opentext™

ALM Octane

Software version: 24.3

Installation Guide for Linux

Go to Help Center online

https://admhelp.microfocus.com/octane/

Document release date: July 2024

Send Us Feedback

Let us know how we can improve your experience with the Installation Guide for Linux.

Send your email to: admdocteam@opentext.com

Legal Notices

Contents

Architecture

You can set up OpenText™ ALM Octane as a single node, or in a cluster configuration. The following diagrams illustrate the system architecture for both options.

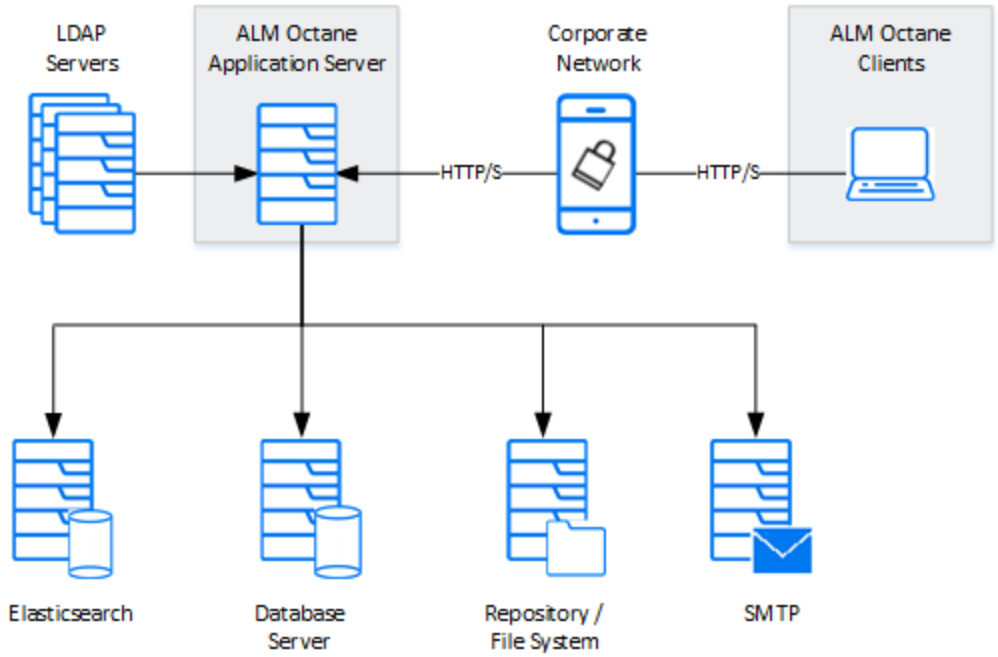
These are followed by descriptions of each of the components.

- "Basic configuration" below
- "Enterprise configuration" on the next page
- "Components" on page 8

Basic configuration

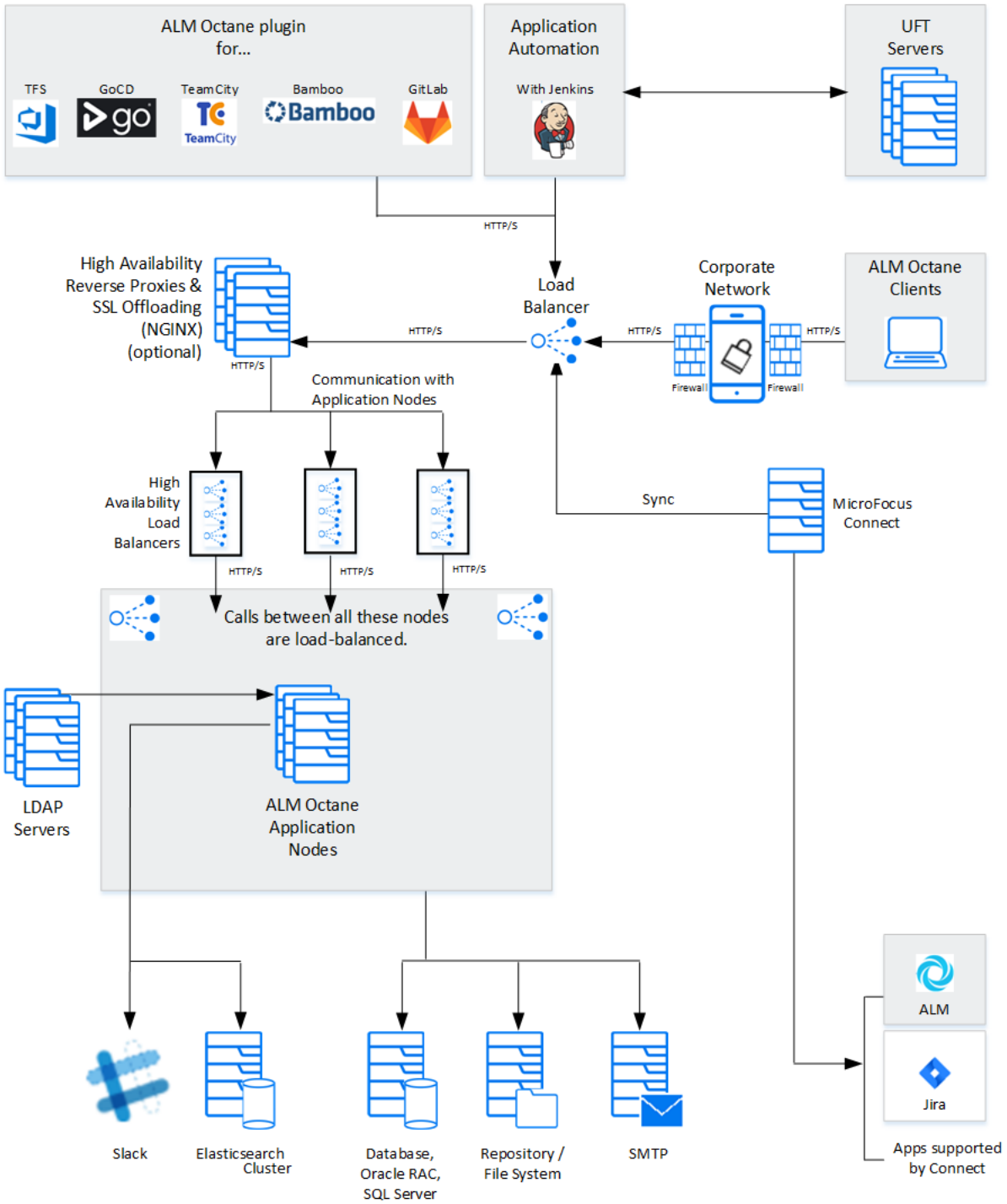
The following diagram illustrates the system architecture of a single-node configuration. Components in gray are OpenText products.

> **Note:** The ALM Octane, database, and Elasticsearch servers should each reside on separate machines.



Enterprise configuration

The following diagram illustrates the system architecture of an enterprise, cluster configuration. Components in gray are OpenText products.



Components

Components	Description
ALM Octane clients	The clients communicate with the ALM Octane server over HTTP/S.
ALM Octane Server application nodes	Client requests from ALM Octane are dispatched to the deployed application. **Note:** The ALM Octane, database, and Elasticsearch servers should each reside on separate machines.
ALM Octane application additional cluster (sync) nodes	**Cluster configuration**: A cluster is a group of application servers that run as a single system. Each application server in a cluster is referred to as a "node." • All nodes must have access to the database server on which the site database schema resides. • All nodes must have access to the repository. Generally, the repository is located on an NFS or SAN server. If the repository is not located on a remote, dedicated machine, the repository location cannot be **/opt/octane**. • All nodes must have access to each other.
Repository / File system	Stores all files to be used by all the projects in the system, such as templates and attachments. **Cluster configuration**: When working in a clustered configuration, the repository must be accessible by all nodes. Also, the repository must be configured to use the same mount point (path) on all nodes.

Components	Description
Database server	A relational database management system, either Oracle RAC or Microsoft SQL Server. The database server stores the following schemas: • **Site schema**. Stores all site-related information, such as database servers, cluster nodes, the SMTP servers, and configuration. • **Space schema**. All space information, such as workspaces, users, and roles. This server can be shared with other applications with the following constraints: • The database must be able to sustain the load of all the applications. • Future versions of ALM Octane might require a database upgrade. This may necessitate migration of data if other applications sharing the same database do not support the database version that ALM Octane requires. **Note:** The ALM Octane, database, and Elasticsearch servers should each reside on separate machines.
Elasticsearch server (or cluster)	A Java-based, open-source search engine. This component is used for various aspects of the application, such as global search and trends. This server can be shared with other applications with the following constraints: • The Elasticsearch engine must be able to sustain the load of all the applications. • Future versions of ALM Octane might require an Elasticsearch upgrade. This may necessitate migration of data if other applications sharing the same Elasticsearch do not support the Elasticsearch version that ALM Octane requires. **Note:** The ALM Octane, database, and Elasticsearch servers should each reside on separate machines. A working Elasticsearch server is a requirement for working with ALM Octane. Make sure you are using a version supported by ALM Octane: For the supported version, see Database and Elasticsearch in the ALM Octane Help Center.

Components	Description
Load balancer	**Cluster configuration**: When working with a load balancer, client requests are transmitted to the load balancer and distributed according to server availability within the cluster. If you are using a load balancer, we recommend you utilize SSL offloading.
High availability load balancers	**Cluster configuration**: These can be "VIPs" (virtual IP addresses) of one physical load balancer.
DMZ	An optional, demilitarized zone.
High availability reverse proxies and SSL offloading	**Cluster configuration**: Optional configuration for load balancing using a software solution (for example, NGINX).
SMTP	A mail server.
Jenkins (with ALM Octane plugin)	**Enterprise configuration**: You can integrate ALM Octane with a Jenkins CI server using the Application Automation Tools Plugin on your CI server.
TFS, TeamCity, or Bamboo server (with ALM Octane plugin)	**Enterprise configuration**: You can integrate ALM Octane with a TFS, TeamCity, or Bamboo CI server using the Application Automation Tools Plugin on your CI server.
Slack	Integration with Slack, which enables all stakeholders of a backlog item to collaborate and communicate. You can integrate with Slack by adding it as a collaboration tool associating it with a workspace.
Open Text testing tools: UFT Developer, UFT One, LoadRunner Cloud, LoadRunner Enterprise	You can integrate ALM Octane with Open Text testing tools. For details, see Integrations overview in the ALM Octane Help Center.

Installation types

This document describes the necessary requirements and procedures for the installation of ALM Octane server, and initial setup steps.

Type	Description
Installation	Instructions for installing on: • A single node. For details, see "Installation flow" on page 14. • A cluster configuration. For details, see "Cluster installation flow" on page 17.
Docker installation	A simplified installation of ALM Octane by deploying a Docker image. For details, see "Install ALM Octane using a Docker image" on page 64.
Upgrade	For details, see Upgrade in the Help Center.

Licensing flow

This topic provides a high-level flow for setting up your trial license.

Overview

To get started with ALM Octane, you begin with a 90-day on-premises free trial for 100 users. You can then install an ALM Octane license file, or allocate licenses from ALM or ALM.

Before you begin a trial, you should be familiar with the different editions of ALM Octane. ALM Octane is available in Enterprise and Pro Editions. For details, see ALM Octane editions in the ALM Octane Help Center.

Request a trial

Submit a request for a free trial here: https://www.microfocus.com/en-us/products/alm-octane/free-trial.

When you first start using ALM Octane, you automatically receive a **Trial** license which gives you a 90-day trial for 100 users.

