Operations Bridge Analytics

Software Version: 3.00

Operations Bridge Analytics Hardening Guide

Document Release Date: January 2017
Software Release Date: January 2017

Hewlett Packard Enterprise

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.

Disclaimer:
Certain versions of documents (“Material”) accessible here may contain branding from Hewlett-Packard Company (now HP Inc.) and Hewlett Packard Enterprise Company. As of September 1, 2017, the Material is now offered by Micro Focus, a separately owned and operated company. Any reference to the HP and Hewlett Packard Enterprise/HPE marks is historical in nature, and the HP and Hewlett Packard Enterprise/HPE marks are the property of their respective owners.

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.

Contents

Chapter 1: Introduction

This guide contains information about how to configure HPE 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 Requirements

See the *Operations Bridge Analytics System Requirements and Sizing Guide* for the hardware and operating system requirements for Operations Bridge Analytics.

Any command examples shown in this document as being run by an opsa user can also be run by a root user.

`$OPSA_HOME` is set to `/opt/HP/opsa` in the Operations Bridge Analytics Server.

Terminology Used in this Document

Analytic Query Language (AQL): This language is the more advanced offering of two query languages supported by Operations Bridge Analytics. Use AQL when the Phrased Query Language (PQL) syntax is not specific enough to return the data you need. When using AQL, it is helpful if you have programming or scripting skills as well as some knowledge of databases. See *About Analytics Query Language (AQL) Functions* in the *Operations Bridge Analytics Help* for more information.

Collection: A collection defines the data to be collected and corresponds to a database table in which the Operations Bridge Analytics Collector host stores the data. Collections can be separated by tenant and the resulting collection information from these collections cannot be shared among tenants.

Custom Collections The list of collections supported by the Operations Bridge Analytics Server that do not have predefined templates.

Operations Bridge Analytics Collector Host: This virtual appliance or server is the server used to manage the data collections.

Data Sources: Operations Bridge Analytics collects metrics, topology, event, and log file data from a diverse set of possible data sources.

Link Tags: Special tags used to relate collection information. Create the same link tag for each collection you want to link together.

Meta Model: A way to describe the data to collect for analysis; it includes the construction and development of the frames, rules, constraints, models, and theories that are applicable and useful for modeling a predefined class of problems.

Metrics: Structured data that is typically collected from HPE's existing management products, other data files, or from other 3rd party management software. A metric is a measurement of one attribute at a specific point in time for a specified sub-entity or resource (such as CPU utilization). A metric is based on the most recent user-initiated search query.

Outlier or **Outliers**: Data that is outside of the normal range based on the data collected to date.

Predefined Collection Templates: The list of predefined collection templates that reside on the Operations Bridge Analytics Server for the collections Operations Bridge Analytics supports by default.

Phrased Query Language (PQL) : The less advanced offering of two query languages supported by Operations Bridge Analytics. Use PQL in the early stages of troubleshooting a problem. With this approach, type a word or phrase that begins to describe the type of problem you want to resolve and then select from the list of suggestions provided by Operations Bridge Analytics. See *About the Phrased Query Language* in the *Operations Bridge Analytics Help* for more information.

Raw Logs: These are log messages as they appear from the log management application with which Operations Bridge Analytics is integrated. These log files must be configured using the log file management software supported by Operations Bridge Analytics. See the *Operations Bridge Analytics System Requirements and Sizing Guide* for more information.

Operations Bridge Analytics Server: This virtual appliance or server is the Operations Bridge Analytics Server.

Structured Logs: Structured logs are fragments of log file data read by Operations Bridge Analytics from HPE ArcSight Logger. This log information is stored (as collections) in Operations Bridge

Analytics. These collections exist so that users can perform analytics on the log file contents. For example, users might want to query for all outliers by host name and application for a particular time range.

Tenant: Operations Bridge Analytics gathers metrics, topology, event, and log file data from a diverse set of possible data sources. Tenants enable you to separate information from these data sources into groups, such as collections, user accounts, and user groups. Collections can be separated by tenants, and the resulting collection information cannot be shared among tenants.

Virtual Appliance: A virtual appliance, also referred to as **appliance** in this document, is a self-contained system that is made by combining a software application, such as Operations Bridge Analytics software, with just enough operating system for it to run optimally on industry standard hardware or a virtual machine such as VMWare.

Data Sources Used in Operations Bridge Analytics

In today's complex data center environments, the source of a problem is not always easy to detect using traditional management and troubleshooting tools that look only for predetermined solutions to known potential problems. For example, many management and troubleshooting tools are designed to provide analytics for a specific problem context, such as root cause isolation, outlier detection, and service level agreement violation. They provide these services by using a specific data set and analytics technique.

With Operations Bridge Analytics, you generate insights from the IT data in your environment that you, the Operations Bridge Analytics administrator, choose to collect in your network. By identifying the most useful analytics to derive from the data depends on the problem context, the user community provides each data request.

As the Operations Bridge Analytics administrator, you configure collections from a diverse set of possible sources. For example, if you have HPE Network Node Manager (NNMi) or HPE Operations Manager i (HPE OMi), you can configure collections to gather NNMi topology or OMi events occurring within your network.

See "Table 2: Predefined Data Collection Sources by Collection Type" on the next page and "Table 3: Custom Data Collection Sources by Collection Type" on the next page for the list of supported data sources.

