Altair Engineering, Inc. makes no representation or warranties with respect to the contents of this manual or the associated software and especially disclaims any implied warranties of merchantability or fitness for any particular purpose. Further, Altair Engineering, Inc. reserves the right to revise this publication and make changes from time to time to its contents without obligation to notify anyone of such revisions or changes.

Altair Knowledge Hub Single Server software is offered and is to be used in accordance with a SOFTWARE LICENSE AND MAINTENANCE AGREEMENT. This agreement stipulates that this software be used only in the computer system designated in that agreement. The agreement further stipulates that the customer shall not copy or alter, or permit others to copy or alter, the software or related materials in whole or in part, in any media for any purpose, except to make an archive (back-up) copy or to make a copy as an essential step in the use of the software with the customer’s computer.

Altair Engineering, Inc. hereby grants the buyer the right to reprint this documentation for internal uses only. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, for any other purposes, without the prior written permission of Altair Engineering, Inc.

**Altair Knowledge Hub Single Server v2.3 Installation Guide**
Copyright © 2019 by Altair Engineering, Inc.
All rights reserved. Printed in the U.S.A.
Unpublished - Rights reserved under the copyright law of the United States.

Altair Knowledge Hub Single Server is a trademark of Altair Engineering, Inc. Other products mentioned herein may be trademarks or registered trademarks of their respective owners in the United States or other countries.

For U.S. Government End Users, the software is a “Commercial Item(s),” as that term is defined at 48 C.F.R. Section 2.101, consisting of “Commercial Computer Software” and “Commercial Computer Software Documentation,” as such terms are used in 48 C.F.R. Section 12.212 or 48 C.F.R. Section 227.7202, as applicable. Consistent with 48 C.F.R. Section 12.212 or 48 C.F.R. Sections 227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the Altair Software License and Maintenance Agreement.

**SALES INFORMATION**

**US:** + 1.800.445.3311  
**International:** + 1.978.441.2200

**Sales Email**

**US:** sales@datawatch.com  
**Europe:** sales_euro@datawatch.com  
**Asia Pacific:** sales_apac@datawatch.com

**SUPPORT CONTACT INFORMATION**

**Customer Portal:**  
https://support.datawatch.com

**Email:** support@datawatch.com  
**US:** +1 800.988.4739  
**International:** +1 978.275.8350

2.3.2/2019.08.23
# Table of Contents

**Altair Knowledge Hub Single Server Installation** ................................................. 1

Pre-Installation Steps .................................................................................................. 1
Pre-Installation Configuration ..................................................................................... 2
Installation .................................................................................................................. 3
Post-Installation Steps ............................................................................................... 4
  Checking the Installation Status .............................................................................. 4
  Installing JDBC Drivers .......................................................................................... 5
Logging ..................................................................................................................... 5
  Configuring the Logging Module .......................................................................... 6
  Configuring the Logging Driver ............................................................................ 6
  Installing the Logging Module .............................................................................. 7
  Deleting the Logging module ................................................................................. 7
  Web Application Logs ......................................................................................... 7
Elasticsearch Log Import and Export ........................................................................... 8

**Updating Knowledge Hub** ....................................................................................... 9

  Updating the Knowledge Hub Application .......................................................... 9
  Updating the Licensing Type of the Application .................................................... 9
  Deleting the Knowledge Single Server Application ......................................... 9

**Backing Up and Restoring the Application** .......................................................... 11

**Knowledge Hub Single Server Properties** ......................................................... 13

  Core-API.Properties .............................................................................................. 13
  Data-Engine-API.Properties ................................................................................ 15
  Social-API.Properties ........................................................................................... 18
Setting Up LDAP/SSO Authentication ..................................................................... 19
Volume Configuration ............................................................................................... 27
Utils Configuration .................................................................................................. 28
Memory Configuration ............................................................................................. 29

**Troubleshooting** .................................................................................................... 30

  Aggregating Status information ........................................................................... 30
  Cleaning the server application .......................................................................... 30
Altair Knowledge Hub Single
Server Installation

This installation guide describes how to install and deploy the Altair Knowledge Hub (formerly Datawatch Monarch Swarm) Linux Single Server application.

Note that prior to installing the application, the following must be ensured:

- Swap needs to be turned off and the swap partition commented out of /etc/fstab
- The user you are installing with needs to be in the admin/sudo group
- The machine should have a static IP and an entry in /etc/hosts
- All .sh files must have execute permissions. To update permissions, use the command:
  
  chmod +x setup-volumes.sh

Note also that an internet connection is required to install the application. Red Hat Enterprise Linux is not officially supported in the current version of Knowledge Hub because it does not support the community edition docker engine.

We strongly advise that all procedures to install Knowledge Hub Linux Single Server be completed by a knowledgeable system administrator.

Pre-Installation Steps

1. Download the installer from the link provided to you by Altair. This installer will come in a zipped file.

2. Unzip the folder and place its contents in a temp folder that you can easily access.

   The following subfolders should be included in the zipped folder.
   - \admin
   - \bin
   - \knowledgehub
   - \logging

3. If you intend to apply file licensing, ensure that you have a license file. The license file should be provided to you by Altair. License server information may be obtained from your system administrator.
If you intend to apply Hyper Works Units licensing, ensure that you have the correct license server port and license server port.

4. Download the necessary libraries from the link provided to you by Altair and then copy them to \bin\utils\libs.

Pre-Installation Configuration

The following configurations must be implemented prior to installing Knowledge Hub.

1. Edit ./knowledgehub/user-config/env.properties. Knowledge Hub has two preset configurations: 4x16 (4-core CPU, 16 Gb memory) or 8x32 (8-core CPU, 32 Gb memory). For actual deployments, Knowledge Hub Single Server requires a minimum configuration of 8x32, so this configuration must be specified. For testing purposes, the configuration 4x16 may be sufficient.

   ```
   SERVER_ENV=8x32
   ```

2. Specify the licensing type.
   - If you are using **File Licensing**, place the license file license.lic in ./knowledgehub/user-config/ folder.

   ```
   APPLICATION_LICENSE_REMOTE_HOST=<license server port>@<license server host>
   ```

   (e.g., **APPLICATION_LICENSE_REMOTE_HOST=6200@10.65.245.20**)

   Note that only one licensing system can be used at any one time.

3. Copy the Nginx certificates tls.key and tls.crt to the ./knowledgehub/user-config/ and logging/user-config folders. While your digital certificate and key may have different file names, we suggest renaming to tls.cert and tls.key to ensure smooth installation.

4. **(Optional)** Configure the necessary Knowledge Hub Single Server settings in the following files:
   - core-api.properties - Core configuration file
   - data-engine-api.properties - Data engine configuration file
   - social-api.properties - Social and machine learning configuration file
   - tableau-writer-api.properties - Tableau writer configuration file
   - krb5.conf - Kerberos configuration (for SSO)
For example, you can set the property `APPLICATION_SERVER_INTERNET_ADDRESS`, which is used to establish OAuth2 connections, such as Google Analytics, in `core-api.properties` and `data-engine-api.properties`.