By default, your trial is Enterprise Edition, which allows one shared space. If you create a shared space in an Enterprise Edition trial and then install a license for Pro Edition, the trial shared space should not be used in a production environment since the sharing capabilities may not be supported in future releases.

Using Pro Edition

There is no Pro Edition trial.

To work with Pro Edition:

1. Install ALM Octane Enterprise Edition as your trial type, but do not create shared spaces. If you create a shared space during an Enterprise Edition trial

and then install a Pro Edition license, the shared space is deactivated.

2. Get an evaluation Pro Edition license from your Sales account manager, or create a support ticket for a one-time evaluation license.
3. In the ALM Octane Settings area, apply your Pro Edition license. For details about applying licenses, see "Installing a license" below.

Installing a license

After you install and configure your trial instance of ALM Octane, you can purchase licenses for Enterprise or Pro Edition. You then install your license key (.dat file) in ALM Octane.

Alternatively, you can allocate your current licenses from ALM or ALM and share them with ALM Octane. Licenses can be allocated from ALM (ALM.Net) Edition to ALM Octane Enterprise Edition, or from Quality Center (QC) Enterprise Edition to ALM Octane Pro Edition.

> **Note:** You can share up to 15% of your licenses from ALM or ALM, or up to 150 licenses, the lower of the two.

To learn more, see Manage licenses in the ALM Octane Help Center.

Next steps:

- "Installation flow" on the next page

Installation flow

This document describes the overall flow for installing the ALM Octane server on Linux.

This section includes:

Prerequisites

Verify your system meets hardware and software requirements.

This includes setting up permissions, opening ports, database configuration, and more.

You need three separate server machines.

- ALM Octane server
- Database server
- Elasticsearch server

For details, see "Prerequisites" on page 20.

> **Note:** We recommend you review security considerations in ALM Octane Secure Deployment and Configuration Guidelines. This contains instructions on how to set up a secure configuration for ALM Octane.

Deploy

Deploy ALM Octane on a machine dedicated for the ALM Octane server on Linux.

ALM Octane is deployed using the RPM Package Manager (as an .rpm file).

The deployment path is /**opt/octane**.

The command to deploy is: `rpm -Uvh <name of the RPM file>`

For details, see "Deploy ALM Octane" on page 33.

Configure

This section describes how to configure.

To configure:

1. Edit the **octane.conf** file with your site's settings for initial configuration.
2. (Optional) Depending on your needs, configure optional configuration files:
   - **elasticsearch-security.conf** to configure secure Elasticsearch.
   - **proxy.conf** to use a proxy server.
   - **ldap.conf** to use LDAP authentication.
   - **sso.conf** to use SSO authentication.

   The path to these files is **<Repository folder>/conf**.

For details, see "Configure site settings" on page 37.

Start the server

Start the ALM Octane server:

```
systemctl start octane
```

For details, see "Start the ALM Octane server" on page 61.

Log in

Verify that ALM Octane was properly installed. For details, see "Checking logs" on page 90.

Log into ALM Octane. For details, see "Log in to ALM Octane" on page 63.

Configure cluster (optional)

After starting the server on the first machine, configure and initialize each additional cluster node. For details, see "Cluster installation flow" on the next page.

Next steps:

- "Prerequisites" on page 20
- "Deploy ALM Octane" on page 33
- "Configure site settings" on page 37

Cluster installation flow

This section provides end-to-end instructions for installing an on-premises ALM Octane server in a cluster configuration on Linux. A cluster is a group of application servers that run as a single system. Each application server in a cluster is referred to as a "node."

To install ALM Octane in a cluster configuration:

1. For each node in the cluster, check requirements and access:

Check requirements	Verify that the all cluster nodes, including the first, meet all requirements and prerequisites. For details, see "Prerequisites" on page 20.
Check database server access	All cluster nodes, including the first, must have access to the database server on which the site database schema resides.
Check repository access	Create an environment variable **OCTANE_REPOSITORY_DIR.** The repository directory has to be a shared directory visible to all cluster nodes. All nodes must have read and write access to the repository. Generally, the repository is located on an NFS or SAN server. The repository must be configured to use the same mount point (path) on all nodes. It is important that you enter the repository path using the same path name on all nodes.
Check access between nodes	All nodes must have access to each other. Verify ports are open in your firewall. ALM Octane needs to communicate between the nodes in the cluster on port 5701. Therefore, make sure that your firewall enables communication between the nodes of the cluster on the specified port.. By default, outbound ports are open. Check inbound ports.

2. Install ALM Octane on the first cluster node, as described in "Installation" on page 33.

a. Verify that you have created an environment variable **OCTANE_REPOSITORY_DIR**, as described above. If this variable is missing, the installation will fail.

b. Deploy the ALM Octane installation files on to the first node.

c. Configure initial site settings in **octane.conf** and optional configuration files.

- Make sure to set the **database server name** to a value that all cluster nodes can access.
- Enter values described in "Cluster settings" on page 45.

  ALM Octane validates these settings when starting. If they are not valid, the ALM Octane server does not start.

d. On the first node only, start the ALM Octane server by running **systemctl start octane**. See "Start the ALM Octane server" on page 61.

3. (Optional) If you want to set up a secure configuration for ALM Octane, follow the instructions in ALM Octane Secure Deployment and Configuration Guidelines.
4. Log in to the first node in the cluster. For details, see "Log in to ALM Octane" on page 63.
5. Download and deploy the ALM Octane package on each cluster node. For details, see "Deploy ALM Octane" on page 33 and "Deploy in cluster environment" on page 36.

> **Caution:**
> - Do not configure **octane.conf** or other configuration files on the nodes.
> - Do not run **connectnode.sh** scripts.

6. On each other node, start ALM Octane by running **systemctl start octane**.

   Each node is automatically configured using the configuration files located in the repository, as defined when you configured the first node.
7. (Optional) If you want to set up a secure configuration for ALM Octane in a cluster configuration, follow these instructions on each other node: ALM Octane Secure Deployment and Configuration Guidelines.

8. Log in to make sure ALM Octane is running on each other node. For details, see "Log in to ALM Octane" on page 63. Use the load balancer URL when you log in.

   > **Tip:** For best performance, configure your load balancer with round-robin (stateless) configuration.

9. If you need to make changes in configuration settings later, edit the **<Repository folder>/conf\octane.conf** file, and not **octane.conf.new**, which is a temporary file that is for internal use only. After modifying these settings, restart the ALM Octane server on each node to pull the configuration changes from the repository.

Troubleshooting:

If the cluster was not properly defined, you may receive an error message when you start the ALM Octane server:

```
Cluster is unhealthy...
```

During installation, values in the hazelcast.xml file change according to the octane.conf configuration. The configuration of the hazelcast.xml file is the one that controls the cluster behavior.

Make sure that the **member** element of the hazelcast.xml file contains the same values that were defined in the **nodes** section of the octane.conf file.

Next steps:

- "Prerequisites" on the next page
- "Deploy ALM Octane" on page 33
- "Configure site settings" on page 37

Prerequisites

Verify that your system meets the requirements listed below, and the detailed Support matrix in the ALM Octane Help Center.

For security requirements, see the ALM Octane Secure Deployment and Configuration Guidelines.

This section includes:

Checklist

Use the following questions to make sure you are ready to install.

Category	Tell us...	Your answer...
ALM OCTANE	On which machine are you going to install ALM Octane?	
	Does the machine have a Quad Core AMD64 processor or equivalent x86-compatible processor?	
	How much memory does the machine have? You need a minimum of 8 GB.	
	What Linux operating system is on the machine?	
	What is the user name and password you are going to use for the installation user?	
	Does the installation user have **sudo** permissions?	
	Are your browsers and screen resolutions compatible with ALM Octane?	
	On-premises installation of ALM Octane supports only English characters for the names of schemas, operating systems, users, and so on. Did you check?	

Category	Tell us...	Your answer...
elastic	Does your Elasticsearch version match ALM Octane requirements? See Support matrix in the ALM Octane Help Center.	
	Do you need to download Elasticsearch? If you haven't installed Elasticsearch, you can download from here: https://www.elastic.co/downloads/past-releases#elasticsearch	
	On which machine is Elasticsearch installed?	
	Did you make sure that the port for outbound communication to Elasticsearch is open? By default, outbound ports are open.	
	Did you make sure that the Elasticsearch ports (such as 9300 and 9200) are accessible directly from the ALM Octane server, not just by checking the HTTP connection?	
	What is the name of the Elasticsearch cluster you have configured?	
	Is the Elasticsearch accessible from the ALM Octane server?	
	Was Elasticsearch configured according to ALM Octane requirements? These are described in detail in "Configure Elasticsearch" on page 30.	

Category	Tell us...	Your answer...
ORACLE	Does your Oracle version match ALM Octane requirements? See Support matrix in the ALM Octane Help Center.	
	On which machine is the database installed?	
	What is the Oracle database port? Default: 1521 You can modify the port in the **connection-string** field in **octane.conf**.	
	Did you make sure that the port for outbound communication to Oracle is open? By default, outbound ports are open.	
	What is the URL for Java Database Connectivity (JDBC) for your database?	
	What is the database admin's user name and password?	
	Does the database admin power user have the necessary permissions? See "Oracle database permissions" on page 25.	
	What table space and temporary table space can be used?	
	Did the DBA add any objects to the schemas? If so, create an exception file before installing. For details, see "Using exception files for manual database changes" on page 79.	

Category	Tell us...	Your answer...
Microsoft	Does your SQL Server version match ALM Octane requirements? See Support matrix in the ALM Octane Help Center.	
	On which machine is the database installed?	
	Are you going to use the SQL Server database port or instance name to connect to the database? • What is the SQL Server database port? Default: 1433 • What is the SQL Server instance name?	
	What is the database admin's user name and password?	
	Does the database administrator (power user) have the necessary permissions? See "SQL database permissions" on page 27.	
	What MSSQL database login user, and password, can be used for ALM Octane?	
	Did the DBA add any objects to the databases/schemas? If so, create an exception file before installing. For details, see "Using exception files for manual database changes" on page 79.	
Java	Do you need to install the JDK on the ALM Octane server and other servers, such as the ElasticSearch server?	
	Does your Java version match ALM Octane requirements? See Support matrix in the ALM Octane Help Center.	
jetty://	Did you make sure that the port for inbound communication with Jetty is open? By default, the port is 8080. For SSL, 8443. You can define the port during initial installation, in **octane.conf**.	

Category	Tell us...	Your answer...
	Did you make sure that ALM Octane can communicate between the nodes in the cluster, using inbound and outbound communication for clusters? By default, the port is 5701. You can define the port during initial installation, in **hazelcast.xml**.	

File system permissions

- Root or sudo user.
- During deployment, ALM Octane creates a user and group named **octane** for running the **octane** service that starts the ALM Octane server. However, if your organization prefers to manage users in a centralized way, without enabling ad hoc creation of local users, create a user and group for this purpose, and define the following environment variables: **OCTANE_USER** and **OCTANE_GROUP**.

  Make sure the user has write permissions to the **/opt/octane/log** directory.
- If you are using Linux SUSE 15.4, make sure you have the **sysvinit-tools** package manager installed.

Oracle database permissions

Permissions depend on how you want to install ALM Octane. Do you want ALM Octane to create schemas, objects, and tables during installation, or do you want your DBA to prepare them?