> **Note**: Operations Bridge Analytics requires that you use a configuration template to configure each collection. See "Table 2: Predefined Data Collection Sources by Collection Type" to determine the

> data sources that have predefined configuration templates. You create Custom Collections for any supported data source that does not have a configuration template provided by Operations Bridge Analytics.

Operations Bridge Analytics provides predefined collection templates for the data sources shown in the following table:

Table 2: Predefined Data Collection Sources by Collection Type

Predefined Data Collection Sources	Metrics Collection Type	Events Collection Type	Topology Collection Type	Inventory Collection Type
HPE BSM RTSM (Configuration Item Inventory)	no	no	no	yes
HPE Business Process Monitor (BPM)	yes	no	no	no
HPE NNMi Custom Poller	yes	no	no	no
HPE Network Node Manager iSPI Performance for Metrics Component Health	yes	no	no	no
HPE Network Node Manager iSPI Performance for Metrics Interface Health	yes	no	no	no
HPE Operations Agent	yes	no	no	no
HPE Operations Smart Plug-in for Oracle	yes	no	no	no
HPE OMi (Operations Manager i) Events	no	yes	no	no
HPE Operations Manager (OM) Events	no	yes	no	no

Operations Bridge Analytics supports, but does not provide, predefined collection templates for the data sources shown in the following table:

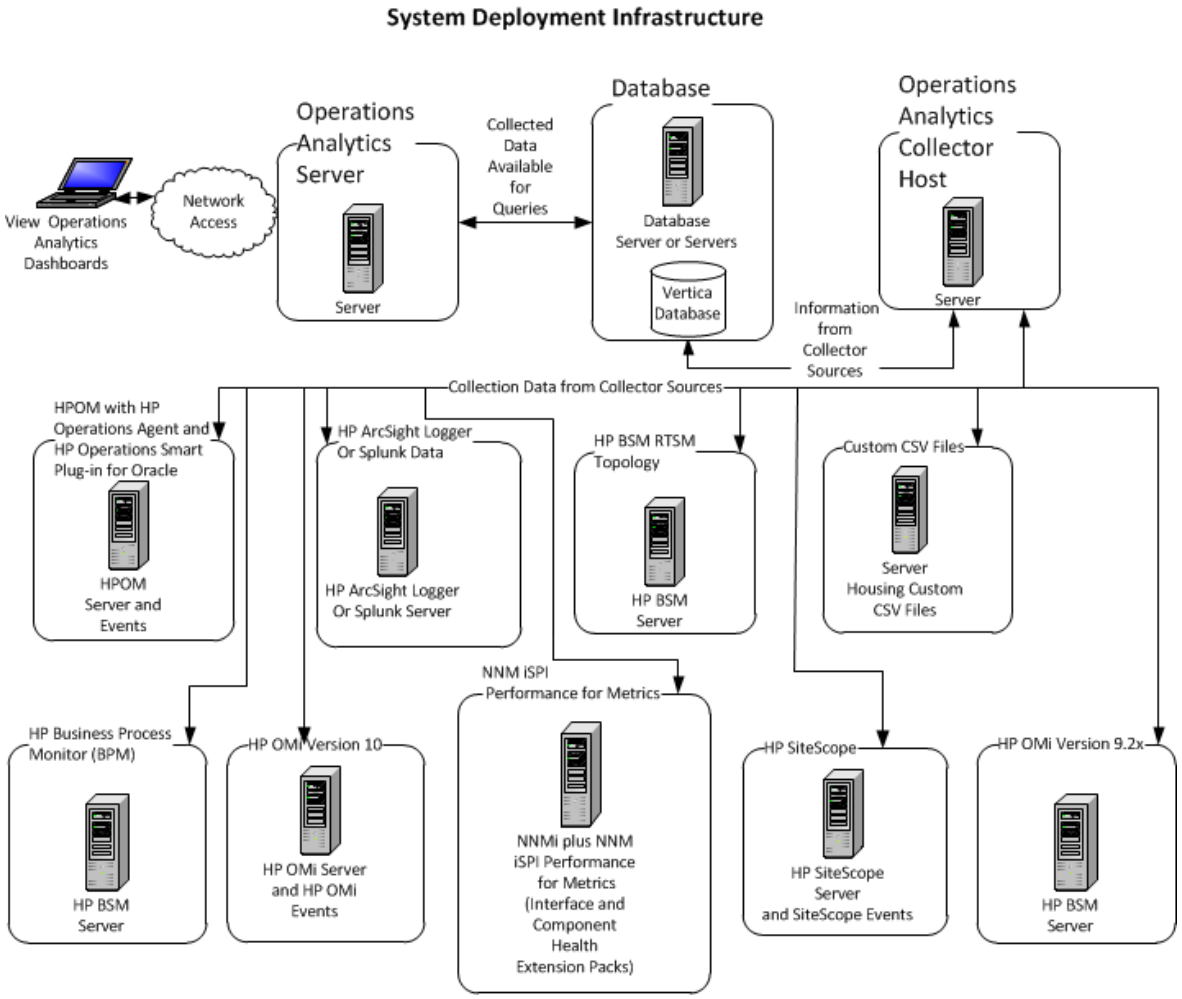
Table 3: Custom Data Collection Sources by Collection Type

Custom Collection Data Source	Topology Collection Type	Metrics Collection Type	Structured Logs Collection Type	Undefined Collection Type
HPE SiteScope	no	yes	no	no
Structured Logs	no	no	yes	no
Custom CSV Files	no	no	no	yes

> **Note:** Operations Bridge Analytics provides scripts to automatically generate templates for the HPE SiteScope and Custom CSV collections.