**NOTE:** If you are deploying Knowledge Hub Single Server Edition for the first time, **DO NOT MODIFY** following properties:

- `APPLICATION_SECURITY_CIPHER_KEYPAIR_PRIVATEKEY`,
- `APPLICATION_SECURITY_CIPHER_KEYPAIR_PUBLICKEY` - In `core-api/properties` and `data-engine-api.properties`
- `APPLICATION_SECURITY_AUTHENTICATION_XAUTH_SECRET` - In `core-api.properties`, `data-engine-api.properties`, `social-api.properties`, and `tableau-writer-api.properties`

These properties will be updated in the config files during execution of the `linux-4-setup-single-server.sh` script.

5. **(Optional)** To configure custom volume locations, run the script `.setup-volumes.sh` in `.bin/utils`. Set `ROOT_FOLDER` in the script file (by default, `ROOT_FOLDER=/tmp`) and update `LIBS`, `FILE_LIBRARY`, `META_DB_DATA`, `SOCIAL_DB_DATA`, and `DATA_ENGINE_DB_DATA` if needed. The root folder stores the Knowledge Hub Data.

This step should be done before executing `.linux-4-setup-single-server.sh`

6. Open the following ports:
   - **80, 443** – Knowledge Hub Single Server application (8080: http; 8443: https)
   - **9000** - Docker Swarm administration console, Portainer
   - **5601** - Logging application, Kibana UI

**Installation**

Unless otherwise indicated, the following scripts must be run from the `.bin/` directory to install Knowledge Hub:

1. Run `./linux-0-install-docker.sh` to install Docker.
2. After running these scripts, log out and then log back into the server to re-evaluate your group membership and use Docker properly.
3. Run `./linux-1-configure-docker.sh` to setup Docker Swarm.
4. Run `./linux-2-setup-admin.sh` to install the Docker Swarm admin tool Portainer.
5. Run `./linux-3-setup-logging.sh` to install the logging manager, ELK Stack.
6. Run `setup-volumes.sh` from the `/utils` folder.
7. Run `./linux-4-setup-single-server.sh` to install the Knowledge Hub Single Server application

8. Upload the libraries to the server using the steps outlined [here](#).

# Post-Installation Steps

## CHECKING THE INSTALLATION STATUS

- **To check the status of installation**, run `docker stack ps <knowledgehub single server stack name>` (e.g., `docker stack ps knowledgehub`) from the `/bin` folder. This command displays all of the Knowledge Hub containers installed and their status.

- **To check whether services are running correctly**, run `docker stack services <knowledgehub single server stack name>` (e.g., `docker stack services knowledgehub`) from the `/bin` folder.

- **Wait several minutes** (e.g., 10 minutes) before launching the Knowledge Hub application in your browser. After the last script is executed, a number of other scripts are still being executed in the background. A “Bad Gateway 502” error may be returned if you access the URL for the application before these background scripts are completed.

Once installation is complete, the following URLs may be opened in your browser:

- **https://<server url>** – Knowledge Hub Single server application
- **https://<server url>:5601** – Logging application, Kibana UI
- **http://<server url>:9000** – Docker Swarm admin

**Note:** When running the Portainer application for the first time, set username/password and on next screen choose `Local` and `Connect`.
INSTALLING JDBC DRIVERS

To create connections to third-party applications such as Google BigQuery, SQL Server, and Amazon Redshift, the appropriate drivers must be obtained and uploaded to the /libs folder.

Steps:

1. Download the Altair Knowledge Hub Linux (JDBC) drivers from the link provided to you by Altair. The drivers will come in a zipped file.
2. Unzip the file and place its contents in ./bin/utils/libs.
3. Run the script ./bin/utils/linux-config.sh and then choose option 3.
4. Restart the Knowledge Hub services by running the script ./bin/utils/linux-config.sh and then choose option 9.

Users seeking to create custom connections using other drivers (i.e., those not currently included in the set of drivers provided by Altair) in Knowledge Hub should follow the steps above to do so. Note that the JDBC versions of these drivers must be used.

Logging

ELK Stack is used to aggregate and visualize logs.

- Kibana is a tool for visualizing log data
- ElasticSearch is a search and analytics data engine
- Fluentd is a data collector for unified logging layers

To use Kibana, you must define the Knowledge Hub index pattern fluentd-*, which is available by default. This configuration is described in the documentation Defining Your Index Patterns. After configuring the Knowledge Hub pattern, you can work with Knowledge Hub Single Server logs on the Discover page.

By default, all logs (time and source) from the whole cluster (from all namespaces) from the last 15 minutes are displayed. You can filter logs by date or any available field to view them more conveniently and add other log information if you wish. You can view detailed information for all logs in Document data view.
CONFIGURING THE LOGGING MODULE

The following steps must be accomplished to configure the logging module.

❑ Edit basic authentication credentials in "/logging/user-config/nginx_htpasswd" (default value is logs@logs)
❑ Copy the Nginx certificates tls.key and tls.crt to "/logging/user-config/
❑ Review/edit the curator job configuration in "/logging/user-config/curator_action.yml"
❑ To change scheduling for curator actions, update the cron expression in CURATOR_CRON in the "./logging/docker-compose.yml curator service environment (e.g., CURATOR_CRON: "*/5 * * * *" – job is run every 5th minute)

Note that:
❑ Default credentials (username/password) can be changed by application administrators in the config file.
❑ The default dashboard is by Metricbeats.
❑ Metrics for the System, File system, Docker Swarm, and PostgreSQL databases are available.

CONFIGURING THE LOGGING DRIVER

Knowledge Hub Single Server supports two log drivers: fluentd and json-file. By default, fluentd is used. To switch to json-file:

❑ Set the property LOGGING_DRIVER=json-file in "/knowledgehub/docker.properties"
❑ Set LOGGING_LOGSTASH_STDOUT=false in
  • "/knowledgehub/user-config/core-api.properties"
  • "/knowledgehub/user-config/data-engine-api.properties"
  • "/knowledgehub/user-config/social-api.properties"
  • "/knowledgehub/user-config/tableau-writer-api.properties"

Additional Information
Configure Logging Drivers | Docker Documentation
INSTALLING THE LOGGING MODULE

Execute the following in a terminal from ./bin/ directory to install the logging manager, ELK Stack:

```bash
./linux-3-setup-logging.sh
```

The logging module can be accessed through https://<server url>:5601

DELETING THE LOGGING MODULE

To delete the logging module, run:

```bash
docker stack rm logs
```

To delete logging data, run:

```bash
docker volume rm logs_esdata
```

WEB APPLICATION LOGS

You can view logs from any component of Knowledge Hub Single Server. To do so, add the LOGGING_LOGSTASH_STDOUT property to the config file of this component and then, in Kibana, filter logs according to the required component’s name.

Kibana also supports the import of pre-defined objects, such as Dashboards, Searches, and Visualization. These objects can be imported as JSON files. To make them part of your Kibana dashboard, perform the following steps:

1. Open the Kibana URL.
2. Click the Management tab at the left-hand portion of the screen.
3. Click the Saved Objects link.
4. Click the Import button.
5. In the opened window, select the JSON file of your object and then click Open.
6. Click the Yes, overwrite all objects button in the popup that displays.
Elasticsearch Log Import and Export

Knowledge Hub Single Server supports the export and import of logs stored in ElasticSearch:

To export logs, run the following script from ./bin/utils/:

```
./elastic-export.sh
```

This command supports the following arguments:

- `--from <date>` - date to start export from in ISO format. Default yesterday. Example 2019-01-01
- `--to <date>` - date to export to in ISO format. Default today's end of day. Example 2019-12-31
- `--dir <output directory>` - Directory to save exported file. Default to export sub directory

The resulting file will be named: `elastic-export-<datetime>.json.gz`

To import logs, run the following script from ./bin/utils/:

```
./elastic-import.sh --file <file name>
```

The command supports the following arguments:

- `--file <input_file>` - File to use as input for import. Should be in plain .gz format. Required
- `--esprefix <esprefix>` - Name to use as index prefix for imported file
Updating Knowledge Hub

UPDATING THE KNOWLEDGE HUB APPLICATION

The following steps are used to update an existing Knowledge Hub Single Server application to a newer version.