Refer to the relevant section for your installation scenario:

- "Allow ALM Octane to create Oracle schemas automatically" on the next page
- "Create your own Oracle schemas for ALM Octane" on the next page

Allow ALM Octane to create Oracle schemas automatically

To enable ALM Octane to create schemas, tables, and objects automatically during the installation, provide ALM Octane with an Oracle power user with the following admin privileges:

- CREATE USER
- CREATE SESSION WITH ADMIN OPTION
- CREATE TABLE WITH ADMIN OPTION
- CREATE SEQUENCE WITH ADMIN OPTION
- DROP USER (optional). If not provided, the DBA must take responsibility for cleaning up unnecessary schemas.

> **Note:** These permissions are for the user you specify in the **admin-user > name** setting in the **octane.conf** file.
>
> When defining your site action in the **octane.conf** file, you specify **CREATE_NEW**. For details, see "CREATE_NEW" on page 43.

This power user can also be created temporarily, for installation purposes only. You can remove this user if:

- The installation is complete, and login to ALM Octane is successful.
- The ALM Octane site admin intends to create spaces using an existing schema, which can be selected when creating a space in the ALM Octane Settings area for the site. For details, see Manage spaces - site admins in the ALM Octane Help Center.

Create your own Oracle schemas for ALM Octane

If you do not want ALM Octane to create schemas, tables, and objects automatically, perform the following:

1. Before installation, create two schemas with the same password.
2. Provide ALM Octane with a regular Oracle user with the following permissions, for both the site and space schemas:

- CREATE TABLE
- CREATE SESSION
- CREATE SEQUENCE
- The QUOTA clause on the user's default tablespace should be unlimited.

> **Note:** During installation when you define the **octane.conf** file, you should enter the name of the site schema in **schemas > site**, the space schema in **schemas > initial-shared-space**, and the password in **schema-password**.
>
> When defining your site action in the **octane.conf** file, you need to specify **FILL_EXISTING**. For details, see "FILL_EXISTING" on page 43.

SQL database permissions

Permissions depend on how you want to install ALM Octane. Do you want ALM Octane to create databases during the installation, or do you want your DBA to prepare them?

Refer to the relevant section for your installation scenario:

- "Allow ALM Octane to create SQL databases automatically" below
- "Create your own SQL databases for ALM Octane" on the next page

Allow ALM Octane to create SQL databases automatically

To enable ALM Octane to create databases automatically during the installation, use the **sa** user, or an ALM Octane database admin power user.

Install ALM Octane with a database admin power user if you cannot use the SQL **sa** user for security reasons. This user can be a temporary user, for installation purposes only.

Request that the SQL Server database admin create a temporary power user with the following privileges (roles), which are required to install ALM Octane:

- Database Creators **dbcreator** role
- Security Administrator **securityadmin** role

> **Note:** These permissions are for the user you specify in the **admin-user > name** setting in the **octane.conf** file.
>
> When defining your site action in the **octane.conf** file, you need to specify **CREATE_NEW**. For details, see "CREATE_NEW" on page 43.

It is important that the ALM Octane database administrative user is not the same as the ALM Octane admin user. The SQL Server database admin could name this power user **octane_install_power_user**, for example. For details on removing this temporary power user, see "Handle database-related issues" on page 67.

Create your own SQL databases for ALM Octane

Before installation, create two databases: one for the site and one for the space.

Associate the login user to 'octane' user in both databases.

The default collation is **SQL_Latin1_General_CP1_CI_AS** (must be case-insensitive).

Example: Create a database and grant user access

```
Use master
CREATE DATABASE <database_name>
GO
alter database <database_name> SET READ_COMMITTED_SNAPSHOT ON
GO
CREATE LOGIN <login_name> WITH PASSWORD = 'thepassword'
GO
USE <database_name>
CREATE SCHEMA [octane]
GO
CREATE USER [octane] FOR LOGIN WITH DEFAULT_SCHEMA= [octane]
GO
ALTER AUTHORIZATION ON Schema::octane TO [octane]
GO
ALTER ROLE [db_ddladmin] ADD MEMBER [octane]
GO
```

Run the previous commands separately for each database (site schema and space schema).

> **Note:** During installation when you define the **octane.conf** file, you should enter the name of the site schema in **schemas > site**, the space schema in **schemas > initial-shared-space**, and the password in **schema-password**.
>
> When defining your site action in the **octane.conf** file, you need to specify **FILL_EXISTING**. For details, see "FILL_EXISTING" on page 43.

Configure Elasticsearch

Before installing ALM Octane, there are a number of settings you must configure in Elasticsearch.

> **Note:** Elasticsearch supports indexes that were created in the current Elasticsearch main version, or one earlier version. Each time ALM Octane extends support for a new Elasticsearch main version, the ALM Octane upgrade includes a reindex process for the older indexes.

Elasticsearch configuration

Before installing ALM Octane, configure Elasticsearch settings:

1. In the **elasticsearch.yml** file, configure the following:
   - **cluster.name**. Assign a unique name which is used when you configure ALM Octane to connect to the cluster. Note that even a single-server installation is considered a cluster.
   - **node.name**. If you do not assign the node a name, Elasticsearch generates a random name on every reboot.
   - **network.host**. The node binds to this hostname or IP address and publishes this host to other nodes in the cluster. You can enter an IP address, hostname, a special value, or an array of any combination of these. Defaults to **_local_**.
   - **action.auto_create_index**. In each of your Elasticsearch cluster nodes, you must have the following line in the elasticsearch.yml files:

     ```
     action.auto_create_index: "-mqm_*,*"
     ```

     > **Note:** If you already have an **action.auto_create_index** line in the yml file, add the **-mqm_*** phrase to the beginning of its specified value. For example, if you have the following line:
     >
     > ```
     > action.auto_create_index: "-index*,*"
     > ```

> You would change that to:
>
> `action.auto_create_index: "-mqm_*,-index*,*"`

2. You can configure Elasticsearch securely using TLS. For details, see https://softwaresupport.softwaregrp.com/doc/KM03712315.
3. In the **jvm.options** file, set the following parameters: **-Xms<*value*>g** and **-Xmx<*value*>g**.

   Define *value* as half of memory available on the machine – 1, but no more than 31GB.

Configuring an Elasticsearch cluster

Elasticsearch can run on a single node but it is designed to run as a cluster. We do not recommend running a production environment on a single host Elasticsearch instance.

Elasticsearch clusters should have at least 3 nodes, or a larger odd number. For details see https://www.elastic.co/guide/en/elasticsearch/reference/master/high-availability.html.

To configure an Elasticsearch cluster, modify the following parameters in the **elasticsearch.yml**:

- **cluster.name**. This name should be identical on all nodes of the cluster to make sure they join the same cluster.
- **discovery.seed_hosts**. To form a cluster with nodes on other hosts, use the static **discovery.seed_hosts** setting to provide a list of other nodes in the cluster that are master-eligible, and likely to be live in order to seed the discovery process.

> **Note:** The cluster nodes should be able to communicate with each other, meaning, the ports should be open in the firewall.

Restart Elasticsearch

After changing Elasticsearch setting files (for example elasticsearch.yml or jvm.options), you must restart the Elasticsearch service.

For details on restarting an Elasticsearch cluster, see https://www.elastic.co/guide/en/elasticsearch/guide/master/_rolling_restarts.html.

Backing up Elasticsearch

For details on backing up Elasticsearch, see https://www.elastic.co/guide/en/elasticsearch/reference/master/snapshot-restore.html.

We recommend performing ELS snapshot at the same time as database backup and file repository backup.

ALM Octane does not need to be stopped for this operation.

You can use curl to issue relevant snapshot commands. Also, consider creating a shell script to back up Elasticsearch data on a regular basis.

Next steps:

- "Deploy ALM Octane" on the next page

Installation

This section describes how to install an on-premises ALM Octane server using Linux.

Before installing:

- Verify that your server fulfills all prerequisites. See Support matrix in the ALM Octane Help Center.
- Review the ALM Octane Secure Deployment and Configuration Guidelines.

Cluster configuration: If you intend to install ALM Octane in a cluster configuration, review the end-to-end process under "Cluster installation flow" on page 17 before starting.

> **Language support:** On-premises installation of ALM Octane supports only English. This means only English characters can be specified for the names of schemas, operating systems, users, and so on.

This section includes:

Deploy ALM Octane

This section describes how to deploy an RPM file for installing an ALM Octane server.

This section includes:

Overview

Installing the ALM Octane RPM package does the following:

- Creates the correct directory structure.
- Copies all the files to the right locations.
- Creates a user and group for running the ALM Octane service that starts the ALM Octane server.

  By default, both the user and group are named **octane**. However, you can use a pre-defined user instead by defining the following environment variables: **OCTANE_USER** and **OCTANE_GROUP**.
- Installs the **octane** service so that the operating system recognizes it.

Prerequisites

Before installing:

- Verify that your server fulfills all prerequisites. See Support matrix in the ALM Octane Help Center.
- Review the ALM Octane Secure Deployment and Configuration Guidelines.

Deploy

This section describes how to deploy.

To deploy:

1. Download the ALM Octane RPM package:

   https://sld.microfocus.com/mysoftware/download/downloadCenter

   > **Tip:** To verify the digital signature of the RPM package, see "Installation Security" in the ALM Octane Secure Deployment and Configuration Guidelines.

2. Set up repository access.

   If the repository is located on a remote, dedicated machine, the ALM Octane server user account must have network access to the remote repository.

   The repository directory has to be shared, so the user performing installation (generally, the **octane** user) can write to the repository.

   - **Single-node configuration**

     Create an environment variable **OCTANE_REPOSITORY_DIR** on the ALM Octane server with the repository location.

     For example: `export OCTANE_REPOSITORY_DIR=/opt/octane/repo`

   - **Cluster configuration**
     - The repository directory has to be a shared directory visible to all cluster nodes.
     - On each cluster node create a mount directory that points to the repository directory, for example: **/mnt/octane/repo**. It is important that you enter the repository path using the same path name on all nodes.
     - On each cluster node create an environment variable **OCTANE_REPOSITORY_DIR** with the repository location.

       For example: `export OCTANE_REPOSITORY_DIR=/mnt/octane/repo`
     - The repository location cannot be /opt/octane on an ALM Octane node.

3. Install the ALM Octane RPM package.

   - To install the ALM Octane RPM package in the default installation directory **/opt/octane**, run:

     ```
     rpm -ivh <name of the RPM file>
     ```

   - For sudoer user, use: `sudo -E rpm -ivh <name of the RPM file>`

     The **-E** parameter is used to access the **OCTANE_REPOSITORY_DIR** environment variable created in previous step.

   - Alternatively, install the ALM Octane RPM package to a different directory:

     ```
     rpm -ivh --prefix <base path> <name of the RPM file>
     ```

> **Note:** If you install RPM to a different directory, make sure to replace "**/opt/octane**" with the relevant path when following these instructions.
>
> If RPM installation fails on Java version, see https://softwaresupport.softwaregrp.com/doc/KM000023838.

4. Verify the required file permissions.

Default directory	Description	Permissions
/opt/octane	ALM Octane installation directory and all its sub-directories and files. These files are used for configuring the server.	Full read, write, and execute
/opt/octane/log	Log file directory.	Full read, write, and execute

5. If planning to install ALM Octane on additional cluster nodes, perform the steps described under "Deploy in cluster environment" below.

Deploy in cluster environment

This section describes how to deploy in cluster environment.

To deploy in cluster environment:

1. **Configure the IP addresses (or fully qualified domain names) of the cluster nodes**. Configure the node IP addresses or fully qualified domain names in the **octane.conf** file. For details, see "Configure site settings" on the next page.
2. **Verify ports are open in your firewall.** When deploying ALM Octane over a cluster, ALM Octane needs to communicate between the nodes in the cluster located on port 5701. Therefore, make sure that your firewall enables communication between the nodes of the cluster on the specified port.