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.

Disabling Unnecessary CentOS Services

Complete the following actions to make your Operations Bridge Analytics installation more secure:

- If you are not planning to use Virtual Appliance Management Infrastructure services, disable the vami-lighttp and vami-sfcbd services using the following commands:
  a. `chkconfig --level 35 vami-lighttp off`
  b. `service vami-lighttp stop`
  c. `chkconfig --level 35 vami-sfcb off`
  d. `service vami-lighttp stop`
- If you are not planning to use Network File System (NFS) mapping to the Operations Bridge Analytics Server, disable the rpcgssd, rpcsvcgssd, rpcidmapd, and nfslock services using the following commands:
  a. `chkconfig --level 345 rpcgssd off`
  b. `service rpcgssd stop`
  c. `chkconfig --level 345 rpcsvcgssd off`
  d. `service rpcsvcgssd stop`
  e. `chkconfig --level 345 rpcidmapd off`
  f. `service vami-rpcidmapd stop`

g. `chkconfig --level 345 nfslock off`

h. `service nfslock stop`

- SSH login for the root account is disabled by default. Operations Bridge Analytics can only be accessed by using the default user name, opsa.
- It is highly recommended that you disable the SSH weak ciphers. To do this, the configuration entries already reside in the `sshd_config` file and need to be uncommented as follows:

  > **Note:** Not all SSH clients support the new ciphers. Make sure that your SSH client supports them.

  a. As the root user, edit the `sshd_config` file.

  b. To uncomment the following two lines, change:

  ```
  # Ciphers aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc
  # MACs hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160
  ```

  to

  ```
  Ciphers aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc
  MACs hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160
  ```

  c. Save your work.

  d. As a root user, run the following command to commit your changes: `service sshd restart`

- It is highly recommended that you use a secure protocol (https) to access Operations Bridge Analytics.
- Enable the CentOS firewall (iptables) allowing, at a minimum, the following traffic:
  - Allow all traffic from and to Loopback adapter: `iptables -A INPUT -i lo -j ACCEPT`
  - Allow traffic from anywhere to SSH port: `iptables -A INPUT -p tcp --dport ssh -j`
  - Allow traffic from and to Vertica DB: `iptables -A INPUT -s [Vertica DB IP] -j ACCEPT`
  - Allow traffic from DNS servers:
    ```
    iptables -A INPUT -p udp --sport 53 -j ACCEPT
    iptables -A INPUT -p udp --dport 53 -j ACCEPT
    ```
  - Allow traffic to Operations Bridge Analytics web server:
    HTTP: `iptables -A INPUT -p tcp --dport 8080 -j ACCEPT`
    HTTPS: `iptables -A INPUT -p tcp --dport 8080 -j ACCEPT`

- If you do not have any other special requirements, drop all other traffic: I `iptables -A INPUT -j DROP`

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,

Securing Browsers

Internet Explorer, Chrome, and Firefox do not recognize `autocomplete=off` in web forms. As a result, when you log on to Operations Bridge Analytics you might be prompted to remember your log on credentials (depending on your browser configuration).

If you are an end user of Operations Bridge Analytics and do not want your log on credentials (user name and password) remembered, do the following:

- When prompted to store your log on credentials, acknowledge (to your browser) that you do not want your credentials saved by the browser.
- Often you can instruct your browser to stop prompting you to save credentials (for a given address).
- Often you can configure your browser to completely stop prompting you to save your passwords. If you prefer to disable this ability entirely, either configure this in the browser itself or work with your

IT organization to create and deploy a corporate IT policy.

> **Note:** See your browser documentation or contact your System Administrator for more details.

Other Security Considerations

Below are some other security items to consider:

- If you have multiple tenants, it is recommended that you use different Operations Bridge Analytics Collector hosts for each tenant. Doing so ensures data separation for each tenant.
- Deploy JBoss according to the security guidelines in your organization.
- Remove all external devices from your environment. These should include, but not be limited to, USB ports, CD drives, and other external media.
- Make it a regular habit to empty the temp drives on your servers.
- Keep your VMware tools updated.
- 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

This section includes:

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.

It is recommended 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 21.

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, run the following command to unregister the collector from the 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.

      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.

      iv. When queried if the user will be used for one AS process to connect to another AS process, select No.

   b. Run the `$OPSA_HOME/bin/opsa-server-manager.sh` script on 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.

      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.

      > **Note:** Set the self-signed certificate attributes, like `common name`, `country`, and `validity`, by editing the `/opt/HP/opsa/conf/ssl/cert/opsa-self-signedcert.template` file.

      iii. 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.src`.

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 **6: Restart OPSA server** to restart the Operations Bridge Analytics Server.

> **Note:** Your configuration changes will not occur unless the server is restarted. If you forget to restart the server before you exit, manually restart the server. If you receive an error, follow the instructions in the error messages.

j. Select option **7: Exit**.