Steps:
1. Download and unzip a new Single Server Knowledge Hub archive.
2. Merge the license file (if any), certificate files (tls.crt, tls.key, knhub.key), and updated properties from the config files (core-api.properties, data-engine-api.properties, social-api.properties, tableau-writer-api.properties, krb5.conf, secrets.properties) to the new installer.
3. Run ./linux-4-setup-single-server.sh from the /bin directory.

UPDATING THE LICENSING TYPE OF THE APPLICATION

You can switch to HWU licensing from a file license when updating an existing Knowledge Hub application. To do so, open the knowledgehub/user-config/core-api.properties file and then set the property APPLICATION_LICENSE_REMOTE_HOST to '<license server port>@<license server host>' (e.g., APPLICATION_LICENSE_REMOTE_HOST=6200@10.65.245.20) and then run the command linux-4-setup-single-server.sh from the bin/ directory.

Note that only one licensing system can be implemented at any one time.

DELETING THE KNOWLEDGE SINGLE SERVER APPLICATION

To delete the Knowledge Hub Single Server application, run:

docker stack rm <knowledgehub single server stack name>
To delete the Docker Swarm server, run:

```bash
docker swarm leave --force
```

**Note:** If you cannot download Docker images, run `docker logout` and `./linux-1-configure-docker.sh`. 
Backing Up and Restoring the Application

Knowledge Hub Single Server supports the backup and restoration of the following components.

- social-db – the Cassandra databases
- meta-db – the PostgreSQL databases
- file-system – the file-libraries and libs docker volumes

To backup Knowledge Hub Single Server, run the following command from ./bin/utils/.

```
./linux-backup.sh
```

The components will be backed up in ./bin/utils/backup/<date_time> (e.g.: ./bin/utils/backup/2019-03-06_07-48-51).

After successful backup, you can find the following files in the backup folder:
dataengineapi_db.gz, newserver_db.gz, fs-file_library.tar, fs-libs.tar, newserver_keyspace.tar.gz, and datawatch_keyspace.tar.gz

To restore Knowledge Hub, run the following command from ./bin/utils/:

```
# stop services
./linux-config.sh # option 8

# restore backup
./linux-restore.sh <date_time>

# start services
./linux-config.sh # option 7
```

where <date_time> - backup folder name from ./bin/utils/backup/ (e.g., ./linux-restore.sh 2019-03-06_07-48-51)

**Note:** Cassandra backups do not allow restoration on empty volumes when migration is not preformed.
The following workflow is recommended:

1. Delete existing installation
2. Delete volumes
3. Perform new Installation
4. Restore backup
Knowledge Hub Single Server Properties

Use the following config files to configure various Knowledge Hub Single Server properties:

- core-api.properties
- data-engine-api.properties
- social-api.properties
- tableauewriter-api.properties

**Note:** Key properties should be in upper case and use '_' instead of '.' and '-' (e.g., spring.data.cassandra.enabled should be SPRING_DATA_CASSANDRA_ENABLED; application.server.internet-address should be APPLICATION_SERVER_INTERNET_ADDRESS.

**CORE-API.PROPERTIES**

The file core-api.properties specifies settings for the Knowledge Hub service.

The following table describes, in detail, the parameters that may be added to/modified in this configuration file.

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPRING_DATA_CASSANDRA_ENABLED</td>
<td>Accepts the values true or false. Enables (when true) or disables (when false) exports to the Library and exports of pinned data</td>
</tr>
<tr>
<td>SPRING_DATASOURCE_URL</td>
<td>Describes the connection to the Postgres database for the Knowledge Hub service</td>
</tr>
<tr>
<td>SPRING_DATASOURCE_URL_JDBC</td>
<td></td>
</tr>
<tr>
<td>SPRING_DATASOURCE_URL_USERNAME</td>
<td></td>
</tr>
<tr>
<td>SPRING_DATASOURCE_URL_PASSWORD</td>
<td></td>
</tr>
<tr>
<td>SPRING_HTTP_MULTIPART_MAXFILESIZE</td>
<td>Describes the maximum size of files that may be uploaded to the application (e.g., 2000MB)</td>
</tr>
<tr>
<td>SPRING_HTTP_MULTIPART_MAXREQUESTSIZE</td>
<td></td>
</tr>
<tr>
<td>SERVER_PORT</td>
<td>Port on which the application is running</td>
</tr>
<tr>
<td>SERVER_PORT_SSL_ENABLED</td>
<td>true if HTTPS is enabled</td>
</tr>
<tr>
<td>SERVER_PORT_SSL_KEY_STORE</td>
<td></td>
</tr>
<tr>
<td>PARAMETER</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SERVER_PORT_SSL_KEY_STORE_PASSWORD</td>
<td>Describe parameters for the SSL certificate</td>
</tr>
<tr>
<td>SERVER_PORT_SSL_KEY_PASSWORD</td>
<td></td>
</tr>
<tr>
<td>SERVER_TOMCAT_ACCESSLOG_ENABLED</td>
<td>These items describe settings for Tomcat logs:</td>
</tr>
<tr>
<td>SERVER_TOMCAT_ACCESSLOG_DIRECTORY</td>
<td>• <strong>buffered</strong> - Buffer output so that it is flushed periodically</td>
</tr>
<tr>
<td>SERVER_TOMCAT_ACCESSLOG_ACCEPT_COUNT</td>
<td>• <strong>pattern</strong> - Format pattern for access logs</td>
</tr>
<tr>
<td>SERVER_TOMCAT_ACCESSLOG_BUFFERED</td>
<td>• <strong>prefix</strong> - Log filename prefix</td>
</tr>
<tr>
<td>SERVER_TOMCAT_ACCESSLOG_PATTERN</td>
<td>• <strong>rename-on-rotate</strong> – Defer inclusion of the date stamp in the filename until rotate time</td>
</tr>
<tr>
<td>SERVER_TOMCAT_ACCESSLOG_RENAME_ON_ROTATE</td>
<td>• <strong>request-attributes-enabled</strong> – Set request attributes for IP address, hostname, protocol, and port used for the request</td>
</tr>
<tr>
<td>SERVER_TOMCAT_ACCESSLOG_REQUEST_ATTRIBUTES_ENABLED</td>
<td>• <strong>rotate</strong> – enable access log rotation</td>
</tr>
<tr>
<td>SERVER_TOMCAT_ACCESSLOG_ROTATE</td>
<td>• <strong>suffix</strong> – Log filename suffix</td>
</tr>
<tr>
<td>SERVER_TOMCAT_ACCESSLOG_SUFFIX</td>
<td></td>
</tr>
<tr>
<td>APPLICATION_SERVER INTERNET ADDRESS</td>
<td>Describes the redirect URL for login to Salesforce, Google Analytics, Google Adwords (should be identical to the URL specified for ClientId and ClientSecret for these connections), etc.</td>
</tr>
<tr>
<td>APPLICATION_HTTP_CACHE_TIMETOLIVEINDAYS</td>
<td>Describes the amount of time in days that may elapse before a data source’s cache times out</td>
</tr>
<tr>
<td>APPLICATION_DATA_ENGINE_STORE_DESIGN_MODE_LIMIT</td>
<td>Describes the row limit to be used for data sources in Design Mode; the default value is 10K</td>
</tr>
<tr>
<td>APPLICATION_DATA_ENGINE_SUGGESTION_PREPARE_CRON</td>
<td>Describes settings for jobs that calculate suggestions based on data type and content, e.g., 0 */30 * * * - jobs are run every 30 min</td>
</tr>
<tr>
<td>APPLICATION_DATA_ENGINE_API_URL</td>
<td>URL for internal communication between Knowledge Hub and Knowledge Hub Data Engine services (http://&lt;machine name&gt;:8081)</td>
</tr>
<tr>
<td>APPLICATION_DSL_SOURCE_CLEANER_CRON</td>
<td>Describes settings for jobs that delete temporary objects</td>
</tr>
<tr>
<td>APPLICATION_DSL_SOURCE_EXPIRATION_IN_HOURS</td>
<td></td>
</tr>
<tr>
<td>APPLICATION_DSL_TEMPORARY_ITEM_CLEANER_CRON</td>
<td></td>
</tr>
<tr>
<td>APPLICATION_DSL_TEMPORARY_ITEM_EXPIRATION_IN_HOURS</td>
<td></td>
</tr>
<tr>
<td>APPLICATION_DSL_PROCESS_RUN_CLEANER_CRON</td>
<td>Settings related to the job run cleaner</td>
</tr>
<tr>
<td>APPLICATION_DSL_PROCESS_RUN</td>
<td></td>
</tr>
</tbody>
</table>
### Knowledge Hub Linux Single Server v2.3 Installation Guide

