ALM Octane

Software Version: 12.60.35

Installation Guide for Linux

Go to **HELP CENTER ONLINE**
http://admhelp.microfocus.com/octane/

Document Release Date: March 10, 2019 | Software Release Date: February 2019

Legal Notices

Disclaimer

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

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Contains Confidential Information. Except as specifically indicated otherwise, a valid license is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

Comodo Code Signing Certificate

The code signing certificate for ALM Octane was changed from Verisign to Comodo starting on January 1, 2017.

If you are installing this product on a computer with an older version of Windows, or on a computer without automatic Windows updates, the Comodo root certificate may not automatically be included as a trusted root certificate.

In such cases, we recommend manually configuring Comodo as a trusted root certificate.

For more details, see: https://technet.microsoft.com/en-gb/library/dn265983.aspx.

Contents

Architecture

You can set up 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.

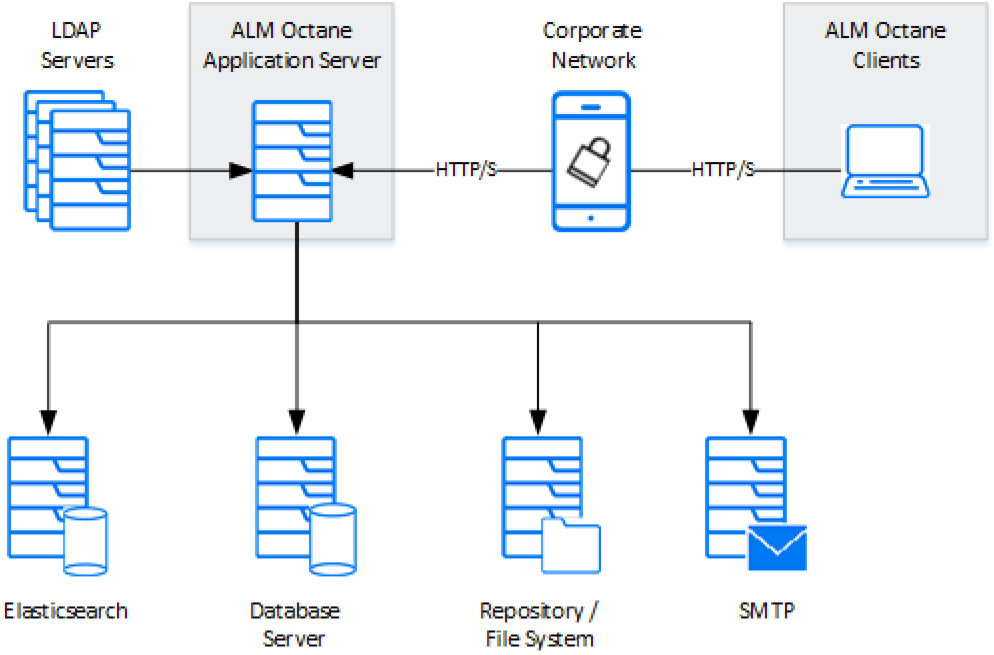
- "Basic configuration" below
- "Enterprise configuration" below
- "Components" on the next page

Basic configuration

The following diagram illustrates the system architecture of a single-node configuration.

Components in grey are Micro Focus products.