> **Note:** In some cases, the `opsa-server` process fails to start after SSL is enabled. If this happens, execute `opsa-server status` to check if it is running. If it is not running, check if the `/opt/HP/opsa/log/opsa-server.log` file contains the following line:
>
> ```
> PBOX000368: Security Vault contains both covnerted (VAULT.dat) and pre-conversion data (ENC.dat). Try to delete /opt/HP/opsa/jboss/vault/ENC.dat file and start over again.
> ```
>
> If you find this message, delete the `/opt/HP/opsa/jboss/vault/ENC.dat`file and execute `opsa-server start`.

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. 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.**

> **Note:** Set the self-signed certificate attributes, like `common name`, `country`, and `validity`, by editing the `/opt/HP/opsa/conf/ssl/cert/opsa-self-signedcert.template` file.

iii. Select option **2: Generate a certificate signing request**. Choose the `opsa_server` alias. Save the certificate to `/tmp/opsa_collector_crf.src`.

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 **4: Restart OPSA Collector**.

i. Select option **5: Exit**.

4. **Reregister the OBA collector.**

a. 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. *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.

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, run the following command to unregister the collector from the 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.

   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.

b. Run the `$OPSA_HOME/bin/opsa-server-manager.sh` script on 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.

   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.

   > **Note:** Set the self-signed certificate attributes, like `common name`, `country`, and `validity`, by editing the `/opt/HP/opsa/conf/ssl/cert/opsa-self-signedcert.template` file.

   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.

c. 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.

d. Select the option **13: Go back to main menu**.

e. Select option **6: Restart OPSA server** to restart the Operations Bridge Analytics Server.

> **Note:** Your configuration changes will not occur unless the server is restarted. If you forget to restart the server before you exit, manually restart the server. If you receive an error, follow the instructions in the error messages.

f. Select option **7: Exit**.

> **Note:** In some cases, the `opsa-server` process fails to start after SSL is enabled. If this happens, execute `opsa-server status` to check if it is running. If it is not running, check if the `/opt/HP/opsa/log/opsa-server.log` file contains the following line:
>
> ```
> PBOX000368: Security Vault contains both covnerted (VAULT.dat) and pre-conversion data (ENC.dat). Try to delete /opt/HP/opsa/jboss/vault/ENC.dat file and start over again.
> ```
>
> If you find this message, delete the `/opt/HP/opsa/jboss/vault/ENC.dat` file and execute `opsa-server start`.

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. 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.**

   > **Note:** Set the self-signed certificate attributes, like `common name`, `country`, and `validity`, by editing the `/opt/HP/opsa/conf/ssl/cert/opsa-self-signedcert.template` file.

   b. 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.

   c. Select option **13: Go back to main menu**.

d. Select option **4: Restart OPSA Collector**.

e. Select option **5: Exit**.

4. **Reregister the OBA collector.**

   a. 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. *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.

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:

   ```
   /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 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:

   ```
   /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 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.

SSL for Kafka

This section includes:

Configuring SSL for Kafka

Complete the steps in "SSL for Servers and Collectors" on page 16 before enabling SSL for Kafka.

To configure Kafka for SSL, do the following on the Operations Bridge Analytics Server and Collector hosts you want to secure:

1. Edit the `/opt/HP/opsa/conf/opsa-config.properties` file as the opsa user.
2. Add the following line at the end of the file contents: `kafka.ssl.enabled=true`

   If you want to enable client authentication, also add the following line:

```
opsa.kafka.client.auth.enabled=true
```

3. Using the Source Type Manager graphical user interface, do the following for each configured collector:
   a. Select an existing source type that is located on the collector, for example, the Operations Agent source type.
   b. Select Stop Collecting and wait until the operation is finished.
   c. Select Start Collecting.
4. As the root user, run the following command on the Operations Bridge Analytics Server:
   ```
   $OPSA_HOME/bin/opsa stop
   ```
   ```
   $OPSA_HOME/bin/opsa start
   ```
5. As the root user, run the following commands on each Operations Bridge Analytics Collector host that you want to secure:
   ```
   $OPSA_HOME/bin/opsa stop
   ```
   ```
   $OPSA_HOME/bin/opsa start
   ```

Two-Way SSL for Accessing HPE 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.OPSACertStoreException:`
> `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:
   - **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`

- **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 opsaadmin user.

c. Choose **Option 2** to configure SSL.

d. Choose **Option 4** to import the trusted certificate into the OpsA 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`