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPLICATION_LICENSE_PROVIDER</td>
<td>Type of license provider; can be “local”, “remote”, or “hwu”</td>
</tr>
<tr>
<td>APPLICATION_LICENSE_LOCAL_FILEPATH</td>
<td>Path to license.lic file</td>
</tr>
<tr>
<td>APPLICATION_LICENSE_REMOTE_URL</td>
<td>URL to the remote server</td>
</tr>
<tr>
<td>APPLICATION_LICENSE_HWU_HOST</td>
<td>Altair License Server address. Should be written as “&lt;port&gt;@&lt;host&gt;”. Note that the URL to the Altair License Server should be set as an environment variable.</td>
</tr>
<tr>
<td>APPLICATION_LICENSE_HWU_CHECKER_CRON</td>
<td>Schedule to execute remote license pool check (e.g., 00/5 * * * *)</td>
</tr>
<tr>
<td>APPLICATION_LICENSE_HWU_GROUP</td>
<td>Name of group on Altair License Server (e.g., ${COMPUTERNAME}). Note that this property should also be set as an environment variable.</td>
</tr>
<tr>
<td>APPLICATION_LICENSE_HWU_LOG_ENABLED</td>
<td>Enable (true) or disable (false) hwu logging</td>
</tr>
<tr>
<td>APPLICATION_LICENSE_HWU_LOG_LEVEL</td>
<td>Level of hwu logging (e.g., info)</td>
</tr>
<tr>
<td>APPLICATION_LICENSE_HWU_LOG_FACILITY</td>
<td>Type of output (e.g., stderr)</td>
</tr>
<tr>
<td>APPLICATION_SCHEDULES_MONITORING_INTERVAL_INMINUTES</td>
<td>Number of minutes that must elapse before the next monitoring operation should be executed in a monitoring schedule</td>
</tr>
<tr>
<td>APPLICATION_SECURITY_AUTHENTICATION_FAILED_ATTEMPT_MIN_DELAY_SEC</td>
<td>Delay after the first failed login attempt (e.g., 8)</td>
</tr>
<tr>
<td>APPLICATION_SECURITY_AUTHENTICATION_FAILED_ATTEMPT_MAX_DELAY_SEC</td>
<td>Maximum delay time after a failed login attempt (e.g., 600)</td>
</tr>
</tbody>
</table>

### DATA-ENGINE-API.PROPERTIES

The file data-engine-api.properties specifies settings for the Knowledge Hub Data Service Engine service.

The following table describes, in detail, the parameters that may be added to this configuration file.

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPRING_DATA_CASSANDRA_ENABLED</td>
<td>Accepts the values true or false. Enables (when true) or disables (when false) exports to the Library and exports of pinned data</td>
</tr>
</tbody>
</table>
Describes the connection to the Postgres database for the Knowledge Hub service.

---

### Logback

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOGGING_FILE</td>
<td>full path to Data Engine service log file</td>
</tr>
<tr>
<td>LOGBACK_LOGLEVEL</td>
<td>Logging level of the Data Engine service log file</td>
</tr>
</tbody>
</table>

---

### Server

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SERVER_PORT</td>
<td>8081 – port on which the Data Engine is running</td>
</tr>
<tr>
<td>SERVER_PORT_SSL_ENABLED</td>
<td><code>true</code> if HTTPS is used.</td>
</tr>
<tr>
<td>SERVER_PORT_SSL_KEY_STORE</td>
<td>Describes parameters for the SSL certificate.</td>
</tr>
<tr>
<td>SERVER_PORT_SSL_KEY_STORE_PASSWORD</td>
<td>Describes parameters for the SSL certificate.</td>
</tr>
</tbody>
</table>