Configure site settings

Configure site settings using the ALM Octane configuration files:

- The **octane.conf** settings are mandatory for all environments.
- In addition, there are other settings that are required in complex ALM Octane environments. These include secure Elasticsearch, proxy settings, and LDAP or SSO authentication, as described below.

These settings are configured during installation, and can also be changed any time, whenever necessary.

This section includes:

Workflow

1. Configure basic settings by editing the **octane.conf** file. In addition, depending on your environment, configure the optional files described in the following sections.

   Configuration files must be readable and editable by the user installing ALM Octane, which is generally the **octane** user. If you copy or edit a configuration file as the **root** or **sudoer** user that does not have the necessary installation permissions, the install fails.

   > **Tip:** To change the owner: `chown <owner>:<group> <file>`
   >
   > **Example**: `chown octane:octane octane.conf`

2. If you are installing ALM Octane, after editing your configuration files proceed with "Start the ALM Octane server" on page 61.
3. If you need to make changes in configuration files later, make sure you edit the **<Repository folder>\conf\octane.conf** file, and not **octane.conf.new**, which is a temporary file that is for internal use only.

   After modifying these settings, restart the ALM Octane server on each node to pull the configuration changes from the repository. For details, see Modify site settings in the ALM Octane Help Center.

   For example, you might initially install ALM Octane to use native user management, and at a later time, decide to implement LDAP authentication for user management instead.

> **Tip:** We recommend that you save a local copy of the **octane.conf** file before making changes to it. Also, for security purposes, **octane.conf** should be stored in a secure, off-site location.

Database server settings

Setting	Description
db-type	Enter **ORACLE** or **MSSQL**.
connection-string	The Java Database Connectivity (JDBC) database connection string. It includes the following details: database type, database server name, database server port number, service name. **Oracle connection-string** The instructions below demonstrate how to set up the string with non-secured database access. To configure secure access to the database, see "Using SSL/SSO in Oracle (optional)" on the next page. **Syntax using service names:** `jdbc:oracle:thin:@//DB_SERVER_NAME:DB_SERVER_PORT/DB_SERVICE_NAME` **Examples:** • `jdbc:oracle:thin:@//dbserver1.net:1521/orcl` • `jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=dbserver1.net)(PORT=1521)))(CONNECT_DATA=(SERVICE_NAME=orcl)))` **Note:** To connect to Oracle RAC, use the Single Client Access Name (SCAN) instead of the database server name.

	SQL connection-string
	
	• **Syntax using port:**
	`jdbc:sqlserver://DB_SERVER_NAME:DB_SERVER_PORT`
	Example:
	`jdbc:sqlserver://dbserver1:1433`
	• **Syntax using instance:**
	`jdbc:sqlserver://DB_SERVER_NAME;instanceName=INSTANCE_NAME`
	Example:
	`jdbc:sqlserver://dbserver1;instanceName=my_instance`

Setting	Description
admin-user > name	ALM Octane uses the **admin-user** both to create objects during installation and also to check that the database server is accessible. • For Oracle, enter the name of the database admin user. • For SQL Server, enter the **sa** user, or an SQL Server power user with the correct permissions. For details about **admin-user** permissions, see "Prerequisites" on page 20.
admin-user > password	The password of the database admin user. Do not include a pound sign (**#**) or accented characters (such as, **ä**, **ç**, **ñ**).
schemas > site	The name of the site schema that is created by the **admin-user** during the installation, or supplied by the organization's DBA. Enter the supplied name.
schemas > initial-shared-space	This parameter is relevant only for the **FILL_EXISTING** site action. If you are using **FILL_EXISTING**, set the **initial-shared-space** to the name of the schema that is designated for the space.

Using SSL/SSO in Oracle (optional)

You can configure a secure connection from the ALM Octane server to the database server using SSL or SSO.

1. On the Oracle database server, convert the client wallet to jks keystore:

   ```
   orapki wallet pkcs12_to_jks -wallet "<path to client wallet folder>/<client wallet folder name>" -pwd <wallet_password> -jksKeyStoreLoc <name of your jks file>.jks -jksKeyStorepwd <jks_pass>
   ```

   For example:

   ```
   orapki wallet pkcs12_to_jks -wallet "/home/oracle19/wallets/client_wallet" -pwd aaa123456 -jksKeyStoreLoc clientstore.jks -jksKeyStorepwd test123#456
   ```

2. Check the content of the newly created jks keystore:

   ```
   keytool -list -keystore <name of your jks file>.jks -storepass <jks_pass>
   ```

For example:

```
keytool -list -keystore clientstore.jks –storepass test123#456
```

3. Copy the client wallet file from the Oracle database server to the ALM Octane Server. Place the newly created keystore jks file in a location on the ALM Octane app server into a directory accessible to all, such as **/opt/octane/conf/<name of your jks file>**. Grant read permissions on this file to ALM Octane users.
4. Copy the following to **octane.conf**, after the **connection-string** parameter. Replace the values with the specific to your installation:

```
connection-properties : [
      {
          "key" : "javax.net.ssl.trustStore",
          "value" : "<full path to keystore file>/<jks keystore
file name>.jks"
      }
  ,
      {
          "key" : "javax.net.ssl.trustStoreType",
          "value" : "JKS"
      }
  ,
      {
          "key" : "javax.net.ssl.trustStorePassword",
          "value" : "<jks keystore password>"
      }
  ]
```

Oracle server settings

Oracle settings	Description
schema-password	The password of the site schema. When installing using existing site schemas (with the **FILL_EXISTING** site action), make sure that the passwords that the DBA defines for the site schema and the space schema both match this **schema-password**.

Oracle settings	Description
table-space	The tablespace in the Oracle database where the site schema segment is created. Case-sensitive.
temp-table-space	The temporary tablespace in the Oracle database. Case-sensitive.
user-default-sort	Defines whether the standard Oracle binary sort (**NLS_SORT="BINARY_CI"**) should be overridden for non-Latin language support. Valid values: **yes**, **no**, or blank **Default**: blank (yes)

SQL server settings

SQL Server settings	Description
app-user > name	MSSQL database login authentication user for ALM Octane. This is the user for day-to-day ALM Octane use. This login is associated with the ALM Octane site and space databases. **Note:** This should be different from the **admin-user > name**. However if you are using **FILL_EXISTING**, this must be the same as the **admin-user** name.
app-user > password	The password for the app-user. If you are using **FILL_EXISTING**, this must be the same as the **admin-user** password.
authentication-method	Enter the authentication method used: **Windows** or **DB** (SQL Server Authentication).

Site actions

The **site-action** setting determines how the installation should handle databases.

CREATE_NEW	Use this site action for new installations. • Creates a new site schema, creates a new space schema, and configures the current node. • Only an **admin-user** with **create schema** permissions can create a new schema. • The **CREATE_NEW** site action fails when the schema already exists.
FILL_EXISTING	Use this site action for new installations, in cases where the database administrator does not give permissions to create a schema (for Oracle) or a database (for SQL Server). In this case, the organization's DBA must create a new site and space schema/database and users **before** installation. See the following for details: • "Create your own Oracle schemas for ALM Octane" on page 26 • "Create your own SQL databases for ALM Octane" on page 28 **Handling schema exceptions** If the organization's DBA made changes to schemas, such as the addition of tables or columns, you can define an exception file. The exception file instructs ALM Octane to ignore manual changes to the database user schema during installation and upgrade. For details, see "Using exception files for manual database changes" on page 79.

Space settings

initial-space-mode	The mode in which the initial space is created when the ALM Octane server starts. Valid values are: • **isolated**. Workspaces associated with the initial space do not share entities or customization settings. • **shared**. Workspaces associated with the initial space can share entities or customization settings.

Elasticsearch settings

A working Elasticsearch server is a requirement for working with ALM Octane. For details on Elasticsearch prerequisites, see "Configure Elasticsearch" on page 30.

hosts	The name of the host running Elasticsearch. If running an Elasticsearch cluster, all node host names should be separated by commas, as follows: **["host1","host2","host3"]**
http-port	Port configured in Elasticsearch for incoming HTTP requests. Default in Elasticsearch is 9200.
cluster-name	The name of the Elasticsearch cluster.

Elasticsearch security (optional)

You can connect ALM Octane with Elasticsearch securely using TLS. For details, see Setting up TLS for ALM Octane and Elasticsearch.

1. Make sure you have the following line in your **octane.conf** file:

   ```
   include "elasticsearch-security.conf"
   ```

2. Set up the **elasticsearch-security.conf** file as follows:

user	• **name**: The username to use when authenticating against Elasticsearch. • **password**: The password of the Elasticsearch user.
key-store	• **file**: The name of the PKCS12 keystore file. The file should be placed in the configuration folder. • **password** (optional, encrypted): The password to use to open the keystore file if the store is password protected. • **keystore type**: Certificate files should be in the PKCS12 format and should be put in the configuration folder.
trust-store	• **file**: The name of the PKCS12 truststore file. The file should be placed in the configuration folder. • **password** (optional, encrypted): The password to use to open the truststore file if the store is password protected. • **keystore type**: Certificate files should be in the PKCS12 format and should be put in the configuration folder.

verification-mode	Determine the level used when verifying the certificate. We recommend using the default setting. • **none**: No certificate verification checks are made. This means that any certificate can be accessed and should only be used to debug issues. • **certificate**: Only checks that the certificate is signed by a trusted CA. Should be used when hosts are dynamic. • **full**: In addition to certificate, also checks that the host name reported by the certificate matches the host the request is coming from. Should be used whenever possible and is the default.

Site admin credentials

site-administrator > name	The email of the site admin user that the installation creates. The email address can be specified now and created later. This is the only user available after installation. Other users can be added later. When using external user authentication, such as LDAP or SSO, this admin should be an existing user in the external system (LDAP or the IdP, respectively).
site-administrator > password	The site admin's password. The password must be at least 8 characters long, and contain at least one uppercase letter, one lowercase letter, and one number or symbol. Do not include a pound sign (**#**) or accented characters (such as, **ä**, **ç**, **ñ**). When using external user authentication, such as LDAP or SSO, this password should be defined as a "dummy" password. It will not be used once ALM Octane is configured for external authentication.

Cluster settings

Here are some settings you must use to establish if you are installing a standalone ALM Octane server or a cluster configuration. For details on cluster configurations, see "Cluster installation flow" on page 17.

single-server	Whether your server is standalone or in a cluster configuration. Mandatory. • For a standalone server, set this value to **true** and do not enter any host names using the **nodes** setting. • For a cluster configuration, set this value to **false**. You must enter node host names in the **nodes** setting.

nodes	Configure the IP addresses or fully qualified domain names for each cluster node. Enter a comma-separated list of node host names or IPs, in the cluster, for example: ["host1","host2","host3"] Make sure **single-server** is set to **false**.

Heap size

heap-size	Before starting the ALM Octane server the first time, change the heap memory values on all active cluster nodes. For example, you may need to increase the heap size if there is an increase in the number of active workspaces in ALM Octane, or an increase in the number of concurrent user sessions. Set **heap-size** to half of available server memory on a dedicated server, regardless of load. Heap size should not exceed 31 GB. Values should be specified in MB (for example, 4096 for 4 GB). Default: **4096**

Proxy settings (optional)

If ALM Octane is behind a firewall, and needs to access an outside server, you may need to configure ALM Octane to use a proxy server.