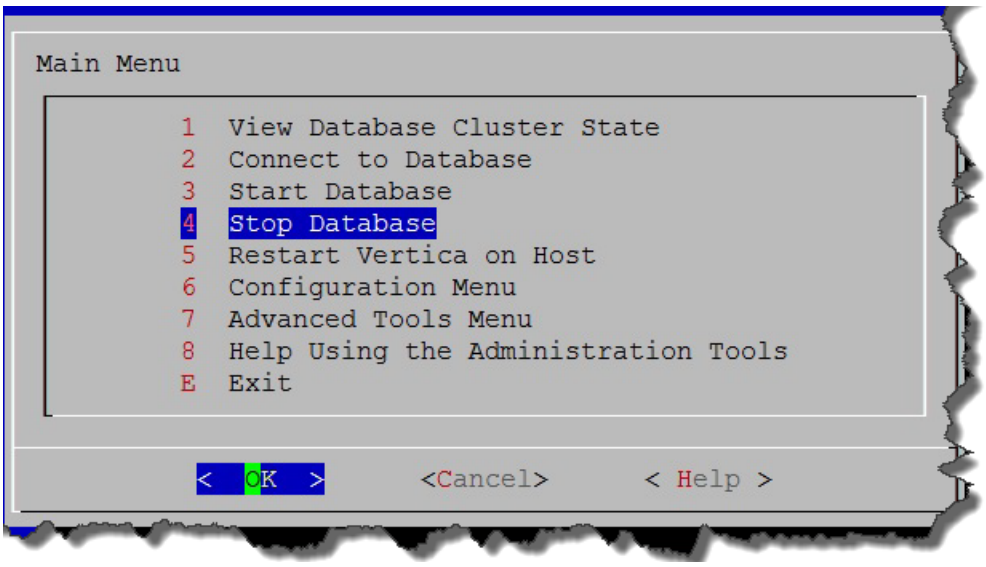
   Add the following lines; then save your work:

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

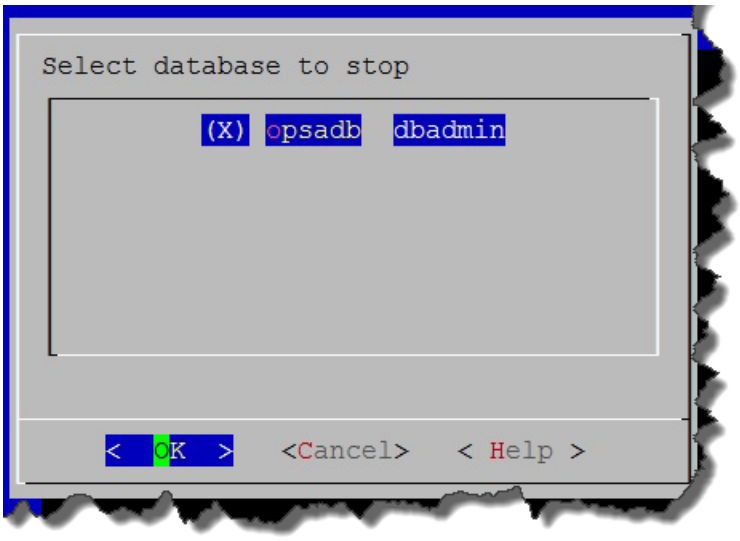
8. Complete the following steps to restart Vertica:

   a. Assuming the username for the database user is `dbadmin`: As `dbadmin` run `/opt/vertica/bin/adminTools`.

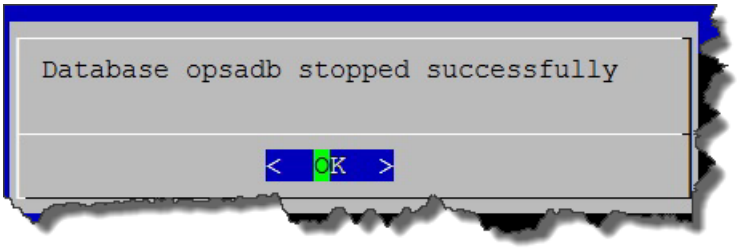
   b. Select **Stop Database**; then click **OK**.



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



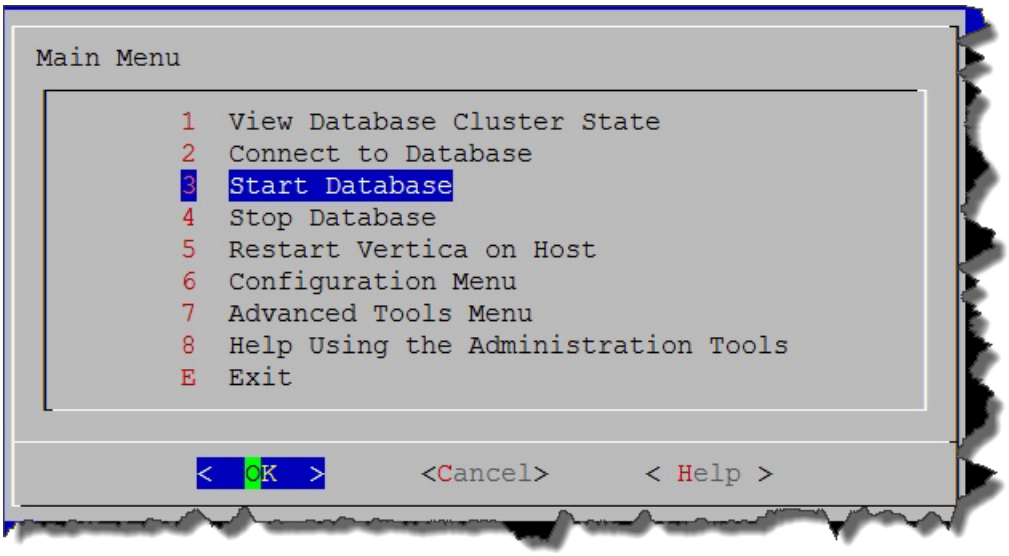
d. Look for the following message to make sure the database stopped; then click **OK** to go back to the main menu.



