this secret.

- b. Set the self-signed certificate attributes, like common name, country, and validity, by editing the `/opt/HP/opsa/conf/ssl/cert/opsa-self-signed-cert.template` file.
- c. As the `opsa` user, change the directory to `/opt/HP/opsa` and run the `$OPSA_HOME/bin/opsa-server-manager.sh` script on the Operations Bridge Analytics Server. See the `opsa-server-manager.sh` reference page (or the Linux man page), for more information.

Note: This script must be run out of the `$OPSA_HOME` directory.

Make the following selections in the resulting flow of options:

- i. Select option **2: Configure SSL**.
- ii. Select option **1: Generate self signed certificate for OPSA** to generate a self sign key pair.
- iii. Select option **5: Export certificate from OPSA keystore**. Enter the `opsa_server` alias from the list of key aliases in the OPSA keystore. Store the file, for example as `/tmp/opsa_server.cer`.
- iv. Select option **4: Import trusted certificate to OPSA truststore**. Specify the file exported in the previous step, for example `/tmp/opsa_server.cer`. If prompted to run a procedure manually, execute it in another shell.
 - v. All server certificates must be imported to the truststore of all collectors, and all collector certificates must be imported to the truststore of all servers (import of collector certificates to other collectors and server certificates to other servers is not required).
- d. Select option **8: Enable/Disable SSL** and select Yes when asked if SSL should be enabled. . You will need to enter the JBoss **Management Realm** user and password you created in the first step. The `opsa-server-manager.sh` script prompts you for the certificate alias to be used for SSL communication. Enter the `opsa_server` alias from the list of key aliases in the OPSA keystore.
- e. Select the option **13: Go back to main menu**.
- f. Select option **7: Exit**.
- g. Restart all OBA processes by calling `sudo /opt/HP/opsa/bin/opsa restart`.

Note: Your configuration changes will not occur unless the server is restarted. If you

receive an error, follow the instructions in the error messages.

3. **Configure SSL communication to the OBA collector.** Complete the following steps to enable SSL communication to the OBA collector using a self-signed certificate:
 - a. Set the self-signed certificate attributes, like common name, country, and validity, by editing the `/opt/HP/opsa/conf/ssl/cert/opsa-self-signed-cert.template` file.
 - b. As the `opsa` user, change the directory to `/opt/HP/opsa` and run the `$OPSA_HOME/bin/opsa-collector-manager.sh` script on the Operations Bridge Analytics Collector host. See the *opsa-collector-manager.sh* reference page (or the Linux man page), for more information.

Note: This script must be run out of the `$OPSA_HOME` directory.

Make the following selections in the resulting flow of options:

- i. Select option **1: Configure SSL**.
 - ii. Select option **1: Generate a self signed certificate for OPSA**.
 - iii. Select option **5: Export certificate from OPSA keystore**. Enter the `opsa_collector` alias from the list of key aliases in the OPSA keystore. Store the file, for example as `/tmp/opsa_collector.cer`.
 - iv. Select option **4: Import trusted certificate to OPSA truststore**. Specify the file exported in the previous step, for example `/tmp/opsa_collector.cer`. If prompted to run a procedure manually, execute it in another shell.
 - v. All server certificates must be imported to the truststore of all collectors, and all collector certificates must be imported to the truststore of all servers (import of collector certificates to other collectors and server certificates to other servers is not required).
 - c. Select option **8: Enable/Disable SSL** and answer `Yes` when asked if SSL should be enabled.
 - d. Select option **13: Go back to main menu**.
 - e. Select option **5: Exit**.
 - f. Restart all OBA processes by calling `sudo /opt/HP/opsa/bin/opsa restart`.
4. **Reregister the OBA collector.**
 - a. On the OBA server as the `opsa` user, run the following command to register the collector with the SSL command:

```
/opt/HP/opsa/bin/opsa-collection-config.sh -register -collectorhost  
<collector IP address> -port 9443 -username <tenant admin username> -  
password <password for tenant admin username> -ssl
```

5. Log to OBA using `https://<oba server IP or FQDN>:8443/opsa`.
6. *Optional.* Select the **Import trusted certificate to OPSA server truststore** option to import trusted certificates (if any). For example, you can add HPE ArcSight Logger's server certificate to the Operations Bridge Analytics truststore file.

Note: You must complete this certificate import on all the Operations Bridge Analytics Collector hosts (for the structured log query). Follow these steps:

- a. Log on to the Logger console, then click **System Admin**.
 - b. Select the **SSL Server Certificate** option under **security** on the left side of the screen.
 - c. Click the View Certificate button at the bottom of the screen.
 - d. After the dialog box opens, copy the certificate text and save it to a file on both the Operations Bridge Analytics Collector host and on the Operations Bridge Analytics Server.
 - e. Complete this step on both the Operations Bridge Analytics Collector host and on the Operations Bridge Analytics Server to import the certificate.
7. *OMi integration only.* **Import the OMi certificate into OBA.**
 - a. On an OMi data processing server, export the certificates by running the following command:

```
ovcert -exporttrusted -file omi.cer
```
 - b. Copy the file to all of the OBA collectors.
 - c. As the `opsa` user on each collector, change the directory to `/opt/HP/opsa` and run the `$OPSA_HOME/bin/opsa-collector-manager.sh` script on the Operations Bridge Analytics Collector host. See the *opsa-collector-manager.sh* reference page (or the Linux man page), for more information.

Note: This script must be run out of the `$OPSA_HOME` directory.

- d. Make the following selections in the resulting flow of options:
 - i. Select option **1: Configure SSL**.
 - ii. Select option **4: Import trusted certificate to OPSA truststore**. Specify the file exported in the previous steps, for example `/tmp/omi/cer`. If prompted to run a

procedure manually, execute it in another shell.

- iii. Select option **13: Go back to main menu**.
- iv. Select option **7: Exit**.
- v. Restart all OBA processes by calling `sudo /opt/HP/opsa/bin/opsa restart`.

Note: Your configuration changes will not occur unless the collector is restarted. If you receive an error, follow the instructions in the error messages.

8. *OMi integration only*. **Import the OBA certificate into OMi.**

- a. On all OBA servers, export the OBA server certificate:
 - i. As the `opsa` user, change the directory to `/opt/HP/opsa` and run the `$OPSA_HOME/bin/opsa-server-manager.sh` script on the Operations Bridge Analytics Server. See the `opsa-server-manager.sh` reference page (or the Linux man page), for more information.

Note: This script must be run out of the `$OPSA_HOME` directory.

Make the following selections in the resulting flow of options:

- A. Select option **2: Configure SSL**.
 - B. Select option **5: Export certificate from OPSA keystore**. Enter the `opsa_server` alias from the list of key aliases in the OPSA keystore. Store the file, for example as `/tmp/opsa_server.cer`.
 - C. Select option **13: Go back to main menu**.
 - D. Select option **7: Exit**.
- b. Copy the exported OBA server certificates to one of the OMi gateway servers.
 - c. Import all the OBA server certificates to OMi:
 - i. On one of the OMi gateway servers, run the following command for all OBA server certificates:

```
<OMi_HOME>\bin\opr-cert-mgmt.[bat|sh] -import opsa_server <path>
```

For more information on the `opr-cert-mgmt` tool, see the *OMi Extensibility Guide*.
 - d. Export the OBA collector certificates by doing the following on all OBA collectors:
 - i. As the `opsa` user, change the directory to `/opt/HP/opsa` and run the `$OPSA_HOME/bin/opsa-collector-manager.sh` script on the Operations Bridge Analytics Collector host. See the `opsa-collector-manager.sh` reference page (or the Linux man page), for more information.

- ii. Select option **1: Configure SSL**.
 - iii. Select option **5: Export certificate from OPSA keystore**. Enter the `opsa_collector` alias from the list of key aliases in the OPSA keystore. Store the file, for example as `/tmp/opsa_collector.cer`.
 - iv. Select option **13: Go back to main menu**.
 - v. Select option **5: Exit**.
 - vi. Convert the certificate to PEM format by running the following commands:

```
-keytool -import -alias opsa_server -file <file exported in previous step> -keystore /tmp/test.keystore -storepass 123456  
  
-keytool -exportcert -alias opsa_server -file <collector certificate> -rfc -keystore /tmp/test.keystore -storepass 123456
```
 - vii. Copy the converted collector certificate to one OMi data processing server and import the certificate:

```
ovcert -importtrusted -file <copied certificate file>
```

OMi automatically distributes the certificate to all OMi data processing and gateway servers.
- e. Restart OMi on all servers to distribute the trust(s) to all of the servers' truststores.

Editing the SSL Configuration for the OBA Server or Collector

How to change the certificate alias used for SSL communication with the server

To change the certificate alias used for SSL communication, do the following:

1. Run the `$OPSA_HOME/bin/opsa-server-manager.sh` script, and log on with **super-admin** credentials. See the *opsa-server-manager.sh* reference page (or the Linux man page), for more information.

Note: This script must be run out of the `$OPSA_HOME` directory.