1. Make sure you have the following line in your **octane.conf** file:

   ```
   include "proxy.conf"
   ```

2. Set up the **proxy.conf** file as follows:

http	• **host**: The proxy host (if using HTTP). • **port**: The proxy port (if using HTTP).
https	• **host**: The proxy host (if using HTTPS). • **port**: The proxy port (if using HTTPS).
user	• **name**: User name accessing the proxy. • **password**: Password for proxy user.
non-proxy hosts	

Public URL and Server Ports

In production systems, only secure configuration (HTTPS) is supported. In staging, we do not recommend using non-secure configuration. For details, see "Configuration tips" on page 60.

Enter the following in the **server-binding** section:

app-url	The fully-qualified domain name and port for the ALM Octane server. This is used for SSO configuration, reverse proxy configuration, SSL offloading configuration, and so on. This URL is also inserted as a link in emails that ALM Octane sends. Email recipients can click the link to access the relevant entity directly in ALM Octane. Use this pattern: `http://<Server URL>:[Port]` **Basic configuration:** Usually the URL of the server on which you installed the ALM Octane server. **Cluster configuration:** The Virtual IP URL. **Note:** If you have a URL with a top-level domain (TLD) that is not listed in https://www.iana.org/domains/root/db (for example http://a.b.corp, where **corp** is not listed), see "Troubleshooting non-standard top-level-domains" on the next page.
http-port	The value of a Jetty port for HTTP, or a Jetty secure port for HTTPS.

https-port	After you install ALM Octane, you may need to change the ALM Octane server port number.
	
	Because the installation uses a non-root user, common ports (below 1024) cannot be used with ALM Octane.
	
	By default, the installation uses port 8080 for HTTP or port 8443 for HTTPS (SSL).
	
	`httpPort: 8080`
	
	`httpsPort: 8443`
	
	Leaving any of these ports empty disables the access using the specified http schema server.
	
	It is possible that the default application server port is used by another application that is running on the same machine. In this case, you can either locate the application that is using the port and stop it, or you can change the ALM Octane server port.

allow-http-requests-if-ssl-enabled	By default, if you define your **app-url** as using HTTPS protocol, users cannot access ALM Octane via HTTP. If you need to enable HTTP access (for example for internal tools inside your network), you can set this parameter to **true**. This allows HTTP access to ALM Octane even though your protocol is set to HTTPS.
java-default-trust-store-password	By default, the Java trust store password is **changeit**. If you changed this password, enter the Java trust store password here. When ALM Octane starts, it encrypts this password. This is useful when ALM Octane server trust is configured.
force-disable-http2	By default, the HTTP/2 protocol is disabled, and this parameter is **true**. To use HTTP/2, change this parameter to **false**. In this case, you must configure HTTPS using the **key-store** fields. If you are using a load balancer or proxy server, make sure that they support HTTP/2.
The key-store fields are mandatory for HTTPS:	
file	Enter the absolute path to the keystore file, or the file name if the keystore is in ALM Octane's configuration folder.
password	Password used to protect the keystore file. When ALM Octane starts, it encrypts this password.
keystore type	Enter JKS or PKCS12. **Note:** This field must be populated (default: **JKS**).

Troubleshooting non-standard top-level-domains

ALM Octane validates that the top-level domain (TLD) entered in the **app-url** parameter is listed in https://www.iana.org/domains/root/db. If you enter a URL with a TLD that is not listed there (for example http://a.b.corp, where **corp** is not listed), server startup fails. In this case, perform the following steps:

1. Enter the default app-url: **https://localhost:8080**.
2. Start ALM Octane.
3. In the configuration parameters, define the parameter **ADDITIONAL_ALLOWED_TLD** with the value of your TLD (for example **corp**).
4. Restart ALM Octane.

5. In the configuration parameters, define the parameter **SERVER_BASE_URL** with the correct value of your server URL (for example http://a.b.corp).

License settings

trial-edition	The trial edition is always **enterprise**. For details, see the information about ALM Octane editions in the ALM Octane Help Center.
license-mode	• If you are using a standalone ALM Octane license, enter **standalone**. You can then skip the remaining fields in the **License** section. Default. • If you are allocating licenses from ALM to ALM Octane, enter **ALM_SHARING**. You then need to fill in the following fields as described below. For details, see Manage licenses (on-premises) in the ALM Octane Help Center.
The following fields are mandatory for ALM_SHARING mode:	
url	Enter the full path that you use to access ALM. Typically, this includes the suffix **qcbin**.
integration-user > name	Enter the user name for accessing ALM. This user was defined in ALM for integration purposes.
integration-user > password	Enter the password for the **integration-user**. This password is automatically encrypted after you restart the ALM Octane server.

Authentication Type

Specify whether the ALM Octane installation should use native user management (default), LDAP, or SSO authentication for user management.

authentication-type	Values are: **internal**. Use internal, native ALM Octane user management. Default. **ldap**. Use LDAP authentication. Define LDAP settings as described in "LDAP authentication settings (optional)" on the next page. **sso**. Use SSO authentication. Define SSO settings as described in "SSO authentication settings (optional) " on page 55.

LDAP authentication settings (optional)

If you plan on authenticating users using LDAP, we recommend you configure LDAP settings using the ALM Octane Settings UI after installation, rather than in the **ldap.conf** file. When you configure LDAP in the Settings UI, your settings are automatically validated and updated in the **ldap.conf** file. For details, see Configure LDAP in the ALM Octane Help Center.

If you prefer to work directly in the configuration files rather than in the Settings UI:

1. Make sure you have the following line in your **octane.conf** file:

   ```
   include "ldap.conf"
   ```

2. In the **ldap.conf** file, configure the LDAP settings as described below.
3. Later, after ALM Octane installation, import users from LDAP into ALM Octane.

> **Tip:** LDAP settings are validated when you start ALM Octane. If there are errors in your LDAP configuration which prevent the ALM Octane server from starting, have a site admin check the wrapper, site, and app logs.

General LDAP settings

Field	Description
connection-timeout	Connection timeout in seconds. Optional. Default: 30 seconds

Field	Description
admin-dn	The user that signs in to ALM Octane after **initially** setting up LDAP authentication. Its purpose is to make sure that one workable user exists to start configuring LDAP user authentication. When the ALM Octane server starts, it checks LDAP configuration settings, verifies that this user exists, and validates this user against the LDAP data. If this attribute is not defined correctly, the server does not start. Correct the user details and restart the server. This user can be same user as the user entered in the **octane.conf** file, or a different user. After entering the value for this user, and then restarting the ALM Octane server, the admin user entered in the **octane.conf** file is overwritten. This becomes the ALM Octane site admin user that can be used to log into ALM Octane the first time. **Note**: If the **admin-dn** is changed and the server is restarted, both the original **admin-dn** and the new **admin-dn** exist as site admins. Modifying the **admin-dn** does not remove the original one.

LDAP server settings

Enter the following settings for each LDAP server separately.

> **Caution:** Back up all passwords set below because they are encrypted after the ALM Octane server is initialized.

servers	Header row to delineate that the information below is for each LDAP server. Do not enter a value.
host	The LDAP server host name or IP address. Mandatory.
port	LDAP server connection port. Mandatory.
ssl	Whether the LDAP server uses SSL. Mandatory. Enter **Y** or **N**. If **Y**, establish trust to the certificate authority that issued the LDAP server certificate. For details, see "Configure trust on the ALM Octane server" on page 70.

base-directories	Root of the LDAP path to use to search for users when including new LDAP users in ALM Octane spaces. This can be a list of common names and domain components (cns and dns), a list of organizational units (ou), and so on.
	Optional. Default: Blank.
	Example:
	`"base-directories" : [`
	`"dc=maxcrc,dc=com",`
	`"ou=Administrative,dc=maxcrc,dc=com"`
	`],`

base-filters	Filters to use to refine the search for users when including new LDAP users in ALM Octane spaces. This is generally a semi-colon delimited list of LDAP **objectClasses**. Optional. Default: (objectClass=*)
description	Description of the LDAP server. Optional.
authentication:	Header row to delineate that the information below is for authentication. Do not enter a value.
method	The LDAP authentication method supported by the LDAP server. Authentication method used by the LDAP server. The following methods are supported: • **anonymous**. In this case, skip the next two parameters, **name** and **password**. • **simple**. **name** and **password** are mandatory.
user name	Only required if you set the **authentication** parameter to **simple**. User name for accessing the LDAP server. This user must have at least read permissions for the LDAP server.
password	Only required if you set the **authentication** parameter to **simple**. Password for accessing the LDAP server. This password will be encrypted.

LDAP server mapping settings

Enter the following mapping settings for each LDAP server separately.

Values used in the mapping section are case-sensitive.

ALM Octane attribute in ldap.conf	Sample LDAP attribute that can be used	Values and descriptions
mapping		Header row to delineate that the information below is for mapping of LDAP attributes. Do not enter a value.
dn	**distinguishedName** **(for Active Directory)**	The LDAP distinguished name attribute. Unique. Mandatory. This attribute is typically in a format that contains the common name and organization details, such as: **cn=<common_name>,ou=<organizational_unit>,dc=<part_of_domain>** The **dn** is a unique string that typically contains other LDAP attributes, such as **cn**, **ou**, and **dc**.
	entryDN **(for other LDAP systems)**	**Example** 1. If in LDAP, the **entryDN** attribute value is: **cn=<*common_name*>,ou=<*organizational_unit*>,dc=<*part_of_domain*>** 2. In the **ldap.conf**, the dn value would be mapped to: **entryDN** 3. When exporting users from LDAP, the **dn** string representation of each LDAP user would be the common name, followed by the organizational unit, followed by a part of the domain, such as: **cn=Joe_Smith@nga,ou=my_org,dc=com**

ALM Octane attribute in ldap.conf	Sample LDAP attribute that can be used	Values and descriptions
uid	**objectGUID** **(for Active Directory)**	The LDAP attribute that should be used as the immutable, globally-unique identifier. Mandatory. In this documentation, we also refer to this as the UUID (universally unique ID). • For Active Directory: To work with ALM Octane with Active Directory, we use **objectGUID**. • For other LDAP systems: To work with ALM Octane, we generally use **entryUUID** for OpenLDAP. However, depending on your LDAP, this attribute might be different, such as **GUID** or **orclguid**. This is an attribute by which ALM Octane identifies each user internally for synchronization between ALM Octane and LDAP, including when importing users into ALM Octane. You can configure other values, such as GUID or orclguid, or any other unique value.
	entryUUID **(for other LDAP systems)**	
first-name	**givenName**	LDAP attribute for first name, such as **givenName**. Mandatory.
last-name	**sn**	LDAP attribute for last name, such as **sn**. Mandatory.
full-name	**cn**	LDAP attribute for full name, such as **cn**. Optional.
logon-name	**mail**	This is the unique identifier between all ALM Octane users, and this attribute is used to log onto ALM Octane. In some cases, ALM Octane may use this attribute to identify each user internally for synchronization between ALM Octane and LDAP, including when importing users into ALM Octane. **mail** is usually unique for each user, so **mail** is an appropriate LDAP attribute to use to map to **logon-name**. Mandatory. You can change the **logon-name** attribute mapping at any time, but make sure the **logon-name** is unique across all ALM Octane users.
email	**mail**	The LDAP attribute for email address, such as **mail**. Mandatory.
phone1	**telephoneNumber**	The LDAP attribute for the primary phone number, such as **telephoneNumber**. Optional.

SSO authentication settings (optional)

Use these settings to set up SSO authentication for connecting to ALM Octane with an external IDP.