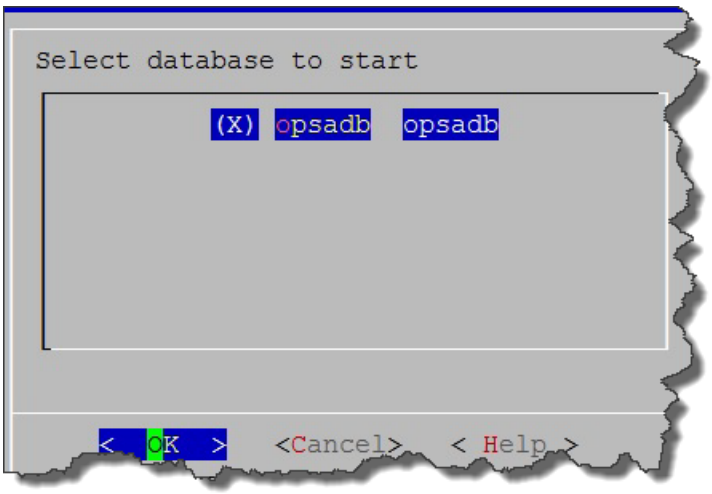
> **Note:** If users are still connected to the database, the **Stop Database** command might not work, as Vertica prevents it from shutting down. To stop the database anyway, do the following:
>
> i. Select the **Advanced Tools Menu**
>
> ii. Select **Stop Vertica on Host**
>
> iii. Select the host.

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

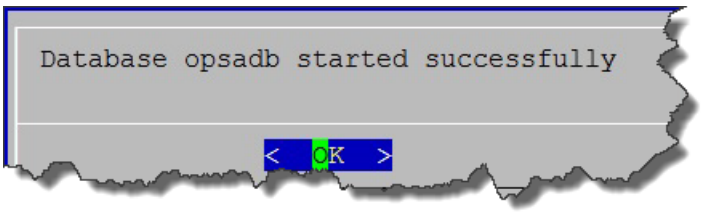
e. Select **Start Database**; then click **OK**.



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 36 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>
<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`

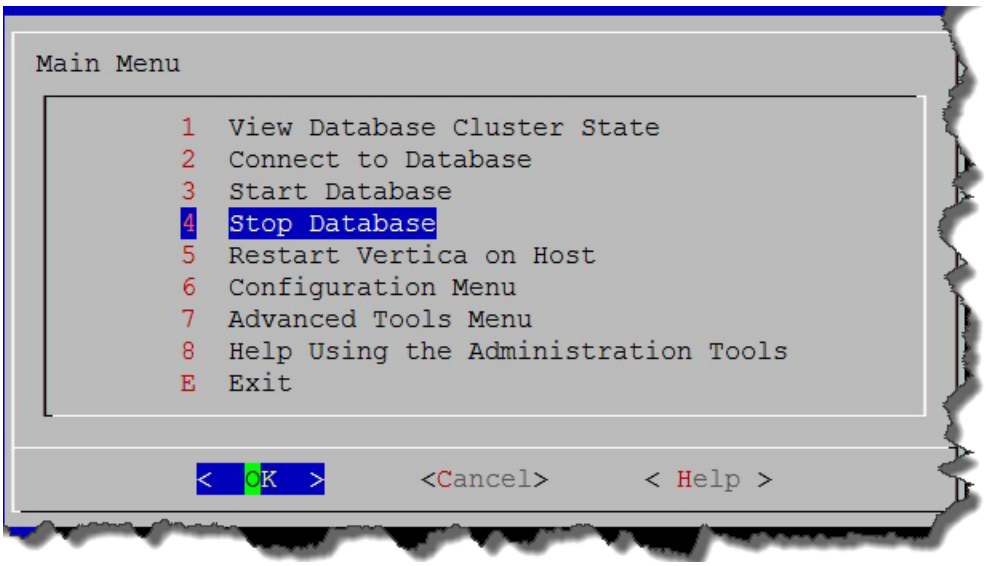
Search for text that resembles the following lines.
```
EnableSSL=1
ClientAuthentication = local all password
ClientAuthentication = hostssl all 0.0.0.0/0 password
```