2. Select option **1: Configure SSL**.

3. Select option **7: Change key alias to be used for SSL communication**.
4. The `$OPSA_HOME/bin/opsa-server-manager.sh` script prompts you for the alias name and lists the existing set of aliases from the OPSA keystore. Enter the desired alias name from the list.
5. Select option **13: Go back to main menu** option, then select option **6: Restart OPSA server** option to restart the Operations Bridge Analytics Server.

Note: Your configuration changes will not occur unless the server is restarted.

How to change server certificate used for SSL communication with the collector

To change the server certificate used for SSL communication, do the following:

1. Unregister the collector. Run the following command as the "opsa user":

Unregister the collector. If OBA is already configured with collections (the collector is already registered) you must unregister all collections either by using the OBA interface or the command line. Run the following command as the opsa user to unregister the collector from the OBA server:

```
/opt/HP/opsa/bin/opsa-collection-config.sh -unregister -collectorhost  
<collector IP address> -port 9443 -username <tenant admin username> -password  
<password for tenant admin username>
```

Run the following command to check that the collector was unregistered successfully:

```
/opt/HP/opsa/bin/opsa-collection-config.sh -list -allversions -collectorhosts -  
port 9443 -username <tenant admin username> -password <password for tenant  
admin username>
```

2. Run the `$OPSA_HOME/bin/opsa-collector-manager.sh` script. See the *opsa-collector-manager.sh* reference page (or the Linux man page), for more information.

Note: This script must be run out of the `$OPSA_HOME` directory.

3. Select option **1: Configure SSL**.
4. Select option **7: Change key alias to be used for SSL communication**.
5. The `$OPSA_HOME/bin/opsa-collector-manager.sh` script prompts you for the alias name, and lists the existing set of certificate aliases from the OPSA keystore. Enter the desired alias name from the list.

6. Select option **13: Go back to main menu**, then select option **4: Restart OPSA Collector** option to restart the Operations Bridge Analytics Collector host.

Note: Your configuration changes will not occur unless the Operations Bridge Analytics Collector host is restarted.

7. Run the following command as the "opsa" user to re-register the collector with the SSL:

```
/opt/HP/opsa/bin/opsa-collection-config.sh -register -collectorhost <collector  
IP address> -port 9443 -username <tenant admin username> -password <password  
for tenant admin username> -ssl
```

Disabling the SSL Configuration for the OBA Server or Collector

How to disable the SSL configuration for the OBA server

To disable the SSL communication, do the following:

1. Run the `$OPSA_HOME/bin/opsa-server-manager.sh` script from the Operations Bridge Analytics Server and log on with **super-admin** credentials. See the `opsa-server-manager.sh` reference page (or the Linux man page), for more information.

Note: This script must be run out of the `$OPSA_HOME` directory.

2. Select option **2: Configure SSL**.
3. Select option **8: Enable/Disable SSL**.
4. The `$OPSA_HOME/bin/opsa-server-manager.sh` script prompts you for a confirmation. Enter yes to disable the SSL communication.
5. Select option **13: Go back to main menu** option, then select option **6: Restart OPSA server** option to restart the Operations Bridge Analytics Server.

How to disable the SSL configuration for the OBA collector

To disable the SSL communication, do the following:

1. Unregister the collector from the server. Run the following command as the "opsa" user:

Unregister the collector. If OBA is already configured with collections (the collector is already registered) you must unregister all collections either by using the OBA interface or the command line. Run the following command as the opsa user to unregister the collector from the OBA server:

```
/opt/HP/opsa/bin/opsa-collection-config.sh -unregister -collectorhost  
<collector IP address> -port 9443 -username <tenant admin username> -password  
<password for tenant admin username>
```

Run the following command to check that the collector was unregistered successfully:

```
/opt/HP/opsa/bin/opsa-collection-config.sh -list -allversions -collectorhosts -  
port 9443 -username <tenant admin username> -password <password for tenant  
admin username>
```

2. Run the `$OPSA_HOME/bin/opsa-collector-manager.sh` script. See the *opsa-collector-manager.sh* reference page (or the Linux man page), for more information.

Note: This script must be run out of the `$OPSA_HOME` directory.

3. Select option **1: Configure SSL**.
4. Select option **8: Enable/Disable SSL**.
5. The `$OPSA_HOME/bin/opsa-collector-manager.sh` script prompts you for a confirmation. Enter `yes` to disable the SSL communication.
6. Select option **13: Go back to main menu** option, then select the **Restart OPSA Collector** option to restart the Operations Bridge Analytics Collector host.
7. Run the following command as the "opsa" user to register the collector:

```
/opt/HP/opsa/bin/opsa-collection-config.sh -register -collectorhost <collector  
IP address> -port 9443 -username <tenant admin username> -password <password  
for tenant admin username> -ssl
```

Managing the Keystore and Truststore for the OBA Server and Collector

How to modify the OBA keystore and truststore password

To modify the Operations Bridge Analytics keystore and truststore password, do the following:

1. Run the `$OPSA_HOME/bin/opsa-server-manager.sh` or the `$OPSA_HOME/bin/opsa-collector-manager.sh` script, and log on with **super-admin** credentials. See the *opsa-server-manager.sh* reference page (or the Linux man page) or the *opsa-collector-manager.sh* reference page for more information.

Note: This script must be run out of the `$OPSA_HOME` directory.

2. Select the **Configure SSL** option.
3. Select the **Modify OPSA keystore/truststore password** option.
4. The script prompts you for the new password for the keystore and truststore. Enter the new passwords.
5. Select the **Go back to main menu** option, then select the **Restart OPSA server** or the **Restart OPSA collector** option to restart the server or collector.

How to delete a certificate in the OBA keystore and truststore

To delete a certificate from the Operations Bridge Analytics keystore and truststore, do the following:

1. Run the `$OPSA_HOME/bin/opsa-server-manager.sh` or the `$OPSA_HOME/bin/opsa-collector-manager.sh` script, and log on with **super-admin** credentials. See the *opsa-server-manager.sh* reference page (or the Linux man page) or the *opsa-collector-manager.sh* reference page for more information.

Note: This script must be run out of the `$OPSA_HOME` directory.

2. Select the **Configure SSL** option.
3. Select the **Delete certificate from OPSA server keystore** or **Delete certificate from OPSA server truststore** option for the server, or the **Delete certificate from OPSA keystore** or **Delete**

certificate from OPSA truststore option for the collector.

4. The script prompts you for the alias name, listing the existing set of aliases from the OPSA keystore/truststore. Enter the alias name to be deleted from the list.
5. Select the **Go back to main menu** option, then select the **Restart OPSA server** option to restart the Operations Bridge Analytics Server or the **Restart OPSA collector** option to restart the collector.

Note: The certificate delete will fail if the certificate is in use.

How to export a certificate from the OBA keystore

To export a certificate from the Operations Bridge Analytics keystore, do the following:

1. Run the `$OPSA_HOME/bin/opsa-server-manager.sh` or the `$OPSA_HOME/bin/opsa-collector-manager.sh` script, and log on with **super-admin** credentials. See the *opsa-server-manager.sh* reference page (or the Linux man page) or the *opsa-collector-manager.sh* reference page for more information.

Note: This script must be run out of the `$OPSA_HOME` directory.

2. Select the **Configure SSL** option.
3. Select the **Export certificate from OPSA server keystore** option.
4. The script prompts you for the alias name, listing the existing set of aliases from the Operations Bridge Analytics keystore. Enter the alias name to be deleted from the list.
5. The script prompts you for the file path to which the certificate should be exported. Enter the path to export the certificate.

How to change an OBA keystore file

To change an Operations Bridge Analytics keystore file, do the following:

Note: The keystore password and the truststore password must be identical.

1. Run the `$OPSA_HOME/bin/opsa-server-manager.sh` script, and log on with **super-admin** credentials. See the *opsa-server-manager.sh* reference page (or the Linux man page) for more information.

Note: This script must be run out of the \$OPSA_HOME directory.

2. Select the **Configure SSL** option.
3. Select the **Change OPSA keystore file** option.
4. The script prompts you with a set of prerequisite actions to take before proceeding. Enter yes after you complete these prerequisites.
5. Enter the absolute path of the keystore file.

How to change an OBA truststore file

To change an Operations Bridge Analytics truststore file, do the following:

Note: The keystore password and the truststore password must be identical.

1. Run the \$OPSA_HOME/bin/opsa-server-manager.sh script, and log on with **super-admin** credentials. See the *opsa-server-manager.sh* reference page (or the Linux man page) for more information.

Note: This script must be run out of the \$OPSA_HOME directory.

2. Select the **Configure SSL** option.
3. Select the **Change OPSA truststore file** option.
4. The script prompts you with a set of prerequisite actions to take before proceeding. Enter yes after you complete these prerequisites.
5. Enter the absolute path of the truststore file.

Two-Way SSL for Accessing ArcSight Logger

Complete the following steps to configure two-way SSL authentication with ArcSight Logger:

1. Create an SSL truststore on the Operations Bridge Analytics Server with HPE ArcSight Logger's server certificate:
 - a. Copy the self-signed or CA certificate from HPE ArcSight Logger. You will find the self-signed certificate in the following location:

```
<Install_Dir>//userdata/platform/ssl.crt/server.crt
```

- b. Run the `opsa-server-manager.sh` script as the root user.