1. Make sure you have the following line in your **octane.conf** file:

   ```
   include "sso.conf"
   ```

2. Set up the **sso.conf** file as follows:

Key-pair settings:

Setting	Description and usage
alias	Unique identifier for the SSO public/private key pair used by the ALM Octane service provider for signing and encrypting authentication information. Mandatory. Example: **sso-osp-keypair**
password	Password for protecting and encrypting the key pair defined with **key-pair alias**. When ALM Octane starts, it encrypts this password. Mandatory. Example: **my-secret**

Key-store settings:

Setting	Description and usage
file	The absolute path to the keystore file identified with **key-pair alias**. The path should be under ALM Octane's configuration folder to avoid permission issues. Mandatory.
password	Password used to protect the keystore file defined with **keystore file**. When ALM Octane starts, it encrypts this password. Mandatory. Example: **my-password** **Note:** If you are using pkcs12, you must use the same password for both the keystore and the key(s). This is a Java limitation.

Setting	Description and usage
keystore-type	This defines the keystore type. The default format for this file is **PKCS12**. You can change the format to Java KeyStore (JKS) by specifying this type here.

OAuth settings:

Setting	Description and usage
client-id	Client ID used for internal OAuth2 configuration and by which the integration that will be accessing ALM Octane will identify itself. Regular expressions are not supported (meaning, no asterisk wildcards). Must be the same on all ALM Octane cluster nodes. Mandatory. Example: **my-client-ID**
client-secret	The OAuth client secret for the integration's client ID defined with **oauth client-id**. Can be any value. We recommend that the secret be complex and hard to guess. Must be the same on all ALM Octane cluster nodes. When ALM Octane starts, it encrypts this password. Mandatory. Example: **secret**
authentication-timeout	The SSO authentication timeout in seconds. Optional. Default: **10800** seconds (3 hours). **Other timeout settings when working with SSO** The following configuration parameters can be used to set other timeouts when working with SSO. These parameters are defined in the Settings area in ALM Octane, not in the **sso.conf** file. They do not have any effect on the SSO authentication timeout. • **MINUTES_UNTIL_IDLE_SESSION_TIMEOUT**. Defines license consumption in minutes. • **MINUTES_UNTIL_GLOBAL_SESSION_TIMEOUT**. Defines API key authorization timeout in minutes. For details on setting these configuration parameters, see Configuration parameters in the ALM Octane Help Center.

SAML settings:

Section	Setting	Description and usage
IdP	**metadata-url**	The IdP's URI for publishing IdP metadata. Part of the pairing process. If this is set, there is no need to set metadata. Using this option, the URL must be available and respond with a valid XML or ALM Octane will not start. Any valid URL is accepted. You can define the SAML metadata descriptor resource with either this setting, or the **saml idp metadata** setting. Mandatory, if **saml idp metadata** is not defined. Example: **http://my-server.company-infra.net:8080/auth/realms/Dev/protocol/saml/descriptor** **Note:** Only one of the parameters **metadata** or **metadata-url** should be defined. If the sso_configuration validator is disabled and both parameters are defined, the URL defined in **saml idp metadata-url** will be ignored.
IdP	**metadata**	Base 64 encoded XML of the SAML metadata descriptor from the IdP. This should be used if the IdP metadata URL cannot be accessed from the ALM Octane server. You can define the SAML metadata descriptor resource with either this setting, or the **saml idp metadata-url** setting. Mandatory, if **saml idp metadata-url** is not defined. **Note:** Only one of the parameters **metadata** or **metadata-url** should be defined. If the sso_configuration validator is disabled and both parameters are defined, the URL defined in **saml idp metadata-url** will be ignored.
Mapping	**user-name**	The parameter in the SAML response which maps to the user name. Valid values are: • **'{$id}'**. Mapping is to the **NameID** in the SAML response's subject. Default. • **userName**. Mapping is to the **username** in the SAML attribute statement. Changing the default to a property name, such as **userName**, in the SAML response, does not require quotes.

Section	Setting	Description and usage
Mapping	**uuid**	The attribute in the SAML response's attribute statement that maps to the user's UUID. Optional. Default: **uuid**
Mapping	**mail**	The attribute in the SAML response's attribute statement that maps to the user's email address. Optional. Default: **mail**
Mapping	**first-name**	The attribute in the SAML response's attribute statement that maps to the user's first name. Optional. Default: **firstName**
Mapping	**last-name**	The attribute in the SAML response's attribute statement that maps to the user's last name. Optional. Default: **lastName**
Mapping	**full-name**	The attribute in the SAML response's attribute statement that maps to the user's full name. Optional. Default: **fullName**

Token-exchange settings:

Setting	Description and usage
token-exchange-enabled	Activates the federated identity option for authenticating APIs within an organization's SSO system. Mandatory. Default: **false**
issuer	Used to define the <baseUrl> in any OpenID Connect (OIDC) endpoint when authorizing against the external OAuth 2.0 authorization server. Use the following endpoints to review the metadata and find the issuer: **https://<OAuth2 Authorization Server>/.wellknown/openid-configuration** Mandatory.

Setting	Description and usage
treat-access-token-as-opaque	If **true**, any access token returned from the OIDC provider is treated as an opaque token even if it appears to be a JWT token. Set to **true** only if the provider returns an access token that appears to be a JWT, but which is invalid. Mandatory. Default: **false**
max-clock-skew	The maximum time difference between the ALM Octane system and the OIDC provider system in milliseconds. The value can be suffixed with "s", "m", "h", or "d" to indicate that the value is seconds, minutes, hours, or days. **Note:** If systems are time-synchronized using NTP, there is no need to set maximum skew time to more than a couple of seconds. Mandatory. Default: **1s**
oidc	The oidc section contains the following settings. • **client-id** and **client-secret**. The OIDC client ID and secret to use in your organization's tool for the token exchange. The OIDC client ID and secret should be placed in the Authorization header as Basic: `Authorization: Basic Base64(clientId:clientSecret)` Mandatory. **Note:** • The OIDC client ID is not the same client ID that is used by the tool for authentication. • OIDC client ID and secret differ from: ◦ The API key used for authentication in the authorization server. ◦ The client ID and secret defined in the **sso.oauth** section because of the different usage scenarios. Client ID and secret from **sso.oauth** are used by ALM Octane during the SSO authentication flow, while client ID and secret from the **token-exchange.oidc** section are used by the tool that performs the token exchange. • **authentication-timeout**. The federated SSO authentication timeout in seconds. Mandatory. Default: **10800** seconds (3 hours).

Setting	Description and usage
mapping	The mapping section contains the following settings. Only the standard OIDC claims are supported. • **user-name**. Defines the claim in the access token from the authorization server that holds the name of the authenticated API key. This is used for mapping the authenticated API key with its role in ALM Octane. Mandatory. • **session-identifier**. Defines the claim in the access token from the authorization server that holds a unique authentication identifier (for example "txn", Transaction Identifier). Mandatory. Default: **jti**

Logging settings:

Setting	Description and usage
directory	The directory in which to create the SSO log files. Optional. If the value is empty then the default logging directory will be used. Default: **<log folder>/sso**
logging-level	Logging level. Possible values are: • **SEVERE** • **INFO** • **WARNING** • **ALL** Optional. Default: **WARNING**

Configuration tips

- In production systems, only secure configuration (HTTPS) is supported. In staging, we do not recommend using non-secure configuration as the industry standard is to always use secure communication. Non-secure configuration results in poorer client performance, which does not fully represent what will happen in the production environment.
- When you install a single node configuration for the Jetty server, you need to use the full address to access it. Meaning, if the Jetty server was installed on a

machine named **myserver.mydomain.com**, then you access it via: **http[s]://myserver.mydomain.com:<port>** and not via **http[s]://myserver:<port>** if there are client-side DNS shortcuts installed.

- When you install a cluster Jetty server environment, the load balancer and all Jetty nodes should all be accessible from one another. The same rules for accessing the server via the load balancer from the client side apply. Meaning, the full address of the load balancer should be used for access.

Start the ALM Octane server

When you finish defining your configuration settings as described in "Configure site settings" on page 37, start ALM Octane.

To start the ALM Octane server:

1. Log in as either the root or sudo user.
2. Run the **octane** service to start the ALM Octane server. Run:

```
systemctl start octane
```

The installation is complete only when the "Server is ready!" message is shown in the **/opt/octane/log/wrapper.log** file. If you do not see the "Server is ready!" message, correct the errors shown in the log.

> **Tip:** When you first start using ALM Octane, you automatically receive a Trial license which gives you a 90-day trial for 100 users. For details, see Trial license in the ALM Octane Help Center.

Next steps:

- "Log in to ALM Octane" on page 63
- **Cluster configuration**: If you successfully installed and logged into ALM Octane on the first cluster node, continue installing on additional cluster nodes.
- If connecting to a database server or an LDAP server over a secure channel

(SSL/TLS), or for license sharing with ALM, configure trust. For details, see "Configure trust on the ALM Octane server" on page 70.

Log in to ALM Octane

This section describes how to log into ALM Octane.

> **Tip:** When you first start using ALM Octane, you automatically receive a Trial license which gives you a 90-day trial for 100 users. For details, see Trial license in the ALM Octane Help Center.

To log into ALM Octane:

1. In a browser, go to **<*serverURL*>:<*serverport*>/ui**.

   Make sure to specify a fully-qualified domain name for the server. The name must include at least one period. Do not specify an IP address.

   Cluster configuration: Use the load balancer URL.

2. Log in with the site admin user name and password you provided in the **octane.conf** file using settings **site-administrator name** and **password**.

> **Note:** Errors might be listed even if the ALM Octane server initializes and starts. If you encounter problems initializing ALM Octane, check for errors in the log files. For details, see "Troubleshooting" on page 85.

Next steps:

- **Cluster configuration**: If you successfully installed and logged into ALM Octane on the first cluster node, continue installing on additional cluster nodes. See "Cluster installation flow" on page 17.
- Set configuration parameters, such as FORGET_USER_ON_DELETE and SMTP_NOTIFICATION_SENDER_EMAIL. See Configuration parameters in the ALM Octane Help Center.
- Create spaces. See Create a space in the ALM Octane Help Center.
- Once you have logged on as the space admin, you can create other users and workspaces. See Users and Create workspaces in the ALM Octane Help Center.

Install ALM Octane using a Docker image

This section describes how to install ALM Octane using a Docker image.

1. Download and install the latest version of Docker for Linux.
2. In the Docker Hub, search for **Octane**.
3. Select **lifecyclemanagement/octane**. The description should say: The official repository for ALM Octane.
4. Select **Tags**.
5. Choose the ALM Octane version you want to install, and copy the download command.

> **Note:** The list you see includes both SaaS versions and on-premises versions of ALM Octane, but only on-premises versions are supported. Select an on-premises version now.

6. In the Linux console, execute the copied command.
7. Run the Docker image using the following command:

```
docker run -d -p 8080:8080 -p 8443:8443 -v /opt/octane_
docker/conf:/opt/octane/conf -v /opt/octane_
docker/log:/opt/octane/log -v /opt/octane_
docker/repo:/opt/octane/repo --name alm_octane
lifecyclemanagement/octane:onprem
```

> **Note:** This command includes the following:
>
> **-d** - Run container in background and print container ID.
> **-v** - Bind mount a volume (local_path:path_in_container).
> **-p** - Publish a container's port(s) to the host (local_port:port_in_container).
> **--name** - Container name

The first run fails with errors, because ALM Octane has not yet been configured.

8. Open the **octane.conf** file located in **/opt/octane_docker/repo/conf-discover/octane.conf**.
9. Configure ALM Octane as described in "Configure site settings" on page 37.

> **Note:** If you want to use resources from your local machine instead of localhost, use host.docker.internal.