---

### Application

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPLICATION_DATA_ENGINE_SUGGESTION_RANK_THRESHOLD</td>
<td>Describes settings for suggestions based on data type and content; shows minimum rank for retrieving and sorting suggestions</td>
</tr>
<tr>
<td>APPLICATION_DATA_ENGINE_STORE_STATISTICS_AWAIT_TIMEOUT</td>
<td>Time to wait before statistics requests time out e.g., 60s</td>
</tr>
<tr>
<td>APPLICATION_DATA_ENGINE_STORE_DESIGN_MODE_LIMIT</td>
<td>Describes the row limit to be used for data sources in Design Mode; the default value is 10K</td>
</tr>
<tr>
<td>APPLICATION_DATA_ENGINE_STORE_GLOBALROWLIMIT</td>
<td>Row limit applied when the Design Mode limit is disabled e.g., 5000</td>
</tr>
<tr>
<td>APPLICATION_DATA_ENGINE_STORE_COLUMN_LIMIT</td>
<td>100 - column limit after Pivot and Transpose.</td>
</tr>
<tr>
<td>APPLICATION_DATA_ENGINE_STORE_DISTINCT_VALUE_LIMIT</td>
<td>250 - number of displayed distinct values limit</td>
</tr>
<tr>
<td>APPLICATION_DATA_ENGINE_STORE_LIMIT_DATA_NODES</td>
<td>Enables or disables limit to count of rows in all data nodes e.g., true (enabled); false (disabled)</td>
</tr>
<tr>
<td>APPLICATION_DATA_ENGINE_STORE_EXPORT_DATA_AWAIT_TIMEOUT_IN_SEC</td>
<td>3600 - export timeout</td>
</tr>
<tr>
<td>APPLICATION_IO_WRITER_COGNOS_HTTP_CLIENT_TIMEOUT</td>
<td>600 - timeout for connection to IBM Cognos Analytics</td>
</tr>
<tr>
<td>APPLICATION_SERVERINTERNETADDRESS</td>
<td>Redirect URL for logins to Salesforce, Microsoft Sharepoint, Google Analytics, Google BigQuery, Google Adwords, Google Drive (redirect url should be specified for ClientId and ClientSecret for Google connections).</td>
</tr>
<tr>
<td>APPLICATION_IO_READER_PREVIEW_LIMIT</td>
<td>1000 - row limit for previewing data sources</td>
</tr>
<tr>
<td>Configuration Settings</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>APPLICATION_IO_READER_JDBC_FETCH_SIZE</td>
<td>Describes the number of rows to fetch for a query to a database using JDBC drivers, e.g., 200</td>
</tr>
<tr>
<td>APPLICATION_IO_READER_JDBC_TIMEOUT_IN_SEC</td>
<td>Describes the time in seconds that may elapse before connections to JDBC drivers time out e.g., 60</td>
</tr>
<tr>
<td>APPLICATION_IO_READER_JDBC_DRIVER_*</td>
<td>Configuration settings for JDBC drivers</td>
</tr>
<tr>
<td>APPLICATION_IO_READER_JDBC_DRIVER_DEFAULT_LOGINTIMEOUT</td>
<td>Describes the time in seconds that may elapse before connections to JDBC drivers time out after login e.g., 60</td>
</tr>
<tr>
<td>APPLICATION_IO_READER_JDBC_DRIVER_DEFAULT_SOCKETTIMEOUT</td>
<td>Describes the time in seconds that may elapse before a socket timeout occurs when using connections to JDBC drivers e.g., 60</td>
</tr>
<tr>
<td>APPLICATION_IO_READER_JDBC_DRIVER_CDATA_JDBC_ALL_TIMEOUT</td>
<td>Describes the time in seconds that may elapse before all connections to JDBC drivers time out e.g., 60</td>
</tr>
<tr>
<td>APPLICATION_IO_READER_JDBC_DRIVER_COM_MYSQL_JDBC_DRIVER_USECURSORFETCH</td>
<td>Settings for mySQL JDBC driver</td>
</tr>
<tr>
<td>APPLICATION_IO_READER_JDBC_DRIVER_COM_MYSQL_JDBC_DRIVER_LOGINTIMEOUT</td>
<td>Settings for Oracle JDBC driver</td>
</tr>
<tr>
<td>APPLICATION_IO_READER_JDBC_DRIVER_ORACLE_JDBC_ORACLEDRIVER_ORACLE_NET_CONNECT_TIMEOUT</td>
<td>Settings for Presto JDBC driver</td>
</tr>
<tr>
<td>APPLICATION_IO_READER_JDBC_DRIVER_ORACLE_JDBC_ORACLEDRIVER_ORACLE_JDBC_READTIMEOUT</td>
<td>Settings for Apache Hive JDBC driver</td>
</tr>
<tr>
<td>APPLICATION_IO_READER_JDBC_DRIVER_COM_FACEBOOK_PRESTO_JDBC_PRESTODRIVER_SSL</td>
<td></td>
</tr>
<tr>
<td>APPLICATION_SECURITY_AUTHENTICATION_XAUTH_SECRET</td>
<td>security token, should be equal to all other security tokens in all other application config files</td>
</tr>
</tbody>
</table>
### SOCIAL-API.PROPERTIES

The file `social-api.properties` specifies settings for the Knowledge Hub Social and Machine Learning service.

The following table describes, in detail, the parameters that may be added to the configuration file.

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>APPLICATION_CORE_API_URL</strong></td>
<td>address for internal communication with the Knowledge Hub service</td>
</tr>
<tr>
<td><strong>READER</strong></td>
<td></td>
</tr>
<tr>
<td>READERS</td>
<td></td>
</tr>
<tr>
<td><strong>READER_PREVIEW_LIMIT</strong></td>
<td>1000 - row limit for preview data sources.</td>
</tr>
<tr>
<td><strong>REPORT</strong></td>
<td></td>
</tr>
<tr>
<td><strong>REPORT_TEXT_VIEW_MAX_CACHE_IN_MB</strong></td>
<td>This option sets the limit in megabytes for storing the converted reports.</td>
</tr>
<tr>
<td><strong>REPORT_TEXT_VIEW_MAX_CACHE_COUNT</strong></td>
<td>This option sets the limit in counts for storing the converted reports.</td>
</tr>
<tr>
<td><strong>REPORT_TEXT_VIEW_NUMBER_OF_PAGES</strong></td>
<td>If the page number of the report exceeds this setting, then conversion option converts from PDF reports to TXT report</td>
</tr>
<tr>
<td><strong>SERVER</strong></td>
<td></td>
</tr>
<tr>
<td><strong>SERVER_JWT_SECRET</strong></td>
<td>A security token that should be identical to all other security tokens indicated in all other application config files (e.g., application.security.authentication.xauth.secret in other config files)</td>
</tr>
<tr>
<td><strong>SERVER_PORT_SSL_ENABLED</strong></td>
<td>true if HTTPS is used.</td>
</tr>
<tr>
<td><strong>SERVER_PORT_SSL_KEYSTORE_PASSWORD</strong></td>
<td>Describes parameters for the SSL certificate.</td>
</tr>
<tr>
<td><strong>SERVER_PORT_SSL_KEYSTORE_PATH</strong></td>
<td></td>
</tr>
<tr>
<td><strong>SPARK</strong></td>
<td></td>
</tr>
<tr>
<td><strong>SPARK_APP_NAME</strong></td>
<td>Spark application name</td>
</tr>
<tr>
<td><strong>SPARK_APP_SCHEDULE</strong></td>
<td>Cron for Spark job for calculating suggestions (e.g., 0 0/20 * 1/1 * ? *)</td>
</tr>
<tr>
<td><strong>SPARK_APP_SCHEDULING_ENABLED</strong></td>
<td>False if only a single run is applied</td>
</tr>
<tr>
<td><strong>SPARK_DRIVER_MEMORY</strong></td>
<td>Allocated memory size for Spark service</td>
</tr>
<tr>
<td><strong>DATABASE</strong></td>
<td></td>
</tr>
<tr>
<td><strong>DATABASE_CASSANDRA_CONNECTION_ATTEMPTS_AMOUNT</strong></td>
<td>Number of attempts to connect to the Cassandra database</td>
</tr>
<tr>
<td><strong>DATABASE_CASSANDRA_CONNECTION_WAIT_TIME_SECONDS</strong></td>
<td>Number of seconds for each attempt to connect to the Cassandra database</td>
</tr>
<tr>
<td><strong>LOGGING</strong></td>
<td></td>
</tr>
<tr>
<td><strong>LOGGING_LOGLEVEL</strong></td>
<td>Logging level</td>
</tr>
<tr>
<td><strong>LOGGING_LOGFILEPATH</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Parameters

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full path to the ML and Spark services log file (e.g., C:\Windows\Temp\MonarchSwarm\Logs\ml-app.log)</td>
<td>Full path to the ML and Spark services log file (e.g., C:\Windows\Temp\MonarchSwarm\Logs\ml-app.log)</td>
</tr>
</tbody>
</table>

| NEXT_CHANGE_MIN_CHANGES | Minimum number of actions in sequence to generate suggestions |

---

### Setting Up LDAP/SSO Authentication

Execute the following steps to enable LDAP/SSO authentication.