Note: This script must be run out of the `$OPSA_HOME` directory.

Note: Running the `opsa-server-manager.sh` script could result in a message similar to the following:

```
com.hp.opsa.server.admin.ssl.config.OPSCertStoreException:
please run this procedure manually with root credentials:
```

If you see this message, there will be no residual effect. The remedy is to complete only one of the following actions:

- Run the `opsa-server-manager.sh` script as root and complete the steps shown below.
- Do not run the `opsa-server-manager.sh` script. Instead, run the following command manually using root credentials:


```
sudo keytool -import -trustcacerts -alias CN=HPQ Issuing Certification
Authority 2016-1, DC=americas, DC=cpqcorp, DC=net -keystore
/opt/HP/opsa/jdk/jre/lib/security/cacerts -file /home/opsa/HPQ Issuing
Certification Authority 2016-1.pem -storepass changeit
```

- i. Log on as the `opsaadmin` user.
 - ii. Choose **Option 2** to configure SSL.
 - iii. Choose **Option 4** to import the trusted certificate into the OpsA truststore.
 - iv. Enter the file name of the certificate you want to import; then press **Enter**.
 - v. Repeat the prior steps for additional certificate files you want to import.
 - vi. Exit the `opsa-server-manager.sh` script.
2. Create a self-signed certificate and a keystore using OpenSSL for the Operations Bridge Analytics Server:
- a. Create a private key using the following command:


```
openssl genrsa -out /opt/HP/opsa/conf/opsa.key 1024
```
 - b. Generate a certificate request using the following command:


```
openssl req -new -key /opt/HP/opsa/conf/opsa.key -out
/opt/HP/opsa/conf/opsa.csr
```
 - c. Create a self-signed certificate using the following command:


```
openssl x509 -req -days 365 -in /opt/HP/opsa/conf/opsa.csr -signkey
```



```
/opt/HP/opsa/conf/opsa.key -out /opt/HP/opsa/conf/opsa.crt
```

- d. Export the self-signed certificate to PKCS#12 format using the following command:

```
openssl pkcs12 -export -out /opt/HP/opsa/conf/opsa.p12 -inkey
/opt/HP/opsa/conf/opsa.key -in /opt/HP/opsa/conf/opsa.crt
```

Note: Retain a copy of the export password.

- e. Use the following command to create a keystore and import the generated PKCS#12 format certificate:

```
keytool -importkeystore -srckeystore /opt/HP/opsa/conf/opsa.p12 -
destkeystore /opt/HP/opsa/conf/opsa_keystore.jks -srcstoretype
pkcs12 -deststoretype JKS -deststorepass <keystore_password> -
srcstorepass <export_password_entered_in_above_step>
```

3. Configure HPE ArcSight Logger to enable client authentication:

- a. Copy the Operations Bridge Analytics Server's self-signed certificate from the following location:

```
$OPSA_HOME/conf/opsa.crt
```

to this location on the HPE ArcSight Logger server:

```
<Install_Dir>/current/local/apache/conf/ssl.crt
```

- b. Edit HPE ArcSight Logger's web server configuration file:

```
<Install_Dir>/current/local/apache/conf/httpd.conf
```

- c. If the following lines do not exist in the file, add them, then save your work:

```
SSLVerifyClient require
```

```
SSLVerifyDepth 0
```

```
SSLCACertificateFile <Install_
```

```
Dir>/current/local/apache/conf/ssl.crt/opsa.crt
```

- d. Run the following command as the root user to restart HPE ArcSight Logger's web server:

```
<Install_Dir>/current/arcsight/service/apache restart
```

4. Configure the Operations Bridge Analytics Server's configuration file:

- a. Edit the following file: `$OPSA_HOME/conf/opsa-config.properties`

- b. Add the following line, then save your changes. `logger.ssl.enabled=true`

5. Configure the JBoss Application server:

- a. Edit the JBoss application server configuration file:

```
$JBOSS_HOME/bin/standalone.conf
```

- b. Add the following lines and save your work:

```
JAVA_OPTS="$JAVA_OPTS -Djavax.net.ssl.trustStore=/opt/HP/opsa/conf/ssl/opsa-truststore.jks"
```

```
JAVA_OPTS="$JAVA_OPTS -Djavax.net.ssl.trustStorePassword=<password of trust store>"
```

```
JAVA_OPTS="$JAVA_OPTS -Djavax.net.ssl.keyStore=/opt/HP/opsa/conf/ssl/opsa_keystore.jks"
```

```
JAVA_OPTS="$JAVA_OPTS -Djavax.net.ssl.keyStorePassword=<password of key store>"
```

6. Use the following commands to restart the JBoss server:

- a. Run the following command to stop JBoss: `$OPSA_HOME/jboss/bin/ jboss-cli.sh --connect controller=<ip_address>:19999 command=:shutdown`

- b. Run the following command to start JBoss:

```
$OPSA_HOME/jboss/bin/standalone.sh
```

SSL for Communication Between Vertica and OBA

The information in this section explains how to manage SSL communications between Operations Bridge Analytics and the Vertica (Operations Bridge Analytics) database.

Enabling SSL Communications between the Operations Bridge Analytics Server and Vertica

Complete the following steps from the server that contains the Vertica database to enable SSL communications between the Operations Bridge Analytics Server and the Vertica (Operations Bridge Analytics) database:

1. Complete only one of the following options:

- o **Option 1:** Self-signed certificate:

- i. Run the following command to create the CA private key:

```
openssl genrsa -des3 -out rootkey.pem
```

- ii. Run the following command to create the CA public certificate. When prompted, fill in the correct information:

```
openssl req -new -x509 -key rootkey.pem -out root.crt
```

- iii. Run the following command to create the server private key:

```
openssl genrsa -out server.key
```

- iv. Run the following command to create the server certificate request. When prompted, fill in the correct information:

```
openssl req -new -out reqout.txt -key server.key
```

o **Option 2: Certificate Authority (CA) Signed Certificate:**

- i. Run the following command to create the server private key:

```
openssl genrsa -out server.key
```

- ii. Run the following command to create the server certificate request. When prompted, fill in the correct information:

```
openssl req -new -out reqout.txt -key server.key
```

- iii. Submit the server certificate request to a public Certificate Authority.

2. Run the following command to sign the certificate for the server that contains Vertica. This command uses the CA private key:

```
openssl x509 -req -in reqout.txt -days 3650 -sha1 -CAcreateserial -CA root.crt -CAkey rootkey.pem -out server.crt
```

Note: Following the completion of this step, you have the server private key (the `server.key` file) and the signed server certificate (the `server.crt` file).

3. Run the following command to convert the signed certificate into a format understood by Java:

```
openssl x509 -in server.crt -out server.crt.der -outform der
```

Look for the `server.crt.der` file in the directory from which you ran the command shown in this step.

4. Move the newly created `server.crt.der` file to a directory on the Operations Bridge Analytics Server.
5. Although you run the other commands in this section from the server that contains the Vertica database, you must complete the following from the Operations Bridge Analytics Server to import the signed certificate from Vertica (the file generated from the previous step) into the Operations Bridge Analytics truststore:

- a. Run the `opsa-server-manager.sh` script.

Note: This script must be run out of the `$OPSA_HOME` directory.

- b. Log on to the Operations Bridge Analytics Server as the `opsadmin` user.
- c. Choose **Option 2** to configure SSL.
- d. Choose **Option 4** to import the trusted certificate into the OBA truststore.
- e. Enter the file name of the certificate you want to import; then press **Enter**.
- f. Repeat the prior steps for additional certificate files you want to import.
- g. Exit the `opsa-server-manager.sh` script.

Note: If you have not updated the default password of the truststore, it is `keystore_neutron_analytics_bigdata_opsa_2013`. Check with the Operations Bridge Analytics administrator to obtain the correct password.

See the `opsa-server-manager.sh` reference page (or the Linux manpage) for more information.

6. Modifying Vertica Configuration:

Assuming the username for the database user is `dbadmin:As dbadmin`, run the commands in the following steps to modify the Vertica configuration.