10. When you are done, run the container using the name defined in step 7:

```
docker start alm_octane
```

11. Check for errors in the **wrapper.log** and **octane.log** files, in the folder **/opt/octane_docker/log**.
12. ALM Octane is now ready for use.

Management

Here are some management tasks you may have to perform during or after installation.

> **Note:** In addition to these management tasks, you can also set configuration parameters to define how your site operates. Configuration parameters for the site are set using Settings. See Configuration parameters in the ALM Octane Help Center.

This section includes:

Start the ALM Octane server manually

If you need to start the ALM Octane server manually, perform the following.

To start (or restart) the ALM Octane server:

- Log in as the root user and run the **octane** service:

```
systemctl start octane
```

  The service runs in the background.

To follow the server's boot process:

- Run:

```
tail -f /opt/octane/log/wrapper.log
```

To start (or restart) ALM Octane in a cluster configuration:

All nodes must be restarted.

Handle database-related issues

This topic provides instructions for handling database-related management tasks.

This section includes:

Change site schema settings and reinitialize

If you need to make changes to the site schema settings, make the changes in the **octane.conf** file.

To change site schema settings and reinitialize:

1. Obtain the names of the indexes related to your instance of ALM Octane in the **sharedspace_logical_name.txt** in the **/opt/octane/server/conf/** directory.
2. Delete the database site schema.
3. Delete the repository.
4. Delete the **mqm_<sp_logical_name>** index from Elasticsearch. From the shell on the ALM Octane server, run:

   ```
   curl -XDELETE 'http://<server address>:9200/mqm_<sp_logical_
   name>/'
   ```

5. Start the ALM Octane server.

   ```
   systemctl start octane
   ```

Update database password in ALM Octane site schema and configuration files

If you change your database password, you can use the database password update tool to update the database password in ALM Octane's site schema, and in the octane.conf configuration files. Note that this does not update the database user's password, but only ALM Octane's configuration.

> **Note:** The tool operates offline. Credential outputs are disabled for security.

1. Stop the ALM Octane server.

   After stopping the server, wait 30 seconds before running the tool. The cluster is considered offline when there is no activity from any node for 30 seconds.
2. Run the following command on your ALM Octane server:

   ```
   /opt/octane/install/updatedbcreds.sh
   ```
3. Enter values as described in the sections below.
4. When you are done, start the ALM Octane server.

Usage

The tool can operate in 2 modes: file, or interactive.

```
updatedbcreds.sh <-m mode> <-f path | -t target>
```

Where:

- mode = {file | interactive}
- target = {admin | user}
- path = valid absolute or relative path to file

File. If mode is set to file, use -f to specify the path to the password definition file. Credentials are taken from the provided file.

Interactive. If mode is set to interactive, use -t to specify the target whose password you want to change - either admin or user. You then enter credentials interactively.

Example: If you want to update the db.admin-user in the config file, the target should be **admin** (in Interactive mode).

If you want to update the db.<db-vendor>.app-user-name in the config file, the target should be **user** (in Interactive mode).

File mode

You can use the CLI in file mode, which allows granular definitions for admin, user, or space passwords.

Using a tool in file mode looks like this:

```
./updatedbcreds.sh -m file -f /path/to/definition.json
```

This is done using a JSON password definition file, in the following format:

```json
{
  "admin" : {
    "password" : "PasswordForAdminUser"
  },
  "appUser" : {
    "password" : "PasswordForAppUser"
  },
  "spaces": {
    "default_shared_space": {
      "password": "PasswordForSpecificSpace"
    }
  }
}
```

You can delete the **spaces** section. In this case all spaces get the appUser password.

Caution: Before the tool runs, your file contains passwords in clear text. It is your responsibility as administrator to secure the file according to your organization's policies. The tool encrypts the file when running. The tool can read the encrypted password if you want to rerun the tool.

For improved security, use interactive mode.

Interactive mode

In interactive mode you update only the admin or user password. This is useful when you do not need extensive password definition and just want to change a password for a single user.

Using a tool in interactive mode looks like this:

```
$ ./updatedbcreds.sh -m interactive -t admin
```

Enter the following:

- New password for ADMIN: Enter a new password for admin user. Output is disabled.
- DB authentication username: Enter a user for CLI database connection. Output is disabled.
- DB authentication password: Enter a password for CLI database connection. Output is disabled.

See also:

- "Management" on page 66

Configure trust on the ALM Octane server

Configure trust on the ALM Octane server when you connect to any remote server (such as a database server, an LDAP server, license sharing with ALM, and so on) over a secure channel.

Note: When connecting to a database server with SSL, or an LDAP server, over a secure channel, you must configure trust before starting the ALM Octane server by running **systemctl start octane**.

To configure trust:

1. Obtain the certificate of the root and any intermediate Certificate Authority that issued the remote server certificate.
2. Import each certificate into the ALM Octane java truststore using a keytool command.
   - Locate your **<java_home>** directory. It is usually under the **user/lib** directory but may be different for your environment. One way to check the location of the ***<java_home>*** directory is to check the environment information settings in the **/octane/log/wrapper.log** file.

     Example: **/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.131-11.b12.el7.x86_64/jre**
   - Locate your keystore **cacerts** file, which is usually here: ***<java_home>*/jre/lib/security/cacerts**
   - Import each certificate.

     Example:

     ```
     cd <java_home>/bin

     ./keytool -import -trustcacerts -alias <CA> -file <path to the CA certificate file> -keystore ../lib/security/cacerts
     ```
3. In the octane.conf file, enter the cacerts password in the **java-default-trust-store-password** parameter.
4. If the ALM Octane service (**octane**) is running, restart it.

> **Tip:** For general details on configuring HTTPS, see "Secure configuration and deployment" in the ALM Octane Secure Deployment and Configuration Guidelines.

Advanced ALM Octane server configuration

This section describes advanced configuration tasks for the ALM Octane server.

This section includes:

Redirect http to https

This procedure describes how to redirect http to https. You need to redirect to https when accessing the ALM Octane server directly, and not through a front-end server.

To redirect http to https:

1. Edit **/opt/octane/webapps/root/WEB-INF/web.xml**, and add the following at the end (before **</web-app>**):

```
<security-constraint>
        <web-resource-collection>
                <web-resource-name>Everything</web-resource-name>
                <url-pattern>/*</url-pattern>
        </web-resource-collection>
        <user-data-constraint>
                <transport-guarantee>CONFIDENTIAL</transport-guarantee>
        </user-data-constraint>
</security-constraint>
```

2. Restart .
3. Access ALM OctaneALM Octane via **http://<ALM Octane>:8080/ui**. Port **8080** is the default port.

   You should be redirected to **https://<ALM Octane>:8443/ui**. If not, ensure that **SecurePort** in **jetty.xml** matches your secure port.

Configure number of allowed open files (Linux)

If ALM Octane is under a very heavy load, it might try to use too many Linux resources. In this case, Linux kills the server process. Do the following to increase the number of allowed open files to 65536:

To configure number of allowed open files:

1. Open the **/etc/security/limits.conf** file.
2. Add the following line:

   ```
   octane hard nofile 65536
   ```

3. Restart the ALM Octane server.

For details, see https://easyengine.io/tutorials/linux/increase-open-files-limit/.

Configure secure database access

This section describes how to configure a secure connection from the ALM Octane server to the database server. The secure connection is protected with SSL/TLS for encryption and authentication.

This section includes:

Defining the connection-string for secure database access

SQL Server

SQL Server Scenario	Instructions
SSL/TLS is required	Add the encryption method to the end of the **ConnectionString** value. **jdbc:sqlserver://<server>:<port>;encrypt=true;trustServerCertificate=true**
SSL without certificate validation	When using SSL, disable validation of the certificate sent by the database server. Add the encryption method to the end of the **ConnectionString** value, and apply the certificate into the java certs file located under **<JAVA_HOME>\jre\lib\security\certs**. **jdbc:sqlserver://<server>:<port>;encrypt=true;trustServerCertificate=false;trustStore=<Java Certs file>;trustStorePassword=<JKS password>**

Oracle

Oracle scenario	Instructions
SSL/TLS required	To configure a secure connection from the ALM Octane server to the database server using SSL or SSO, refer to the section "Using SSL/SSO in Oracle (optional)" on page 40. The connection string should include the port defined in the Oracle database as the port for SSL connections. The protocol should be set to TCPS: `connection-string = "jdbc:oracle:thin:@(DESCRIPTION= (ADDRESS=(PROTOCOL=tcps)(HOST=<hostname>)(PORT=<ssl port>)) (CONNECT_DATA=(SERVICE_NAME=<ORA_SERVICENAME>)))"`

To configure a secure database connection for a previously-unsecured database

This step provides instructions for configuring the site schema connection.

Skip this section if you have a separate database server for your workspaces and you only want a secure connection to that database.

This section is relevant if the database server that was configured for a secure connection contains your site schema.

1. Edit the **octane.conf** file. The default location is **/opt/octane**):
   a. Set the value of **site-action** to **CONNECT_TO_EXISTING**:

      `site-action=CONNECT_TO_EXISTING`

   b. Edit the line with **connection-string**. For details, see "Advanced ALM Octane server configuration" on page 72.
2. If SSL/TLS is required, make sure the trust on the ALM Octane server has been established. For details, see "Configure trust on the ALM Octane server" on page 70.
3. Run the service to start the ALM Octane server.

```
systemctl start octane
```

To configure a secure database connection for a new ALM Octane installation

1. After installing ALM Octane, start the server:

   ```
   systemctl start octane
   ```

2. In the Database Server step, select the **connection-string** option and set the values for your database. For details, see "Advanced ALM Octane server configuration" on page 72.
3. Make sure the trust on ALM Octane the ALM Octane server has been established. For details, see "Configure trust on the ALM Octane server" on page 70.

Configure SSL offloading

When ALM Octane is installed with SSL offloading, make sure re-directions go to HTTPS addresses instead of HTTP addresses.

To configure SSL offloading:

1. The X-Forwarded-Proto header must be defined in a reverse proxy.

   For example (on Apache):

   a. Add this line at the end of httpd.conf:

      ```
      RequestHeader set X-Forwarded-Proto https
      ```

   b. Restart Apache.

2. Open the ***<ALM Octane-installation-folder>*/octane/server/conf/jetty.xml** file in an editor.

   In the section **<New id="httpConfig" class="org.eclipse.jetty.server.HttpConfiguration">**, make sure that the following lines are uncommented:

   ```
   <Call name="addCustomizer">
   ```

```
<Arg><New
class="org.eclipse.jetty.server.ForwardedRequestCustomizer"/></A
rg>

</Call>
```

Dedicate a cluster node for background jobs – 12.60 CP8 and later

You can dedicates nodes for certain purposes, such as for running background asynchronous jobs. This frees up nodes for processing requests that come directly from the ALM Octane UI, as users work.

Overview

Cluster nodes can be one of the following types:

- **Worker nodes**. Cluster nodes that handle background asynchronous jobs, such as synchronization.
- **Web nodes**. All other nodes. Web nodes generally handle direct requests from ALM Octane, but can also handle background jobs if the worker nodes are not available. The load balancer distributes the requests as usual among the web nodes.

To dedicate a node for background jobs

After the ALM Octane installation is complete, and you have verified that the server is up and you can log into ALM Octane, perform the following:

1. Stop the ALM Octane server.
2. Add another node to the cluster that is not connected to the load balancer.
3. Follow the instructions for installing ALM Octane on cluster nodes. For details, see "Cluster installation flow" on page 17.
4. The ALM Octane site admin authenticates, and then updates the ROLE for this cluster node in the SERVER table using the REST API.

```
PUT https://<server>:<port>/admin/servers

{  "data": [
       {

           "role":"WORKER",
```

```
            "id":"<serverID>"
        }
    ]
}
```

For details on authenticating and working with the REST API, see Overview for developer in the ALM Octane Help Center.