**Steps:**

1. Install Knowledge Hub with default parameters.
2. Edit the Kerberos configuration file .:/knowledgehub/user-config/krb5.conf.

```bash
[libdefaults]
default_realm = <DOMAIN>
default_keytab_name = /keytab/linuxsso.keytab
forwardable=true
dns_lookup_realm = true
rdns = false
dns_lookup_kdc = true

[realms]
<DOMAIN> = {
    kdc = <name of domain controller>.<domain>:88
    admin_server = <name of domain controller>.<domain>:88
}

[domain_realm]
.<domain> = <DOMAIN>

[appdefaults]
kinit = {
    renewable = true
    forwardable= true
}
```
For example, if the full computer name of the domain controller is **WIN-LDAPSERVER** and the domain name is **altair.com**: 

```ini
[libdefaults]
default_realm = ALTAIR.COM
default_keytab_name = /keytab/linuxsso.keytab
forwardable = true
dns_lookup_realm = true
rdns = false
dns_lookup_kdc = true

[realms]
ALTAIR.COM = {
kdc = WIN-LDAPSERVER.altair.com:88
admin_server = WIN-LDAPSERVER.altair.com:88
}

[domain_realm]
altair.com = ALTAIR.COM
.altair.com = ALTAIR.COM

[appdefaults]
kinit = {
renewable = true
forwardable = true
}
```

3. **Add JAVA_OPTS to the core-api.configuration.**

   ```
   JAVA_OPTS=-Djava.security.krb5.conf=/sso/krb5.conf -Dsun.security.krb5.debug=true
   ```

4. **Generate a linuxsso.keytab and replace this keytab in .knowledgehub/user-config/linuxsso.keytab.**

   **Additional Information**

   ktpass | Microsoft Docs All you need to know about Keytab files.

   For example, if the full computer name of the Knowledge Hub server is **WIN-SWARMSERVER** and the domain name is **altair.com**, run the following script in Powershell:

   ```
   setspn -A HTTP/WIN-SWARMSERVER.altair.com knhubsingle
   ktpass /out c:\temp\linuxsso.keytab /mapuser knhubsingle@ALTAIR.COM /princ HTTP/WIN-SWARMSERVER@ALTAIR.COM /pass Password# /ptype KRB5_NT_PRINCIPAL /crypto All
   ```

5. **Check the principal in the keytab file in linux: klist -k -t linuxsso.keytab.**

   The result should contain a valid principal and the same principal should be in core-api.properties.
6. Configure `./knowledgehub/user-config/core-api.properties` as follows.

**For SSO Authentication**

```
JAVA_OPTS=-Djava.security.krb5.conf=/sso/krb5.conf -Dsun.security.krb5.debug=true
APPLICATION_SECURITY_AUTHENTICATION_PROVIDER=ldap <available values: basic, ldap, oauth2>
APPLICATION_SECURITY_AUTHENTICATION_USERS_PROVISIONED=false
APPLICATION_SECURITY_AUTHENTICATION_DEFAULT_PASSWORD=<default password for users created through LDAP and added multiple users>
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SSO_ENABLED=true
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SSO_SERVICE_PRINCIPAL=HTTP/<full computer name of Knowledge Hub server>/',@<DOMAIN NAME>
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SSO_KEY_TAB_LOCATION=<path of keytab file>
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SSO_REQUEST_REGEX=^/api/.+/ldap_sso
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_LOGIN=userPrincipalName
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_FIRST_NAME=givenname
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_LAST_NAME=sn
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_COMMON_NAME=cn
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_EMAIL=mail
APPLICATION_SECURITY_AUTHENTICATION_LDAPQUERY_ATTRIBUTE_MAPPING_PHONE_NUMBER=telephoneNumber
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_GROUPS=memberOf
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_CUSTOM_ATTRIBUTES='["displayName","distinguishedName","name","objectCategory","objectClass","primaryGroupID","sAMAccountName","sAMAccountType","servicePrincipalName"]'
APPLICATION_SECURITY_AUTHENTICATION_LDAP_ACTIVE_DIRECTORY=true
APPLICATION_SECURITY_AUTHENTICATION_LDAP_DOMAIN=<DOMAIN>
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SERVER=ldap://<full computer name of LDAP server>/<domain name>/
APPLICATION_SECURITY_AUTHENTICATION_LDAP_MANAGE_DN=<LDAP admin user>
APPLICATION_SECURITY_AUTHENTICATION_LDAP_MANAGE_PASSWORD=<password of admin user>
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SEARCH_BASE=DC=<domain component 1>,DC=<domain component 2>
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SEARCH_FILTER=(
(userPrincipalName={0}) (sAMAccountName={0}))
APPLICATION_SECURITY_AUTHENTICATION_LDAP_USER_ROLES=3
APPLICATION_SECURITY_AUTHENTICATION_LDAP_ADMIN_USERS=<admin user1>, <admin user2>
```
For example, if the full computer name of the Knowledge Hub server is **WIN-SWARMSERVER**, the LDAP server is **WIN-LDAPSERVER**, and the domain name is **altair.com**:

```
JAVA_OPTS=-Djava.security.krb5.conf=/sso/krb5.conf -Dsun.security.krb5.debug=true
APPLICATION_SECURITY_AUTHENTICATION_PROVIDER=ldap
APPLICATION_SECURITY_AUTHENTICATION_USERS_PROVISIONED=false
APPLICATION_SECURITY_AUTHENTICATION_DEFAULT_PASSWORD=Passw0rd#
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SSO_ENABLED=true
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SSO_SERVICE_PRINCIPAL=HTTP/WIN-SWARMSERVER.altair.com/@ALTAIR.COM
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SSO_KEY_TAB_LOCATION=/keytab/linuxss.ks.keytab
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SSO_REQUEST_REGEX=/api/+/ldap_sso
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_LOGIN=userPrincipalName
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_FIRST_NAME=givenname
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_LAST_NAME=sn
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_COMMON_NAME=cn
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_EMAIL=mail
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_PHONE_NUMBER=telephoneNumber
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_GROUPS=memberOf
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_CUSTOM_ATTRIBUTES='["displayName","distinguishedName","name","objectCategory","objectClass","primaryGroupID","sAMAccountName","sAMAccountType","servicePrincipalName"]'
APPLICATION_SECURITY_AUTHENTICATION_LDAP_ACTIVE_DIRECTORY=true
APPLICATION_SECURITY_AUTHENTICATION_LDAP_DOMAIN=ALTAIR.COM
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SERVER=ldap://WIN-LDAPSERVER.altair.com/
APPLICATION_SECURITY_AUTHENTICATION_LDAP_MANAGE_DN=swaradmin@altair.com
APPLICATION_SECURITY_AUTHENTICATION_LDAP_MANAGE_PASSWORD=#Passw0rd#
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SEARCH_BASE=DC=altair,DC=com
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SEARCH_FILTER=(| (userPrincipalName={0}) (sAMAccountName={0}))
APPLICATION_SECURITY_AUTHENTICATION_LDAP_GROUP_MAPPING=true
APPLICATION_SECURITY_AUTHENTICATION_LDAP_ROLE_MAPPING=true
APPLICATION_SECURITY_AUTHENTICATION_LDAP_ROLESMAP_1=Accounting,Finance
APPLICATION_SECURITY_AUTHENTICATION_LDAP_ROLESMAP_2=BusDev,Sales
APPLICATION_SECURITY_AUTHENTICATION_LDAP_USER_ROLES=3
APPLICATION_SECURITY_AUTHENTICATION_LDAP_ADMIN_USERS=mbarnes@altair.com,tjones@altair.com
```
For LDAP Authentication