Note: You can also complete these steps using the following Vertica tool:

```
/opt/vertica/bin/adminTools
```

- a. `cp server.crt /home/dbadmin/opsadb/v_opsadb_node0001_catalog`
- b. `cp server.key /home/dbadmin/opsadb/v_opsadb_node0001_catalog`
- c. `chmod 700 /home/dbadmin/opsadb/v_opsadb_node0001_catalog/server.crt`
- d. `chmod 700 /home/dbadmin/opsadb/v_opsadb_node0001_catalog/server.key`

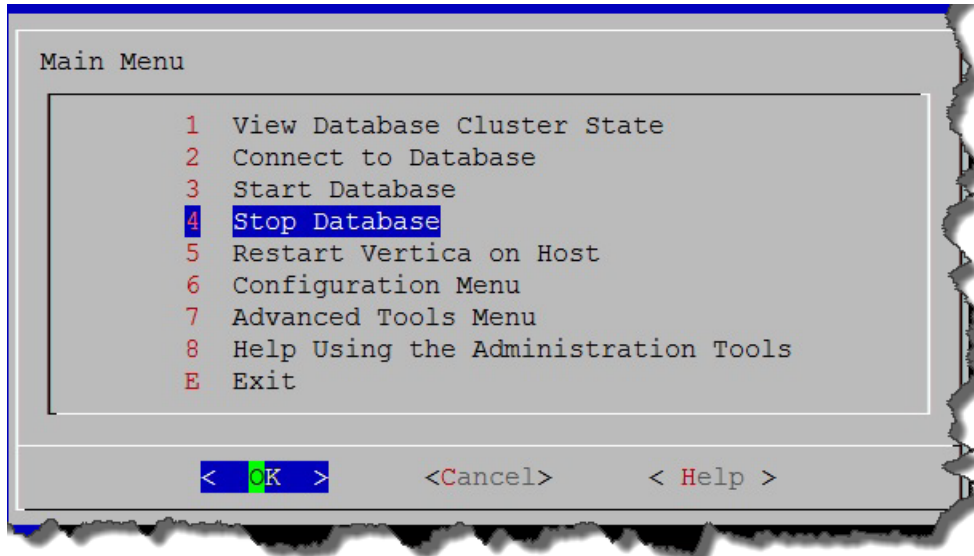
7. Assuming the username for the database user is `dbadmin:As dbadmin`, edit the following file:

```
/home/dbadmin/opsadb/v_opsadb_node0001_catalog/vertica.conf
```

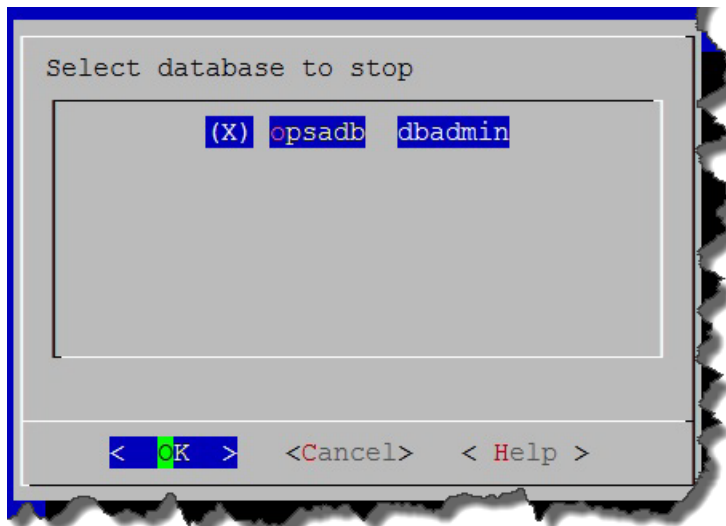
Add the following lines; then save your work:

```
EnableSSL=1
ClientAuthentication = local all password
ClientAuthentication = hostssl all 0.0.0.0/0 password
```

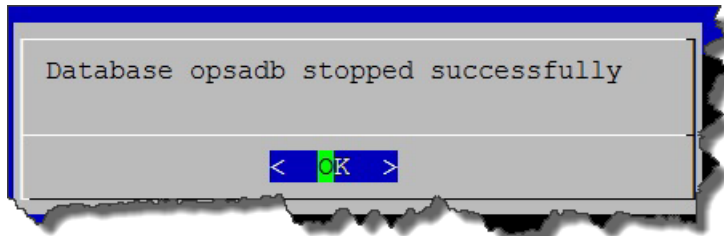
8. Complete the following steps to restart Vertica:
 - a. Assuming the username for the database user is dbadmin: As dbadmin run `/opt/vertica/bin/adminTools`.
 - b. Select **Stop Database**; then click **OK**.



- c. Select the database you want to stop (opsadb); then click **OK**.



- d. Look for the following message to make sure the database stopped; then click **OK** to go back to the main menu.

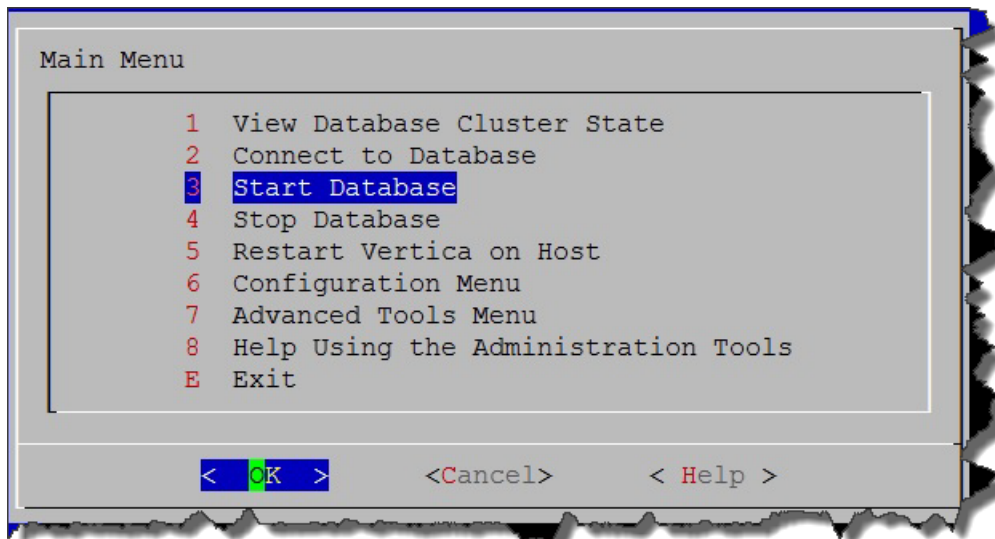


Note: If users are still connected to the database, the **Stop Database** command might not work, as Vertica prevents it from shutting down. To stop the database anyway, do the following:

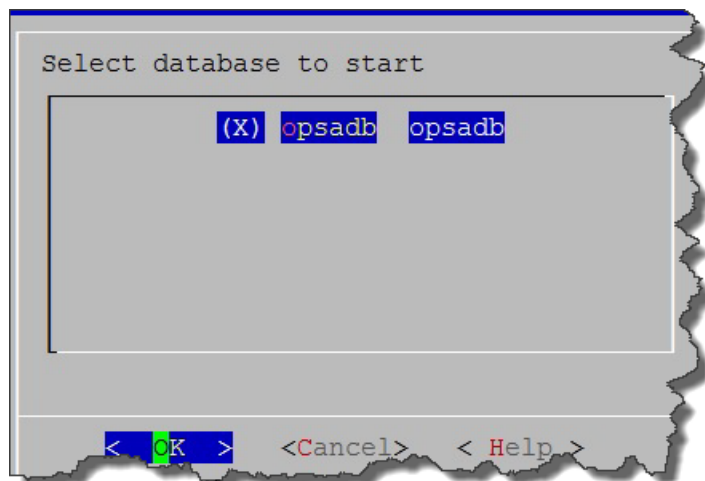
- i. Select the **Advanced Tools Menu**
- ii. Select **Stop Vertica on Host**
- iii. Select the host.

Note: After completing these steps you can start the database again.

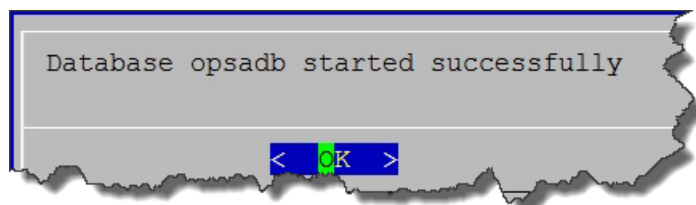
- e. Select **Start Database**; then click **OK**.



- f. Select the database you want to start (opsadb); then click **OK**.



- g. Look for the following message to make sure the database started successfully; then click **OK** to go back to the main menu.



- h. Exit the admin tool.

Note: If you set the file permissions incorrectly, it could result in the following error messages:

```
Unsafe permissions on private key file "/home/dbadmin/opsadb/v_
opsadb_node0001_catalog/server.key"
```

```
Could not load server certificate file "/home/dbadmin/opsadb/v_
opsadb_node0001_catalog/server.crt": error:0200100D:system
library:fopen:Permission denied
```

If you see error messages like this, see ["Modifying Vertica Configuration:" on page 33](#) to correct any file permissions issues and continue.

9. Complete the following steps on the Operations Bridge Analytics Server to enable SSL:

- a. Edit the `$OPSA_HOME/conf/opsa-config.properties` file.
- b. Search for the following string: `vertica.ssl.enabled=false`

Note: If the string in this step does not exist, add the string shown in the next step to the bottom of the text.