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
```

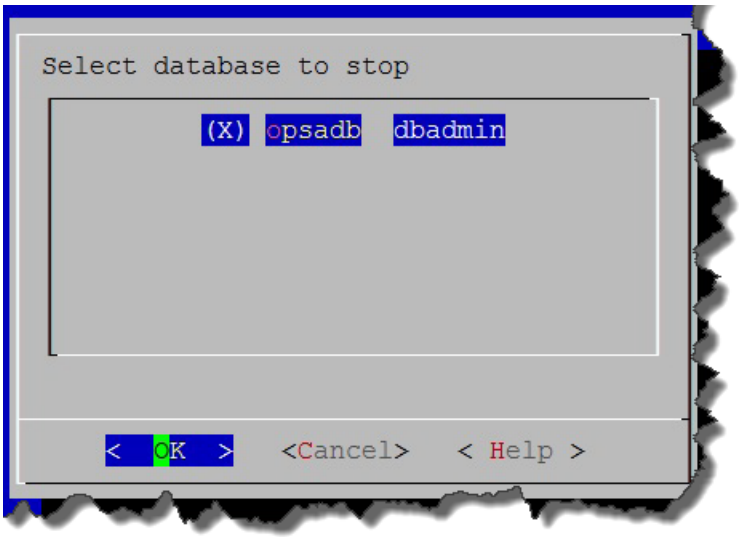
2. Complete the following steps to restart Vertica:

   a. Run `/opt/vertica/bin/adminTools`.

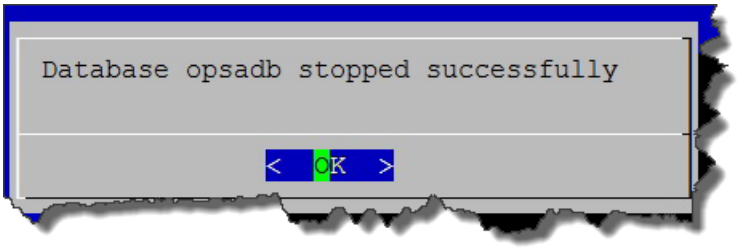
   b. Select **Stop Database**; then click **OK**.



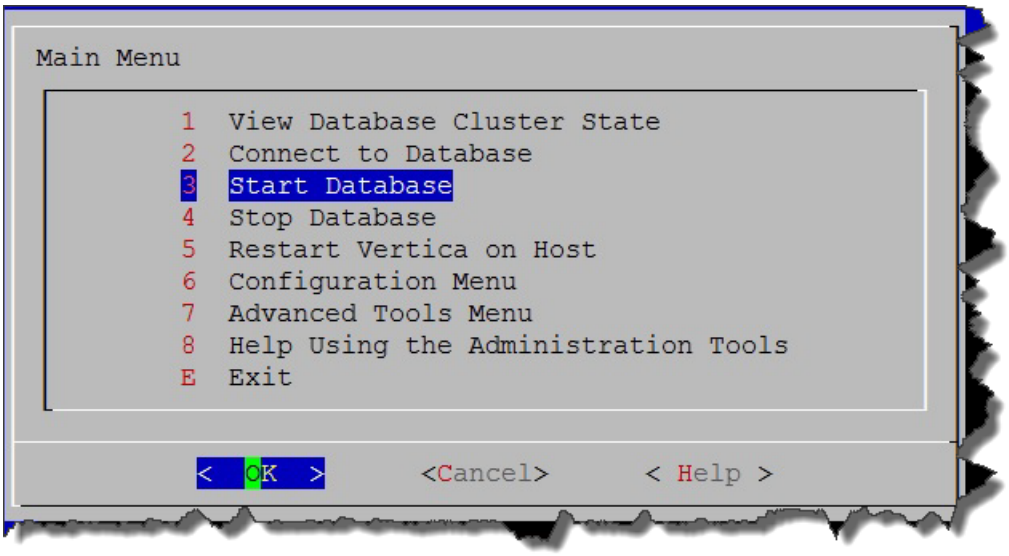
   c. Select the database you want to stop (opsadb); then click **OK**.



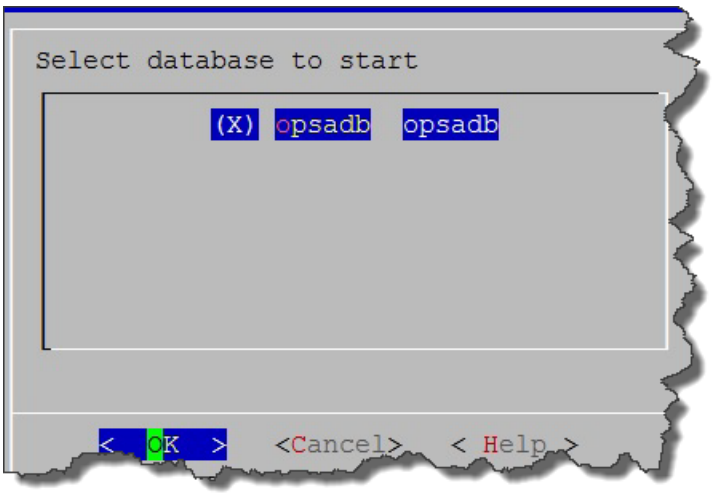
d. Look for the following message to make sure the database stopped; then click **OK** to go back to the main menu.



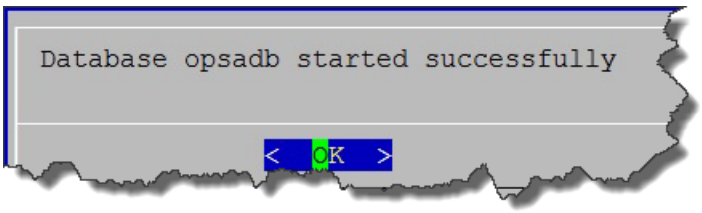
e. Select **Start Database**; then click **OK**.



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 34 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 42 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:** It is recommended 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 OpsA 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**. It is recommended 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.

> **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. 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** > **Admin** > **Platform** > **Users and Permissions** > **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 fully-qualified domain name of the Operations Bridge Analytics Server.
8. When prompted with **Enter trusted domains separated by comma**, enter the trusted domain names (separated by a comma). 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. This step is important to complete if, considering the example being shown in these steps, the BSM or OMi domain is not in the same domain in which the Operations Bridge Analytics Server resides.

   > **Note:** If you already enabled LWSSO and need to make LWSSO configuration changes, skip the instructions in this step.

   If this step is similar to the LWSSO configuration for your environment, complete the following:

a. Select the **Configure LWSSO** option.

b. From a browser, open the JMX console on the BSM or OMi server using the following syntax:

```
http://<FQDN of the BSM or OMi Server> :8080/jmx-
console/HtmlAdaptor?action=inspectMBean&name=Topaz%3Aservice%3DLW-
SSO+Configuration
```

c. Invoke the `addDNSDomainToTrustedHosts()` method and add the domain in which your Operations Bridge Analytics Server resides to the list.

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. 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 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. 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 6: LDAP Authentication

Configuring LDAP Authentication for Operations Bridge Analytics

The Operations Bridge Analytics console supports Lightweight Directory Access Protocol (LDAP) for user authentication. The instructions in this section explain how to configure Operations Bridge Analytics to connect to an LDAP server to validate Operations Bridge Analytics users. Only a Super Admin User, opsaadmin by default, can configure Operations Bridge Analytics to authenticate users through an LDAP Server.

> **Note:** When adding an LDAP authenticated user, Operations Bridge Analytics searches for the user being added in the configured LDAP server or servers. Operations Bridge Analytics adds the user only if it can find the user in one of the configured LDAP servers. If the user cannot be found in one of the configured LDAP servers, no user is added.

> **Note:** For a more automated method of configuring LDAP authentication for Operations Bridge Analytics, see *Configuring LDAP server Authentication for Operations Bridge Analytics* in the *Operations Bridge Analytics Help*.

The instructions in this section assume the following:

- One or more LDAP servers are presently configured and successfully being used in your environment.

  > **Note:** Operations Bridge Analytics does the following to authenticate users when multiple LDAP servers exist:
  >
  > - Operations Bridge Analytics does not contact LDAP servers in any specific order.
  > - Operations Bridge Analytics sequences through the LDAP servers until it successfully authenticates the user or it reaches the end of the list.

- You are able to log on to the Operations Bridge Analytics Server as a opsaadmin user.
- You have information about the LDAP credentials and its internal hierarchy (group structure).

When configuring this LDAP authentication, you can also enable SSL for LDAP server authentication. To do this, complete the steps shown in "Configuring SSL for LDAP Server Authentication" on the next page before continuing.

To configure Operations Bridge Analytics to authenticate users through an LDAP server, use a process similar to the following:

1. Run the following command to save the LDAP server configuration information to Operations Bridge Analytics:

   ```
   $OPSA_HOME/bin/opsa-ldap-configuration-manager.sh add --username <opsa_superadmin_username> --password <opsa_superadmin_password> --ldapusername <ldap_username> --ldappassword <ldap_password> --ldaphostname <ldap_hostname> --ldapbasedn <ldap_basedn> --ldapport <port> --userdn <userdn> --ssl <true | false> -groupbasedn <ldap_group_basedn> --groupAttribute <group_attribute> --userAttribute <user_attribute>
   ```

   > **Note:** The add option is used to add the LDAP server configuration information to Operations Bridge Analytics. All of the Operations Bridge Analytics users are authenticated by communicating to this LDAP server based on the additional configuration input. For example, notice the `ldap-basedn` and `userdn` attributes used in this example.

   > **Note:** When adding an LDAP authenticated user, Operations Bridge Analytics searches for the user being added in the configured LDAP server or servers. Operations Bridge Analytics adds the user only if it can find the user in one of the configured LDAP servers. If the user cannot be found in in one of the configured LDAP servers, no user is added.

   > **Note:** Only use the ssl option if you completed the steps shown in "Configuring SSL for LDAP Server Authentication" on the next page

   > **Note:** If you do not specify the optional LDAP integration username and LDAP integration user password during this LDAP configuration, `anonymous binding` must be enabled on the LDAP Servers.

   > **Note:** If you want to use the **optional** group attributes, `groupbasedn`, `groupAttribute`, and `userAttribute`, you must specify all three fields as shown in the example.

2. Run the following command to check that the LDAP information you added to Operations Bridge Analytics is accurate:

   ```
   $OPSA_HOME/bin/opsa-ldap-configuration-manager.sh list --username <opsa_superadmin_username> --password <opsa_superadmin_password>
   ```

3. Using **Users Manager** in the Operations Bridge Analytics console, create an Operations Bridge Analytics user that uses an LDAP server for authentication. In this case you do not need to create a password when creating this user.

   > **Note:** You must belong to either the Super Admin or Tenant Admin user group to access the Users Manager.

4. **Optional Step**: Using **LDAP Group Mapping** in the Operations Bridge Analytics console, provide mapping that enables automatic user profile creation in Operations Bridge Analytics after the LDAP Authentication during a user's first log on.

   > **Note:** You must belong to the Tenant Admin user group to access **LDAP Group Mapping**.

See the *opsa-ldap-configuration-manager.sh* and *opsa-ldap-group-mapping-manager.sh* reference pages (or the Linux man pages) for more information.

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" on page 56 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 OpsA 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. Choose **Option 6** from the main menu to restart the Operations Bridge Analytics Server.

g. Exit the `opsa-server-manager.sh` script.

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 theOperations 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 60.
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, we recommend 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 Operations Bridge Analytics Hardening Guide (Operations Bridge Analytics 3.00)

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!