JAVA_OPTS=-Djava.security.krb5.conf=/sso/krb5.conf -Dsun.security.krb5.debug=true
APPLICATION_SECURITY_AUTHENTICATION_PROVIDER=ldap <available values: basic, ldap, oauth2>
APPLICATION_SECURITY_AUTHENTICATION_USERS_PROVISIONED=false
APPLICATION_SECURITY_AUTHENTICATION_DEFAULT_PASSWORD=<default password for users created through LDAP and added multiple users>
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_LOGIN=userPrincipalName
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_FIRST_NAME=givenname
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_LAST_NAME=sn
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_COMMON_NAME=cn
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_EMAIL=mail
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_PHONE_NUMBER=telephonenumber
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_GROUPS=memberOf
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_CUSTOM_ATTRIBUTES='["displayName","distinguishedName","name","objectCategory","objectClass","primaryGroupID","sAMAccountName","sAMAccountType","servicePrincipalName"]'
APPLICATION_SECURITY_AUTHENTICATION_LDAP_ACTIVE_DIRECTORY=true
APPLICATION_SECURITY_AUTHENTICATION_LDAP_DOMAIN=<DOMAIN>
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SERVER=ldap://<full computer name of LDAP server>.<domain name>/
APPLICATION_SECURITY_AUTHENTICATION_LDAP_MANAGE_DN=<LDAP admin user>
APPLICATION_SECURITY_AUTHENTICATION_LDAP_MANAGE_PASSWORD=<password of admin user>
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SEARCH_BASE=DC=<domain component 1>,DC=<domain component 2>
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SEARCH_FILTER=(| (userPrincipalName={0}) (sAMAccountName={0}) )
APPLICATION_SECURITY_AUTHENTICATION_LDAP_USER_ROLES=3
APPLICATION_SECURITY_AUTHENTICATION_LDAP_ADMIN_USERS=<admin user1>,<admin user2>

For example, if the full computer name of the Knowledge Hub server is WIN-SWARMSERVER, the LDAP server is WIN-LDAPSERVER, and the domain name is altair.com:
Each of the properties added to the core-api configuration file is described as follows:

<table>
<thead>
<tr>
<th>PROPERTY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPLICATION_SECURITY_AUTHENTICATION_PROVIDER=ldap</td>
<td>Use ldap for LDAP/SSO; may also be basic for basic or oauth2 for OAuth2 authentication</td>
</tr>
<tr>
<td>APPLICATION_SECURITY_AUTHENTICATION_USERS_PROVISIONED=false</td>
<td>Enables (true) or disables (false) explicit provisioning. If explicit provisioning is disabled, the system creates Knowledge Hub users automatically. When set to true, users must be created manually</td>
</tr>
<tr>
<td>PROPERTY</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>APPLICATION_SECURITY_AUTHENTICATION_DEFAULT_PASSWORD</td>
<td>The default password for new users created through LDAP and added multiple users</td>
</tr>
<tr>
<td>APPLICATION_SECURITY_AUTHENTICATION_SSO_ENABLED</td>
<td>true to enable SSO; false if using LDAP authentication</td>
</tr>
<tr>
<td>APPLICATION_SECURITY_AUTHENTICATION_SSO_SERVICE_PRINCIPAL</td>
<td>Full computer name of the Knowledge Hub server in the form HTTP/&lt;COMPUTER NAME&gt;.&lt;domain&gt;@&lt;DOMAIN&gt; (e.g., HTTP/WIN-SWARMSERVER.altair.com@ALTEN.COM)</td>
</tr>
<tr>
<td>APPLICATION_SECURITY_AUTHENTICATION_SSO_KEY_TAB_LOCATION</td>
<td>Path to keytab file (e.g., /keytab/linuxsso.keytab)</td>
</tr>
<tr>
<td>APPLICATION_SECURITY_AUTHENTICATION_SSO_REQUEST_REGEX</td>
<td>^/api/.+/ldap_sso - Setting for SSO</td>
</tr>
<tr>
<td>APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_LOGIN</td>
<td>Attributes used to add users by LDAP query</td>
</tr>
<tr>
<td></td>
<td>USERPRINCIPALNAME</td>
</tr>
<tr>
<td></td>
<td>FIRST_NAME: GIVENNAME</td>
</tr>
<tr>
<td></td>
<td>LAST_NAME: SN</td>
</tr>
<tr>
<td></td>
<td>COMMON_NAME: CN</td>
</tr>
<tr>
<td></td>
<td>EMAIL: MAIL</td>
</tr>
<tr>
<td></td>
<td>PHONE_NUMBER: TELEPHONENUM</td>
</tr>
<tr>
<td></td>
<td>GROUPS: MEMBEROF</td>
</tr>
<tr>
<td>APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_CUSTOM_ATTRIBUTES</td>
<td>DISPLAYNAME</td>
</tr>
<tr>
<td></td>
<td>DISTINGUISHEDNAME</td>
</tr>
<tr>
<td></td>
<td>NAME</td>
</tr>
<tr>
<td></td>
<td>OBJECTCATEGORY</td>
</tr>
<tr>
<td></td>
<td>OBJECTCLASS</td>
</tr>
<tr>
<td></td>
<td>PRIMARYGROUPID</td>
</tr>
<tr>
<td></td>
<td>SAMACCOUNTNAME</td>
</tr>
<tr>
<td></td>
<td>SAMACCOUNTTYPE</td>
</tr>
<tr>
<td></td>
<td>SERVICEPRINCIPALNAME</td>
</tr>
<tr>
<td>APPLICATION_SECURITY_AUTHENTICATION_LDAP_ACTIVE_DIRECTORY</td>
<td>true when AD is used</td>
</tr>
<tr>
<td>APPLICATION_SECURITY_AUTHENTICATION_LDAP_DOMAIN</td>
<td>Domain name</td>
</tr>
<tr>
<td>PROPERTY</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>APPLICATION_SECURITY_AUTHENTICATION_LDAP_DOMAIN_USERS</td>
<td>Allow LDAP authentication for any of two forests in one domain. The default value for this setting is <code>false</code>. To authenticate users from just one domain via LDAP, set this property to <code>true</code> and then set the correct domain in the property <code>APPLICATION_SECURITY_AUTHENTICATION_LDAP_DOMAIN</code>.</td>
</tr>
<tr>
<td>APPLICATION_SECURITY_AUTHENTICATION_LDAP_SERVER</td>
<td>Full computer name of LDAP server</td>
</tr>
<tr>
<td>APPLICATION_SECURITY_AUTHENTICATION_LDAP_MANAGE_DN</td>
<td>User name and password to use to connect to LDAP server when <code>SSO_ENABLED = false</code> and <code>LDAP_ACTIVE_DIRECTORY = false</code>. If <code>SSO_ENABLED = true</code> and <code>LDAP_ACTIVE_DIRECTORY = true</code>, these properties may be omitted from the config file. These credentials are also used to add multiple users to Knowledge Hub using LDAP query.</td>
</tr>
<tr>
<td>APPLICATION_SECURITY_AUTHENTICATION_LDAP_MANAGE_PASSWORD</td>
<td></td>
</tr>
<tr>
<td>APPLICATION_SECURITY_AUTHENTICATION_LDAP_SEARCH_BASE</td>
<td>Domain name components (e.g., DC=altair,DC=com if domain is altair.com).</td>
</tr>
<tr>
<td>APPLICATION_SECURITY_AUTHENTICATION_LDAP_SEARCH_FILTER</td>
<td>Filter used to search for LDAP users.</td>
</tr>
<tr>
<td>APPLICATION_SECURITY_AUTHENTICATION_LDAP_USER_ROLES</td>
<td>User role(s) for SSO users.</td>
</tr>
<tr>
<td>APPLICATION_SECURITY_AUTHENTICATION_LDAP_ADMIN_USERS</td>
<td>List of users automatically created with the Super Administrator role in Knowledge Hub (if <code>USERS_PROVISIONED = false</code>). When this list is provided, there is no need to login as an administrator and create the first LDAP user.</td>
</tr>
<tr>
<td>APPLICATION_SECURITY_AUTHENTICATION_LDAP_ROLEMAPPING</td>
<td><code>true</code> to enable role-mapping in Knowledge Hub; <code>false</code> to disable.</td>
</tr>
<tr>
<td>APPLICATION_SECURITY_AUTHENTICATION_LDAP_GROUPMAPPING</td>
<td><code>true</code> to enable group-mapping in Knowledge Hub; <code>false</code> to disable.</td>
</tr>
<tr>
<td>APPLICATION_SECURITY_AUTHENTICATION_LDAP_ROLESMAP</td>
<td>Mapping of Knowledge Hub roles to LDAP groups.</td>
</tr>
</tbody>
</table>