- c. Change the string as follows: `vertica.ssl.enabled=true`; then save your work.
- d. Edit the `$OPSA_HOME/jboss/standalone/configuration/standalone.xml` file. You should see text that resembles the following:

```
datasource jndi-name="java:jboss/datasources/VerticaDS" pool-
name="VerticaDS" enabled="true" use-java-context="true">
<connection-url>jdbc:vertica://fully-qualified domain name of
Vertica Server:5433/opsadb</connection-url>
<driver>vertica</driver>
<pool>
<min-pool-size>20</min-pool-size>
<max-pool-size>100</max-pool-size>
</pool>
<security>>
<security-domain>opsa-ds</security-domain>
</security>
<validation>
<validate-on-match>>false</validate-on-match>
<background-validation>>false</background-validation>
</validation>
<statement>
<share-prepared-statements>>false</share-prepared-statements>
</statement>
</datasource>
```

- e. Add the line shown in bold font; then save your work.

```
datasource jndi-name="java:jboss/datasources/VerticaDS" pool-
name="VerticaDS" enabled="true" use-java-context="true">
<connection-url>jdbc:vertica://fully-qualified domain name of
Vertica Server:5433/opsadb</connection-url>
<b>connection-property name="ssl">true</connection-property>
<driver>vertica</driver>
<pool>
```

```

<min-pool-size>20</min-pool-size>
<max-pool-size>100</max-pool-size>
</pool>
<security>>
<security-domain>opsa-ds</security-domain>
</security>
<validation>
<validate-on-match>>false</validate-on-match>
<background-validation>>false</background-validation>
</validation>
<statement>
<share-prepared-statements>>false</share-prepared-statements>
</statement>
</datasource>

```

10. Do the following to add the truststore location and password so that Jboss can find them and initialize the SSL handshake when communicating with Vertica.

a. Edit the `$OPSA_HOME/jboss/standalone/configuration/standalone.xml` file.

b. Locate the first bold phrase shown in following section in the `standalone.xml` file:

```

<system-properties>
<property name="org.apache.coyote.http11.Http11Protocol.MAX_HEADER_SIZE"
value="2097152"/>
<!--
To enable JDBC over SSL, uncomment this block:
<property name="javax.net.ssl.trustStorePassword" value="your_
truststore_password"/>
<property name="javax.net.ssl.trustStore"
value="/opt/HP/opsa/conf/ssl/opsa-truststore.jks"/>
-->
</system-properties>

```

c. Remove the bold `<!--, To enable JDBC over SSL, uncomment this block.,` and `-->` strings shown in the previous step (doing so uncomments the lines), then add the correct truststore password to `your_truststore_password`. See the example shown below in bold font:

```

<system-properties>
<property name="org.apache.coyote.http11.Http11Protocol.MAX_
HEADER_SIZE" value="2097152"/>
<property name="javax.net.ssl.trustStorePassword" value="your_truststore_
password"/>
<property name="javax.net.ssl.trustStore" value="/opt/HP/opsa/conf/ssl/opsa-

```

```
truststore.jks"/>
</system-properties>
```

Note: If you have not updated the default password of the truststore, it is `keystore_neutron_analytics_bigdata_opsa_2013`. Check with the Operations Bridge Analytics administrator to obtain the correct password.

d. Save your work.

11. You must restart Jboss any time you change the setting in the `opsa-config.properties` or `standalone.xml` files. Use the following command to restart the JBoss server: `$OPSA_HOME/bin/opsa-server restart`

Note: After running an `opsa-server restart` command, information logged in the `/opt/HP/opsa/log/opsa-server.log` file is removed. To view the files that retain this information across restarts, see the log files located in the `/opt/HP/opsa/jboss/standalone/log` directory. Look for log file names that begin with `server.log`.

Disabling SSL Communications between the Operations Bridge Analytics Server and Vertica

Complete the following steps from the server that contains the Vertica database to disable SSL communications between the Operations Bridge Analytics Server and the Vertica (Operations Bridge Analytics) database:

1. Edit the following file:

```
/opt/vertica/opsa_data/opsadb/v_opsadb_node0001_catalog/vertica.conf
```

Search for text that resembles the following lines.

```
EnableSSL=1
```

```
ClientAuthentication = local all password
```

```
ClientAuthentication = hostssl all 0.0.0.0/0 password
```

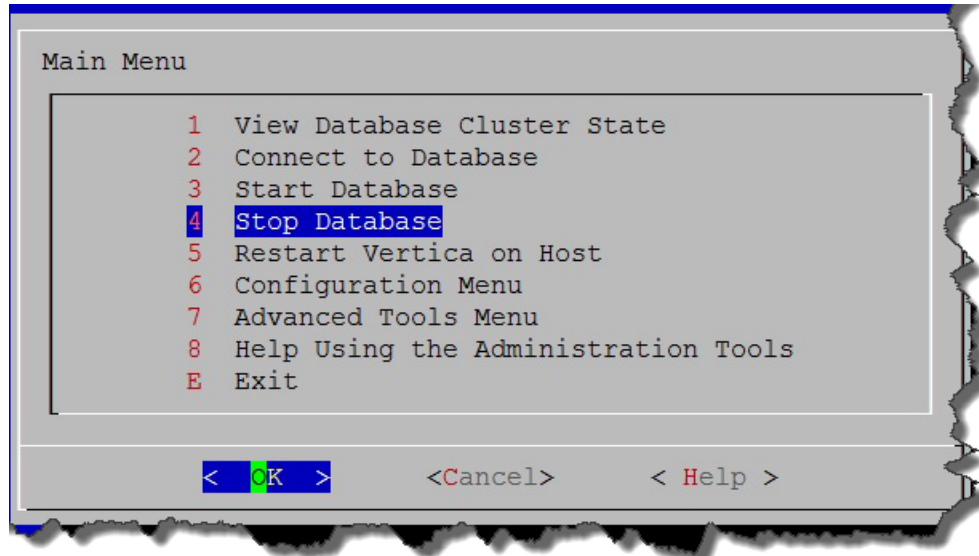
Comment the lines with the `#` character (shown in bold font below); then save your work:

```
#EnableSSL=1
```

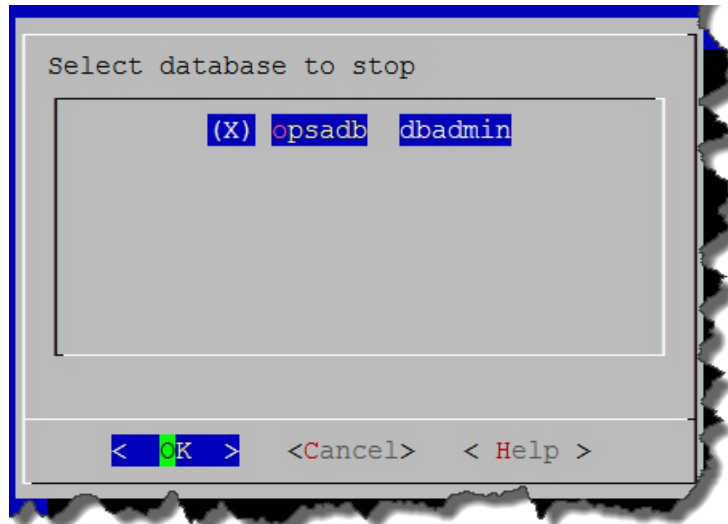
```
#ClientAuthentication = local all password
```

```
#ClientAuthentication = hostssl all 0.0.0.0/0 password
```

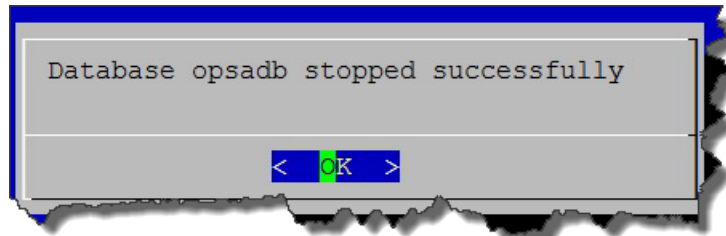
2. Complete the following steps to restart Vertica:
 - a. Run `/opt/vertica/bin/adminTools`.
 - b. Select **Stop Database**; then click **OK**.



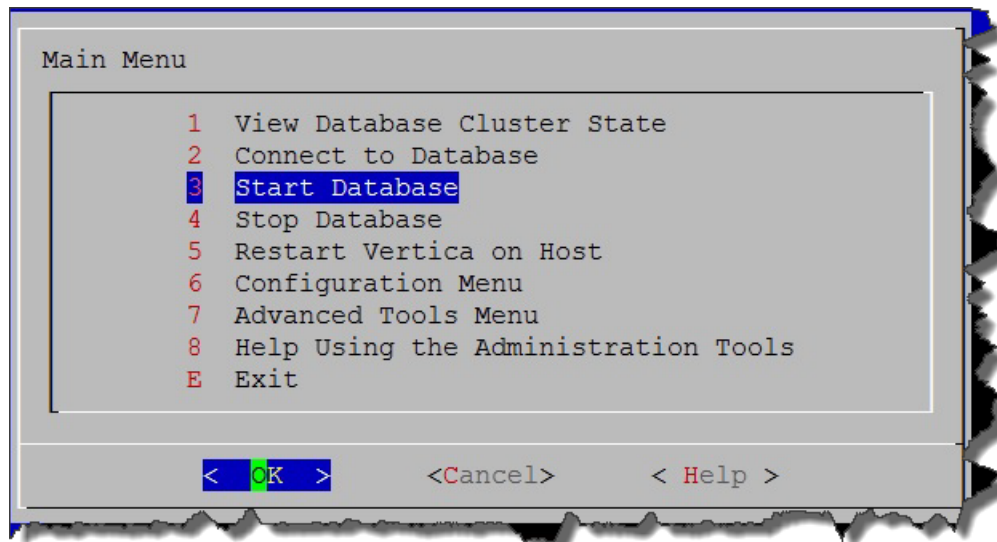
- c. Select the database you want to stop (opsadb); then click **OK**.