5. Start the ALM Octane server.

See also:

- "Management" on page 66

Using exception files for manual database changes

This topic provides instructions for defining exception files. Use exception files if the organization's DBA added objects to database schemas, such as tables, indexes, stored procedures, columns, or other objects.

This section includes:

Overview

Exception files instruct ALM Octane to ignore any errors issued because of manual additions to the database schema. These errors would typically stop the installation or upgrade process.

You can use exception files to ignore errors for extra tables, views, columns, and sequences. For any other problem, consult with your database administrator.

> **Caution:** Using the exception file to ignore errors for objects that are added manually to the schema may compromise stability and the validity of the database user schema.

You can use the exception files during a new ALM Octane installation, when upgrading, and when creating a space.

Define exception files

Define exception files before installation, before upgrading, or before you create the new spaces.

To define exception files:

1. Copy both of the **mqm_exception.xml** files from the ALM Octane installation directories. You can rename them.
2. Locate the MQM_EXCEPTIONS part of the file.

```
<MQM_EXCEPTIONS>
    <exceptions>
        <declaration>
            <!--<object pattern="TABLE_1_EXAMPLE" type="missing"
/>-->
            <!--<object pattern=" TABLE_1_EXAMPLE" type="extra"
/>-->
        </declaration>
    </exceptions>
</MQM_EXCEPTIONS>
```

3. Change the <declaration> to one of the following. Add as many declarations as you need.
   - TableMissing
   - ViewMissing
   - ColumnMissing
   - ConstraintMissing
   - IndexMissing

- PartitionFunctionMissing
- PartitionSchemeMissing
- ProcedureMissing
- SequenceMissing
- TriggerMissing

4. For each object pattern, you can specify one of the following types:

missing	The object is needed but is missing.
extra	The object is extra because it was created after ALM Octane installation or before upgrading.

Examples

- For an extra table:

```
<TableMissing>
         <object pattern="MY_Table" type="extra"/>
</TableMissing>
```

- For an extra view:

```
<ViewMissing>
         <object pattern="MY_VIEW" type="extra"/>
</ViewMissing>
```

- For an extra column:

```
<ColumnMissing>
         <object pattern="MY_COLUMN" type="extra"/>
</ColumnMissing>
```

- For an extra sequence:

```
<SequenceMissing>
         <object pattern="MY_SEQUENCE" type="extra"/>
</SequenceMissing>
```

Set up use of the exception file

This topic explains how to use the exception file when installing ALM Octane or when creating a new space.

Use of the exception files during first-time installation

You can use exception files when installing ALM Octane using existing schemas/databases instead of having ALM Octane create new schemas for you. This is the **FILL_EXISTING** installation option and it is set in the **octane.conf** file.

1. During installation, when configuring the **/opt/conf/octane.conf** file in the configuration folder, add these two settings using an editor:

MqmExceptionsSiteAdminPath	The exception file for the site. **/opt/tmp/site/mqm_exceptions.xml**.
MqmExceptionsSharedSpacePath	The exception file for the default space. **/opt/tmp/shared_space/mqm_exceptions.xml**

2. Continue installing.
3. After the installation, check that the ALM Octane Server is up and that you have proper access to the site and the default space.

Use of the exception files when upgrading

You can use exception files when upgrading ALM Octane.

After installation, the exception files are copied to the repository folder. So when upgrading, modify the copies of the exception files in the repository folder instead of the files in the configuration folder.

1. During the upgrade, when configuring the **octane.conf** file in the repository folder, add or modify these two settings using an editor:

The exception file for the site	**/opt/octane/repo/storage/schema/maintenance/exceptions/site_admin/mqm_exception.xml**
The exception file for the new space	**/opt/octane/repo/storage/schema/maintenance/exceptions/shared_space/mqm_exception.xml**

2. Continue upgrading.
3. After the upgrade, check that the ALM Octane Server is up and that you have proper access to the site and the default space.

Use of the exception files when creating a space

ALM Octane processes the exception files also when adding new spaces.

After installation, the exception files are copied to the repository folder.

Before adding a new space, modify the copies of the exception files in the repository folder instead of the files in the configuration folder.

1. Add exceptions as necessary to the exception files using an editor:

The exception file for the site	**/opt/octane/repo/storage/schema/maintenance/exceptions/site_admin/mqm_exception.xml**
The exception file for the new space	**/opt/octane/repo/storage/schema/maintenance/exceptions/shared_space/mqm_exception.xml**

2. In ALM Octane Settings area, add the space using an existing schema. For details, see Create a space in the ALM Octane Help Center.
3. Check that you have proper access to the space.

See also:

- "Configure site settings" on page 37
- Troubleshooting: ""My FILL_EXISTING installation failed, indicating that I have extra tables, view, indexes, and so on."" on page 88

Troubleshooting

This section contains troubleshooting suggestions for issues relating to the ALM Octane installation.

You can also check the log here: **/opt/octane/log**

For an up-to-date list of installation troubleshooters, see knowledge base article KM02703217.

"ALM Octane displays an error indicating that the ALM Octane server is not responding. I cannot work in ALM Octane."

If ALM Octane is under a very heavy load, it might try to use too many Linux resources. In this case, Linux kills the server process. Do the following to increase the number of allowed open files to 65536:

1. Open the **/etc/security/limits.conf** file.
2. Add the following line:

   ```
   octane hard nofile 65536
   ```

3. Restart the ALM Octane server.

For details, see https://easyengine.io/tutorials/linux/increase-open-files-limit/.

"I rebooted the ALM Octane server machine. The **octane** service did not start up automatically."

When you reboot the machine, you need to manually restart the ALM Octane server:

```
systemctl restart octane
```

The service runs in the background.

"I cannot log into ALM Octane because ports are closed."

By default, the ALM Octane server uses port 8080 or port 8443 (secure). The port must be opened in the firewall for incoming traffic.

"I am unexpectedly logged out."

Typically, a user is logged out of ALM Octane only after session timeout. If, however, you are unexpectedly logged out while actively working in ALM Octane, you may need to clear cookies before you can log in again.

To prevent an unexpected logout:

- When working with a local DNS, make sure that you access ALM Octane only with a fully-qualified machine name, together with the machine's domain.

> **Example:** `http://myserver-123545.domain.com:8080/`

"JVM does not load."

If JVM fails to load after the **octane** service is started, check that Java is properly installed and that `JAVA_HOME` is configured correctly.

The **/opt/octane/log/wrapper.log** file shows the following error message:

```
ERROR  | wrapper  | JVM exited while loading the application.
INFO   | jvm 1    | Unrecognized VM option
'UseCompressedClassPointers'
INFO   | jvm 1    | Error: Could not create the Java Virtual
Machine.
INFO   | jvm 1    | Error: A fatal exception has occurred. Program
will exit.
```

To identify the important parameters of the system that may affect the installation, run the following commands:

To get...	Command
Java information	`java -XshowSettings:properties -version`
All installed Java applications	`find / -name java`

To get...	Command
All installed Java versions	`find / -name java -exec {} a \;`
The **JAVA_HOME** property	`echo $JAVA_HOME`
The **PATH** property	`echo $PATH`

"Application server address shows port 8080 even when changed."

By default, the installation uses port 8080 for HTTP or port 8443 for HTTPS (SSL). If you change the port to a non-default value after the initial installation phase, the site Servers tab shows:

- The original application server address still displays as port 8080.
- The server state is inaccessible even though the server is accessible.

"Failure to create SA schema due to nonexistent TableSpace or TempTableSpace."

If errors occur during site schema creation, and the **site.log** file contains a message indicating that a certain tablespace or a temporary tablespace does not exist, check that the specified TableSpace or TempTableSpace is correct.

"When initializing, the ALM Octane installation failed with a site schema problem."

If you receive a site schema error, such as "Cannot upgrade SA. SA schema version must be lower than the current server version," do the following:

1. Open a backup copy of the site schema.
2. Fix the problem.
3. Restart the server (meaning, run **systemctl restart octane** again).

"The **wrapper.log** has Java-related warnings (Linux)"

After installing or upgrading, the following warning appears in the **/opt/octane/log/wrapper.log** file.

```
INFO   | jvm 1    | 2017/06/27 17:20:56.318 | Caused by:
java.net.UnknownHostException: <…some host name…> unknown error
```

To eliminate this warning:

1. Add the ALM Octane server to the **/etc/hosts** file.

   Example: For non-dynamic IPs, you can add the server in this format:

   <*ip_of_machine*> <*name_of_machine*> `localhost`

   Such as: **192.168.0.185 machine-72 localhost**

2. Restart the ALM Octane Server. For details, see "Start the ALM Octane server manually" on page 66.

"My **FILL_EXISTING** installation failed, indicating that I have extra tables, view, indexes, and so on."

Check if your DBA made manual additions to the database schema, such as adding tables, indexes, and so on. If the installation encounters objects that it does not expect in the database schema, the installation can fail.

To avoid this, create exception files. For details, see "Using exception files for manual database changes" on page 79.

If you still have problems:

- Check that the parameters in the **octane.conf** file and the exception files have been entered correctly.
- Check the **/opt/octane/log/wrapper.log** for errors.

ALM Octane cannot fetch Jetty files

The **conscript** library allows you to enable HTTP/2 in Jetty. Sometimes, however, using the conscript library causes issues. To resolve these issues, disable the **conscript** library and switch back to native Java SSL. For instructions, see knowledge base article KM03310408.

Exception thrown when creating a space

Under heavy loads, ALM Octane can use more threads than allocated for the octane service by Linux. In this case the admin needs to check the settings for the maximum number of threads for ALM Octane, and compare it with the current number of used threads.

The maximum number is stored in the file **/sys/fs/cgroup/pids/system.slice/octane.service/pids.max**.

The current number of threads is stored in the file **/sys/fs/cgroup/pids/system.slice/octane.service/pids.current**.

If the current number is approaching the maximum, increase the number of maximum threads using the command:

```
systemctl set-property octane.service TasksMax=<new maximum number>
```

Restart the octane service after this change.

> **Note:** For some Linux variants these locations and commands may be different. The system administrator should handle this process.

See also:

- "Management" on page 66

Checking logs

ALM Octane's log files are stored in the **/opt/octane/log** directory, or the directory that you specified when you deployed.

This section includes:

- "Log files" below
- "Monitor the deployment procedure" below

Log files

Log	Path
Application logs	**/opt/octane/log/nga/app/app.log**
Site logs	**/opt/octane/log/nga/site/site.log**
octane service (server) logs	**/opt/octane/log/nga/wrapper.log**
Overall **octane** log, which summarizes the contents of day-to-day log files in one file.	**/opt/octane/log/nga/octane.log**

Monitor the deployment procedure

Run the following command and wait until you see a **server boot complete** message:

```
tail -f /opt/octane/log/wrapper.log
```

See also:

- "Management" on page 66

Uninstall

This section describes how to uninstall the ALM Octane server.

To uninstall the ALM Octane server:

1. Query the package name. Run:

```
rpm –q octane
```

2. Uninstall ALM Octane. Run:

```
rpm -e <package name>
```

3. The uninstall process does not delete the repository, log, and configuration directories, in case you want to reinstall. Delete them if necessary:

```
rm -rf /opt/octane
```

See also:

- "Installation" on page 33