Notes:
- The property `APPLICATION_SECURITY_AUTHENTICATION_LDAP_SEARCH_FILTER` uses the format "username@domain".
- If a user does not specify the domain in the login form, the value in `APPLICATION_SECURITY_AUTHENTICATION_LDAP_DOMAIN` will be used as the domain.
- LDAP search attributes should have values in "username@domain" format.
• If the property `USERS_PROVISIONED` is set to `TRUE`, and the user is not included in the `ADMIN_USERS` list, an error (i.e., “Users %user_login% does not exist”) is returned when the user logs into the application via SSO. In this case, the user must be manually added through the User Management page (via LDAP) of Knowledge Hub.

• If the property `USERS_PROVISIONED` is set to `FALSE`, and the user exists in Active Directory, a new user is created upon login to Knowledge Hub via SSO. This user’s profile will include a login, last name, and first name, and s/he will have the role(s) specified in `USER_ROLES`.

• If the user exists in Active Directory, and the new user is included in the `ADMIN_USERS` list, the user can log into Knowledge Hub via SSO and this user will have the role Super Administrator regardless if the property `USERS_PROVISIONED` is set to `TRUE` or `FALSE`.

To enable role/group mapping, set the following properties:

• `APPLICATION_SECURITY_AUTHENTICATION_LDAP_ROLEMAPPING` – `true` to enable role mapping; `false` otherwise

• `APPLICATION_SECURITY_AUTHENTICATION_LDAP_GROUPMAPPING` - `true` to enable group mapping; `false` otherwise

• `APPLICATION_SECURITY_AUTHENTICATION_LDAP_ROLESMAP %role_id1%: "%GroupName1, GroupName2%“` – Mapping of first Knowledge Hub role to LDAP groups

• `APPLICATION_SECURITY_AUTHENTICATION_LDAP_ROLESMAP %role_id2%: "%GroupName1, GroupName2%“` – Mapping of second Knowledge Hub role to LDAP groups

7. After configuration, restart all services and then launch Knowledge Hub.

**Volume Configuration**

To deploy Single Server Knowledge Hub to custom volume locations, the following steps are performed:

1. Open the `.bin/utils/setup-volumes.sh` file for and then set the `ROOT_FOLDER` property to a folder to which you have access (e.g., `ROOT_FOLDER=/home/<user>`). Note that by default, `ROOT_FOLDER=/tmp`.

2. (Optional) Update paths for the properties `LIBS`, `FILE_LIBRARY`, `META_DB_DATA`, `SOCIAL_DB_DATA`, and `DATA_ENGINE_DB_DATA` if needed.

3. Save changes to the `.bin/utils/setup-volumes.sh` file and then run `.setup-volumes.sh` from the `.bin/utils` directory. Doing so creates the required docker volumes.
4. Run `./linux-4-setup-single-server.sh` from the `.bin` directory. Knowledge Hub Single Server will be deployed to the pre-configured volumes.

**Utils Configuration**

To configure the Knowledge Hub Single Server application, run `./bin/utils/linux-config.sh` and then select:

- 1 – Libs-Is
  - Show libs from the shared `/libs` folder

- 2 – Libs-download
  - Download libraries on the local machine to the `.bin/utils/libs` from the shared `/libs` folder

- 3 – Libs-upload
  - Upload libraries from the local machine folder `.bin/utils/libs` to the shared `/libs` folder. After execution of this command, all services must be restarted to apply changes.

- 4 – Libs-remove
  - Removes libraries from the shared `/libs` folder. After execution of this command, all services must be restarted to apply changes.

- 5 – License-update
  - Before execution, copy a new version of `license.lic` to the folder `.knowledgehub/user-config/`

- 6 – Certificate-update
  - Before execution, copy new versions of `tls.crt` and `tls.key` to the folder `.knowledgehub/user-config/`

- 7 – Start services
  - Start all API services in Docker Swarm.

- 8 – Stop services
  - Stop all API services in Docker Swarm.

- 9 – Restart services
  - Stop and start all API services in Docker Swarm.

- 10 – Exit
  - Exit the utils menu.
Memory Configuration

The Knowledge Hub Single Server application has two predefined CPU/memory configurations: 4x16 or 8x32.

To change configuration options, modify:

- 4x16 - ./knowledgehub/docker-compose.4x16.yml
- 8x32 - ./knowledgehub/docker-compose.8x32.yml

Knowledge Hub Single Server requires a minimum configuration of 8x32, so this configuration must be used. To change the default configuration, edit the properties of SERVER_ENV in ./knowledgehub/user-config/env.properties.

To configure resources for each service, modify the following parameters:

```yaml
reservations:
    cpus: '0.25'
    memory: 100M

limits:
    cpus: '2.0'
    memory: 4100M
```

**IMPORTANT:** CPU and memory limits must be added to all services.

To apply the new configuration, run ./linux-4-setup-single-server.sh.
Troubleshooting

AGGREGATING STATUS INFORMATION

- **Export all logs.** Navigate to `./bin/utils` and run:

  ```bash
  ./elastic-export.sh --from 2019-01-01
  ```

  Archive all folders in `./bin/utils/export-*` with exported logs and attach to email/ticket for support.

CLEANING THE SERVER APPLICATION

- **Delete the Knowledge Hub deployment by running** `docker stack rm knowledgehub`

- **Wait 2–3 minutes, delete the volume** `docker volume prune`, **and check** `docker volume ls`. The following volumes should be deleted: `data-engine-db-data`, `meta-db-data`, `social-db-data`, `file_library`, and `libs`.

- **To install Knowledge Hub Single Server, run** `./linux-4-setup-single-server.sh`. 