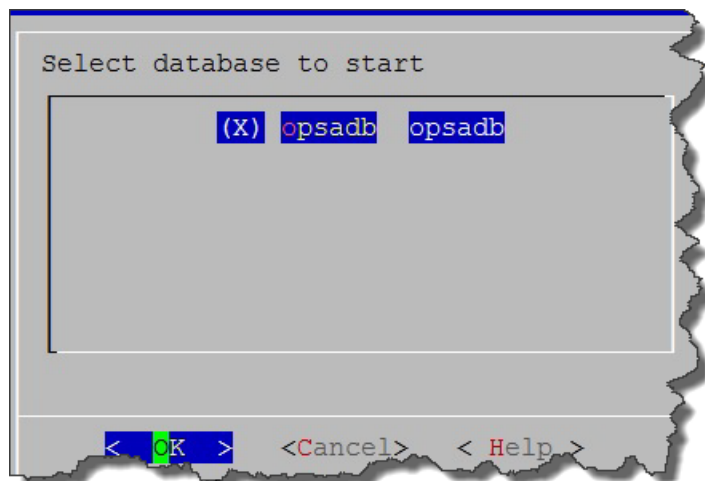
- d. Look for the following message to make sure the database stopped; then click **OK** to go back to the main menu.



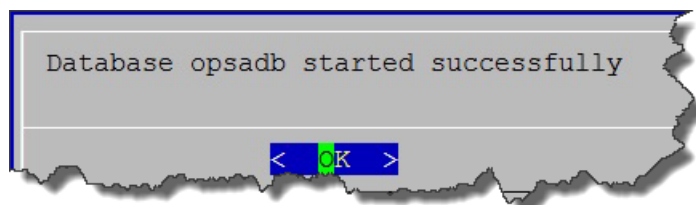
- e. Select **Start Database**; then click **OK**.



- f. Select the database you want to start (opsadb); then click **OK**.



- g. Look for the following message to make sure the database started successfully; then click **OK** to go back to the main menu.



- h. Exit the admin tool.

SSL communications between between the Operations Bridge Analytics Server and the Vertica (Operations Bridge Analytics) database is now disabled.

Enabling SSL Communications between the Operations Bridge Analytics Collector Host and Vertica

Complete the following steps on the Operations Bridge Analytics Collector host to enable SSL between the Operations Bridge Analytics Collector host and the Vertica (Operations Bridge Analytics) database:

1. Complete steps 1-8 in ["Enabling SSL Communications between the Operations Bridge Analytics Server and Vertica" on page 31](#) to enable SSL on Vertica.
2. Edit the `$OPSA_HOME/conf/opsa-config.properties` file.
3. Search for the following string: `vertica.ssl.enabled=false`

Note: If the string in this step does not exist, add the string shown in the next step to the bottom of the text.

4. Change the string as follows: `vertica.ssl.enabled=true`; then save your work.
5. Run the following command for the changes to take effect: `$OPSA_HOME/bin/opsa-collector restart`

SSL communications between the Operations Bridge Analytics Collector host and the Vertica (Operations Bridge Analytics) database is now enabled.

Disabling SSL Communications between the Operations Bridge Analytics Collector Host and Vertica

Complete the following steps on the Operations Bridge Analytics Collector host to disable SSL between the Operations Bridge Analytics Collector host and the Vertica (Operations Bridge Analytics) database:

1. Complete the steps shown in ["Disabling SSL Communications between the Operations Bridge Analytics Server and Vertica" on page 39](#) to disable SSL on Vertica.
2. Edit the `$OPSA_HOME/conf/opsa-config.properties` file.
3. Search for the following string: `vertica.ssl.enabled=true`

Note: If the string in this step does not exist, add the string shown in the next step to the bottom of the text.

4. Change the string as follows: `vertica.ssl.enabled=false`; then save your work.
5. Run the following command for the changes to take effect: `$OPSA_HOME/bin/opsa-collector restart`

SSL communications between the Operations Bridge Analytics Collector host and the Vertica (Operations Bridge Analytics) database is now disabled.

Adjusting Operations Bridge Analytics for RC4 Cipher Security Changes

Do the following on Operations Bridge Analytics Server and Collector hosts if you configured Operations Bridge Analytics to work over a secure channel (https):

1. Edit the `$OPSA_HOME/jboss/standalone/configuration/standalone.xml` file.
2. Locate the following section in the `standalone.xml` file:

```
<!--connector name="https" protocol="HTTP/1.1" scheme="https" secure="true"
socket-binding="https">
<ssl ca-certificate-file="/opt/HP/opsa/conf/ssl/opsa-truststore.jks"
certificate-key-file="/opt/HP/opsa/conf/ssl/opsa-keystore.jks" key-alias="opsa_
server" name="ssl" password="${VAULT::ks::pwd::${Password Key}}"
protocol="TLSv1,TLSv1.1,TLSv1.2" verify-client="false"/>
```

Uncomment this block as show below:

```
<connector name="https" protocol="HTTP/1.1" scheme="https" secure="true"
socket-binding="https">
<ssl ca-certificate-file="/opt/HP/opsa/conf/ssl/opsa-truststore.jks"
certificate-key-file="/opt/HP/opsa/conf/ssl/opsa-keystore.jks" key-alias="opsa_
server" name="ssl" password="${VAULT::ks::pwd::${Password Key}}"
protocol="TLSv1,TLSv1.1,TLSv1.2" verify-client="false"/>
```

3. Save your work.
4. You must restart Jboss any time you change the setting in the `opsa-config.properties` or `standalone.xml` files. Use the following command to restart the JBoss server: `$OPSA_HOME/bin/opsa-server restart`

Note: After running an `opsa-server restart` command, information logged in the `/opt/HP/opsa/log/opsa-server.log` file is removed. To view the files that retain this information across restarts, see the log files located in the `/opt/HP/opsa/jboss/standalone/log` directory. Look for log file names that begin with `server.log`.

5. Make the following modifications to the `java.security` file.

Note: HPE recommends that you back up the existing `java.java.security` file before making these modifications.

- a. Navigate to the `/opt/HP/opsa/jdk/jre/lib/security` directory.
- b. Using a text editor, open the `java.security` file that resides in the directory to which you just navigated.
- c. Locate the `jdk.tls.disabledAlgorithms` line located towards the bottom of this file. Replace the text in that line with the following text. If the line does not exist, add the following line:

```
“jdk.tls.disabledAlgorithms=MD5, SSLv3, RC4, DSA”
```
- d. Save your work.

SSL for the SMTP Server Used for OBA Alerts

The information in this section explains how to manage SSL communications to your SMTP server.

1. Verify that Operations Bridge Analytics servers are already communicating using SSL.
2. Copy the SMTP's root server certificate to the Operations Bridge Analytics servers and give the file full permissions.
3. Do the following to import the SMTP's root server certificate into the Operations Bridge Analytics truststore:
 - a. Run the `opsa-server-manager.sh` script.

Note: This script must be run out of the `$OPSA_HOME` directory.
 - b. Log on to the Operations Bridge Analytics Server as the `opsaadmin` user.
 - c. Choose **Option 2** to configure SSL.
 - d. Choose **Option 4** to import the trusted certificate into the OBA truststore.
 - e. Enter the file name of the certificate you want to import; then press **Enter**.
 - f. Repeat the prior steps for additional certificate files you want to import.
 - g. Exit the `opsa-server-manager.sh` script.

Chapter 4: HTTP and HTTPS

Configuring the HTTP and HTTPS Port for the Operations Bridge Analytics Collector Host

The Operations Bridge Analytics Collector host comes with a pre-configured HTTP and HTTPS port of 9443. If you run into any conflicts with port 9443, the value can be changed.

To change the HTTPS port to which the Operations Bridge Analytics Collector host listens, do the following:

1. Run the `$OPSA_HOME/bin/opsa-collector-manager.sh` script. See the *opsa-collector-manager.sh* reference page (or the Linux man page), for more information.

Note: This script must be run out of the `$OPSA_HOME` directory.

2. Select the **Configure HTTP(S) port** option.
3. When prompted, change the port to a value greater than 1024.
4. Select the **Restart OPSA Collector** option.
5. After the HTTPS port is changed, you must register the Operations Bridge Analytics Collector host on the Operations Bridge Analytics Server using the following command:

```
$OPSA_HOME/bin/opsa-collection-config.sh -register -collectorhost  
<collectorhost> -port <port> -username opsatenantadmin [-ssl] -  
coluser <collector_username> (the default collector username is opsa)  
-colpass <collector web service password> (the default password is  
opsa)
```

See the *opsa-collection-config.sh* reference page (or the Linux man page) for more information.

After you complete this step, future communication to this Operations Bridge Analytics Collector host uses the new HTTPS port.

Configuring the HTTP and HTTPS User Name and Password for the Operations Bridge Analytics Collector Host

The Operations Bridge Analytics Collector host comes with a pre-configured HTTPS user name, **opsa**, having an identical password, **opsa**. HPE recommends that customers change the user name and password for those environments where security is a concern.

1. Run the `$OPSA_HOME/bin/opsa-collector-manager.sh` script. See the *opsa-collector-manager.sh* reference page (or the Linux man page), for more information.

Note: This script must be run out of the `$OPSA_HOME` directory.

2. Select the **Configure username/password** option.
3. When prompted, change the username and password values.

Note: The `opsa-collector-manager.sh` script prompts you for the user name and password, then prompts you for the password again and validates that the passwords you entered are identical.

4. Select the **Restart OPSA Collector** option.
5. After the HTTP and HTTPS port is changed, you must register the Operations Bridge Analytics Collector host on the Operations Bridge Analytics Server using the following command:

```
$OPSA_HOME/bin/opsa-collection-config.sh -register -collectorhost  
<collectorhost> -port <port> -username opsatenantadmin [-ssl] -  
coluser <collector_username> (the default collector username is opsa)  
-colpass <collector web service password> (the default password is  
opsa)
```

See the *opsa-collection-config.sh* reference page (or the Linux man page) for more information.

After you complete this step, future access to this Operations Bridge Analytics Collector host uses the new username and password values.

Chapter 5: Single Sign On

Configuring and Enabling Single Sign-on to Access Operations Bridge Analytics

These instructions provide a practical example of configuring and enabling LWSSO between Operations Bridge Analytics and BSM or OMi. Use this practical example to help you configure LWSSO between Operations Bridge Analytics and other applications you plan to use.

Enabling Single Sign-on (LWSSO) in Operations Bridge Analytics permits users to launch the Operations Bridge Analytics console from a BSM or OMi event browser without needing to log on again. LWSSO is not enabled by default.

When using Single Sign-on, consider the following:

- Both systems must be configured for http or both systems must be configured for https. A mixture of these two protocols is not supported.
- Single Sign-on does not work if you use the Operations Bridge Analytics Server's IP address or short hostname. When using Single Sign-on, you must use the fully-qualified domain name of the Operations Bridge Analytics Server in the URL.

The below procedure must be performed on all OBA server systems.

Note: For this example, the user accounts for the BSM or OMi server and the Operations Bridge Analytics Server must match for these instructions to work correctly. The user name is case sensitive, so the user name used in each application must be identical.

1. Before enabling LWSSO to the Operations Bridge Analytics Server, complete the following steps to create a user in JBoss **Management Realm**:
 - a. As the `opsa` user, run the `$OPSA_HOME/jboss/bin/add-user.sh` script.
 - b. For the first question, answer **"a" - Management User (mgmt-users.properties)**, then follow the instructions.

Note: You will need to provide the JBoss management realm credentials when enabling LWSSO later in these instructions.

2. Run the `$OPSA_HOME/bin/opsa-server-manager.sh` script, and log on with **super-admin** credentials. See the *opsa-server-manager.sh* reference page (or the Linux man page), for more information.

Note: This script must be run out of the `$OPSA_HOME` directory.

3. Select the **Configure LWSSO** option.
4. Select the **Configure LWSSO parameters** option.
5. When prompted with **Enter the Token Creation Key (initString) [xxxxxxx]**, enter the `initString` key. For example, if you are configuring LWSSO for Operations Bridge Analytics and BSM or OMi, the value must match the `initString` configured in BSM or OMi.

Note: To view the `initString` configured in BSM or OMi, log on to BSM or OMi and navigate to:

BSM: **BSM > Admin > Platform > Users and Permissions > Authentication Management**

OMi: **Administration > Users > Authentication Management**

It is important to use the exact `initString` configured in BSM or OMi for this example. It is also important to use the exact `initString` with other applications you plan to use with Operations Bridge Analytics.

6. When prompted with **Enter the expiration period in minutes [60]**, enter the duration, in minutes, you want an LWSSO session to last before expiring.
7. When prompted with **Enter OPSA server domain**, enter the domain of the Operations Bridge Analytics Server.
8. If the BSM or OMi system is in a different domain, enter the trusted domain names (separated by a comma) when prompted with **Enter trusted domains separated by comma**. If they are in the same domain, this field can be left blank. Use the following form:

```
mytrusteddomain1.com, mytrusteddomain2.com
```

When finished, look for a **Configured LWSSO Successfully** message.

Note: You must include the domain for the BSM or OMi server, considering the BSM or OMi example being show in these steps. This is even more important if the domain is not in the same domain in which the Operations Bridge Analytics Server resides.

9. If OMi and OBA are in different domains, add them to the OMi Single Sign-On Configuration.

- a. On the OMi server go to **Administration > Users > Authentication Management**. On a BSM server, go to **BSM > Admin > Platform > Users and Permissions > Authentication Management**. In the Single Sign-On Configuration section click **Edit**.
 - b. Select Lightweight, then select Domain. Enter the domain for OMi.
 - c. Repeat steps a and b for OBA to create a second entry for the OBA domain.
10. After the `opsa-server-manager.sh` script finishes configuring LWSSO, it displays a **Configured LWSSO successfully** message, and gives you three options, one of which is to **Enable/Disable LWSSO**. Select the **Enable/Disable LWSSO** option to enable LWSSO. You will need to enter the JBoss **Management Realm** user and password you created in the first step. The `opsa-server-manager.sh` script prompts you for the certificate alias to be used for LWSSO communication. Enter one of the aliases from the list.
11. Exit the tool and restart the OBA processes as the root user:

```
sudo /opt/HP/opsa/bin/opsa restart
```

Note: Your configuration changes will not occur unless the server is restarted.

After completing the steps in this section, and configuring the correct URL on BSM or OMi, you can launch the Operations Bridge Analytics console from a BSM or OMi event browser without providing access credentials.

Note: If you already enabled LWSSO and need to make LWSSO configuration changes, complete the above instructions, skipping step 8.

Disabling Single Sign-on to Access Operations Bridge Analytics

To disable LWSSO, do the following:

1. Run the `$OPSA_HOME/bin/opsa-server-manager.sh` script, and log on with **super-admin** credentials. See the `opsa-server-manager.sh` reference page (or the Linux man page), for more information.

Note: This script must be run out of the `$OPSA_HOME` directory.

2. Select the **Configure LWSSO** option.
3. Select the option **Enable/Disable LWSSO** to disable LWSSO.

4. Exit the tool and restart the OBA processes as the root user:

```
/opt/HP/opsa/bin/opsa restart
```

Note: Your configuration changes will not occur unless the server is restarted.


Chapter 6: LDAP Authentication

Configuring LDAP Authentication for Operations Bridge Analytics

For information on configuring LDAP Authentication for Operations Bridge Analytics, see the OBA Online Help.

Configuring SSL for LDAP Server Authentication

The Operations Bridge Analytics console supports Lightweight Directory Access Protocol (LDAP) for user authentication. When configuring this LDAP authentication, you can also enable SSL for LDAP server authentication. You can configure LDAP server authentication using one of two methods:

- Click  **Settings**, then select **LDAP Servers**. See *Configuring LDAP Server Authentication for Operations Bridge Analytics* in the *Operations Bridge Analytics Help* for more information.
- Using the `opsa-ldap-configuration-manager.sh` script. See "[Configuring LDAP Authentication for Operations Bridge Analytics](#)" above for more information.

If you plan to enable SSL for LDAP server authentication when completing either of the above methods, you must complete the instructions in this section before configuring LDAP server authentication.

To configure SSL for LDAP server authentication, do the following:

1. Copy the LDAP's root server certificate to the Operations Bridge Analytics servers and give the file full permissions.
2. Run the `opsa-server-manager.sh` script.

Note: This script must be run out of the `$OPSA_HOME` directory.

- a. Log on as the `opsaadmin` user.
- b. Choose **Option 2** to configure SSL.

- c. Choose **Option 4** to import the trusted certificate into the OBA truststore.
- d. Enter the file name of the certificate you want to import; then press **Enter**.
- e. Repeat the prior steps for additional certificate files you want to import.
- f. Exit the `opsa-server-manager.sh` script.
- g. Restart OBA processes as the root user:

```
/opt/HP/opsa/bin/opsa restart
```

Now that you enabled SSL for LDAP server authentication, continue configuring LDAP server authentication using one of the methods shown at the beginning of this section. You can now select the option to enable SSL for LDAP server authentication.

Chapter 7: PKI

Configuring User Authentication using Public Key Infrastructure (PKI) to Access Operations Bridge Analytics

SSL Client Certificate authentication using PKI enables users to log on to the Operations Bridge Analytics console with a client-side X.509 certificate.

As part of user authentication, you can configure the Operations Bridge Analytics Server to check the certificate to make sure it has not been revoked. You can configure the revocation check to do one of the following:

- Validate the certificate using a Certificate Revocation List (CRL) .
- Validate the certificate using the Online Certificate Status Protocol (OCSP) to run a direct query to the PKI.

PKI authentication is disabled by default. To enable PKI authentication, do the following:

1. Before enabling SSL to the Operations Bridge Analytics Server, complete the following steps to create a user in JBoss **Management Realm**:
 - a. Run the `$OPSA_HOME/jboss/bin/add-user.sh` script.
 - b. For the first question, answer **"a" - Management User (mgmt-users.properties)**, then follow the instructions.

Note: You will need to provide the JBoss management realm credentials when enabling SSL later in these instructions.

2. Run the `$OPSA_HOME/bin/opsa-server-manager.sh` script, and log on with **super-admin** credentials. See the `opsa-server-manager.sh` reference page (or the Linux man page), for more information.

Note: This script must be run out of the `$OPSA_HOME` directory.

3. Select the **Configure PKI Authentication** option.

4. Use one of the following approaches:
 - **Self-signed Certificate:** Select the **Generate self-signed certificate for OPSA server** option to generate a self-signed certificate and add the certificate to the Operations Bridge Analytics Server keystore.
 - **CA Signed Certificate:** Select the **Import CA certificate to OPSA server keystore** option to import a CA signed certificate to the Operations Bridge Analytics Server keystore.
5. **Mandatory Step:** Select the **Import trusted certificate to OPSA server truststore** option to import the trusted root CA certificate that will be used for PKI authentication.

Note: The certificate should be in base 64, otherwise the import will not work.

6. Select the **Enable/Disable PKI authentication** option to enable PKI. You will need to enter the JBoss **Management Realm** user and password you created in the first step. The `opsa-server-manager.sh` script prompts you for the certificate alias to be used for SSL communication. Enter one of the aliases from the list. For example, you might enter `opsa-server`.
7. When prompted with **Allow smart card logon only [yes/no]**, enter `yes` if only a smart log on is permitted. Enter `no` if a smart log on is not mandatory.
8. When prompted to select the field to use for a user name, enter the option you want Operations Bridge Analytics to use.
9. When prompted for **Check for certificate revocation [yes/no]**, enter `yes` for Operations Bridge Analytics to check if the certificate provided by the client is revoked or not. Enter `no` to disable the revocation check. If you enter `yes`, the `opsa-server-manager.sh` script prompts you to select between the following revocation test methods:
 - **Option 1:** Validate the certificate using a Certificate Revocation List (CRL) .
 - **Option 2:** Validate the certificate using the Online Certificate Status Protocol (OCSP) to run a direct query to the PKI .

Note: If you select option 2, the `opsa-server-manager.sh` script prompts you to configure the OCSP responder URL. You can accept the default behavior and have Operations Bridge Analytics use the value of the `authorityInfoAccess` field of the client certificate to obtain the responder URL, or you can directly configure the OCSP responder URL.

10. When prompted with **Do you want to configure proxy host [yes/no]**, enter `yes` if you want to configure the proxy host to check for certificate revocation status. Enter `no` if you do not want to configure the proxy host to check for certificate revocation status (a local OCSP responder is

available).

If you enter `yes`, the `opsa-server-manager.sh` script prompts you for the following information:

- proxy http proxy host
 - http port number
 - https proxy host
 - https port number
11. After successfully completing the registration, the `opsa-server-manager.sh` script shows an `authentication enabled successfully` message.
 12. Select the **Go back to main menu** option; then select the **Restart OPSA server** option to restart the Operations Bridge Analytics Server.

Note: Your configuration changes will not occur unless the server is restarted.

After completing the above steps, Operations Bridge Analytics users can access the Operations Bridge Analytics console using HTTP or HTTPS as follows:

See the `opsa-server-manager.sh` reference page (or the Linux man page) for more information.

1. If an Operations Bridge Analytics user enters an HTTP URL, Operations Bridge Analytics automatically redirects the URL to HTTPS, and shows a **Login with digital certificate** button.
2. After clicking the **Login with digital certificate** button, Operations Bridge Analytics presents its digital certificate, and the browser verifies it against its truststore.
3. After verifying the Operations Bridge Analytics certificate, Operations Bridge Analytics prompts the user to select the client certificate. On selecting the client certificate, Operations Bridge Analytics verifies the client certificate and performs authentication.

Note: The client certificate must be installed and imported to the browser, otherwise the user is not prompted for the client certificate.

4. If the authentication is successful, the browser opens the Operations Bridge Analytics home page.

Disabling User Authentication using Public (PKI) to Access Operations Bridge Analytics

To disable PKI authentication, do the following:

1. Run the `$OPSA_HOME/bin/opsa-server-manager.sh` script and log on with **super-admin** credentials. See the *opsa-server-manager.sh* reference page (or the Linux man page), for more information.

Note: This script must be run out of the `$OPSA_HOME` directory.

2. Select the **Configure Client Authentication** option.
3. Select the **Enable/Disable client authentication** button.
4. The `$OPSA_HOME/bin/opsa-server-manager.sh` script prompts you for confirmation. Enter `yes` to disable PKI authentication.
5. The `$OPSA_HOME/bin/opsa-server-manager.sh` script disables PKI, then prompts, **Do you want to disable SSL as well [yes/no]**. Enter `yes` to disable SSL communication or `no` to keep the existing SSL configuration.
6. Select the **Go back to main menu** option; then select the **Restart OPSA server** option to restart the Operations Bridge Analytics Server.

Note: Your configuration changes will not occur unless the server is restarted.

After completing the above steps, Operations Bridge Analytics presents its users with a user name and password page to access the Operations Bridge Analytics console.

Editing User Authentication using Public (PKI) to Access Operations Bridge Analytics

To modify PKI authentication, do the following:

1. Run the `$OPSA_HOME/bin/opsa-server-manager.sh` script and log on with **super-admin** credentials. See the *opsa-server-manager.sh* reference page (or the Linux man page), for more

information.

Note: This script must be run out of the \$OPSA_HOME directory.

2. Select the **Configure Client Authentication** option.
3. Select the **Edit client authentication settings** button.
4. The \$OPSA_HOME/bin/opsa-server-manager.sh script prompts you for PKI configuration information, similar to the prompts shown in ["Configuring User Authentication using Public Key Infrastructure \(PKI\) to Access Operations Bridge Analytics"](#) on page 54.
5. Select the **Go back to main menu** option; then select the **Restart OPSA server** option to restart the Operations Bridge Analytics Server.

Note: Your configuration changes will not occur unless the server is restarted.

Chapter 8: Resetting User Passwords

By default, users are prompted to select new passwords every 182 days. The number of days between resets can be modified by an administrator.

Note: If you are using LDAP to authenticate Operations Bridge Analytics users, do not use the information in this section when resetting passwords for LDAP authenticated users.

To modify the password reset time:

1. Go to **`/opt/HP/opsa/conf/opsa-config.properties`**
2. Modify the **`password.expiration.period.days`** property to the desired value.

Chapter 9: Changing the Port Used by the Operations Bridge Analytics Console

There might be a need to change the port used by the Operations Bridge Analytics console to comply with local security policies. Do the following:

1. As the opsa user, edit the `$JBOSS_HOME/bin/standalone.xml` file.
2. Search for the **standard-sockets** stanza and change the **http** port, **https** port, or both to the ports you want to use as shown in the following example (the items to search for are in bold font):

```
<socket-binding-group name="standard-sockets" default-interface="public"
port-offset="{jboss.socket.binding.port-offset:0}">
<socket-binding name="management-native" interface="management"
port="{jboss.management.native.port:19999}" />
<socket-binding name="management-http" interface="management"
port="{jboss.management.http.port:9990}" />
<socket-binding name="management-https" interface="management"
port="{jboss.management.https.port:9991}" />
<socket-binding name="ajp" port="8009" />
<socket-binding name="http" port="8080" />
<socket-binding name="https" port="8443" />
<socket-binding name="remoting" port="4447" />
<socket-binding name="txn-recovery-environment" port="4712" />
<socket-binding name="txn-status-manager" port="4713" />
<outbound-socket-binding name="mail-smtp">
<remote-destination host="localhost" port="25" />
</outbound-socket-binding>
</socket-binding-group>
```

3. Save your work.
4. Run the `$OPSA_HOME/bin/opsa-server restart` command to restart the Operations Bridge Analytics Server.

Chapter 10: Securing Data Among Tenants

If you have multiple tenants, HPE recommends using different Operations Bridge Analytics Collector hosts for each tenant. Doing so ensures data separation for each tenant.

Send documentation feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Hardening Guide (Operations Bridge Analytics 3.01)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to ovdoc-asm@hpe.com.

We appreciate your feedback!