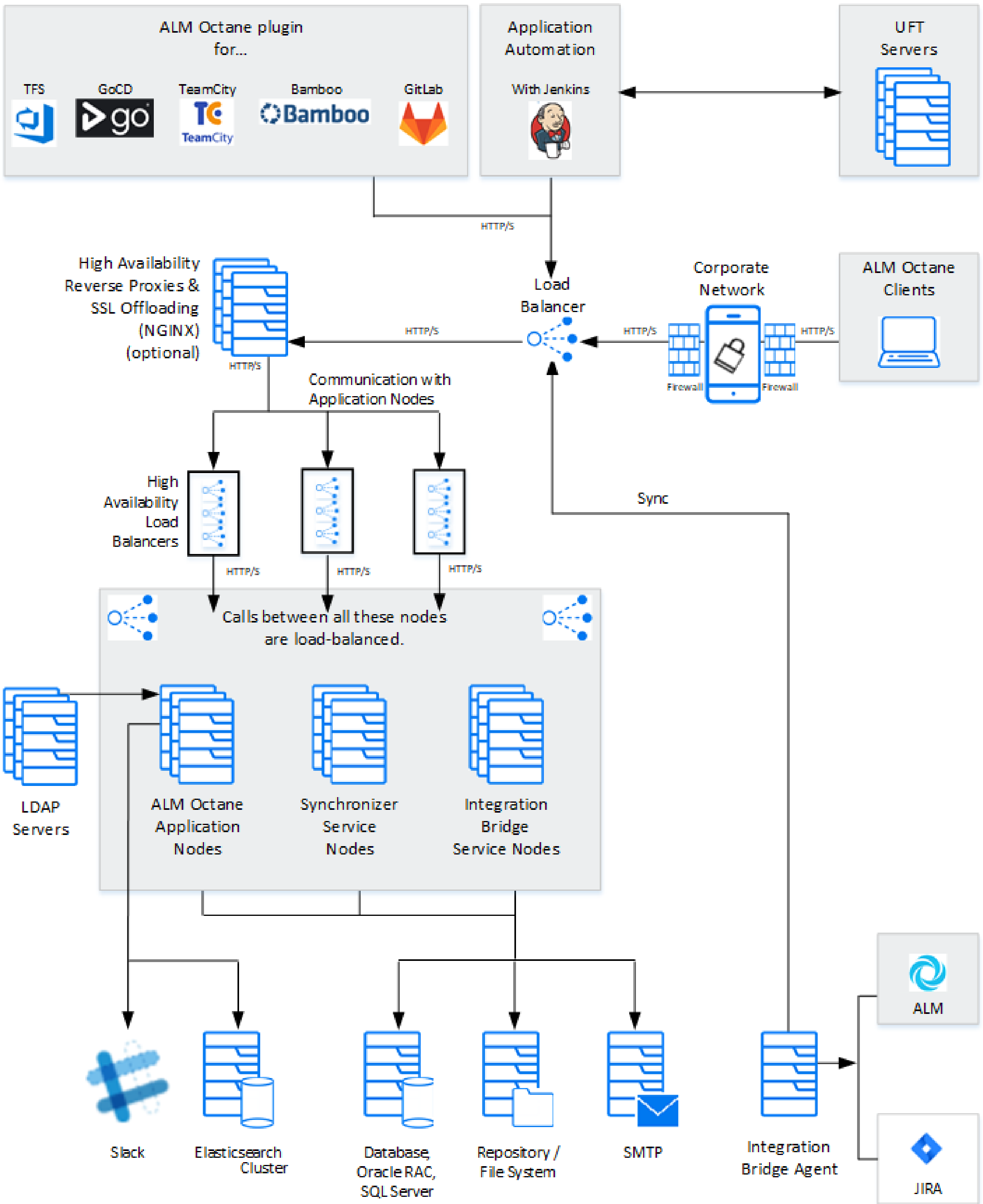
> **Note:** The ALM Octane, database, and Elasticsearch servers should each reside on separate machines.



Enterprise configuration

The following diagram illustrates the system architecture of an enterprise, cluster configuration:

Components in grey are Micro Focus products.



Components

Components	Description
ALM Octane clients	The clients communicate with the ALM Octane server over HTTP/S.

Components	Description
Integration bridge and external sources	**Enterprise configuration**: The integration bridge enables ALM Octane to integrate with external applications ("off-organization" communication). This is generally optional, but required for synchronization. Also used for Trigger Webhook rules to an endpoint URL, SaaS deployments, and for communication between Micro Focus SaaS and an on-premises deployment.
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 will be 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.
Integration bridge service nodes	The service handles communication between the Integration Bridge and Synchronizer.
Synchronizer service nodes	The service nodes handle synchronization between ALM Octane and ALM or JIRA.
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: • **Space schema**. All space information, such as workspaces, users, and roles.. • **Site schema**. Stores all site-related information, such as database servers, cluster nodes, the SMTP servers, and configuration. 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 will 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 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 will not support the database 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 the requirements for database and Elasticsearch in the *ALM Octane* *Help Center*. • For details on installing Elasticsearch, see knowledge base article KM02494295. • For details on upgrading to a new Elasticsearch version, see knowledge base article KM03207448.
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.

Components	Description
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.
TeamCity, Bamboo, or TFS server (with ALM Octane plugin)	**Enterprise configuration**: You can integrate ALM Octane with a TeamCity, Bamboo, or TFS CI server using the ALM Octane CI 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.
Micro Focus testing tools: LeanFT, UFT, LoadRunner, StormRunner Functional, StormRunner Load, Performance Center	You can integrate ALM Octane with Micro Focus testing tools. For details, see ALM Octane DevOps integrationsthe topic on ALM Octane DevOps integrations in the *ALM Octane Help Center*.

See also:

- "Prerequisites" on page 17
- "Installation types" on the next page
- "Installation flow" on page 15
- "Installation" on page 27
- "Deploy ALM Octane" on page 28

Installation types

This topic 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" on page 27. • A cluster configuration. For details, see "Cluster installation (optional)" on page 55.
Upgrade	For details, see "Upgrade" on page 59.

See also:

- "Prerequisites" on page 17
- "Deploy ALM Octane" on page 28
- "Configure initial site settings " on page 30
- "Configure other settings" on page 38

Licensing flow

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

In this topic:

- "Overview" below
- "Request a trial" below
- "Using Pro Edition" below
- "Installing a license" on the next page

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 Quality Center.

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

Request a trial

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

When you install ALM Octane, you can choose between an Enterprise Edition or Team Edition trial. For details on selecting your trial, see the topic on license settings and trials in the *ALM Octane Help Center*.

> **Caution:** If you want to use the Pro Edition, choose the Enterprise Edition for your trial. Make sure to follow the instructions under "Using Pro Edition" below.

You cannot switch between editions once configuration is done, so choose your trial and editions carefully. If you chose the wrong edition, re-install ALM Octane.

Using Pro Edition

There is no Pro Edition trial. To work with Pro Edition:

1. Install ALM Octane and select 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" on the next page.

Installing a license

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

Alternatively, you can allocate your current licenses from ALM or Quality Center 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.

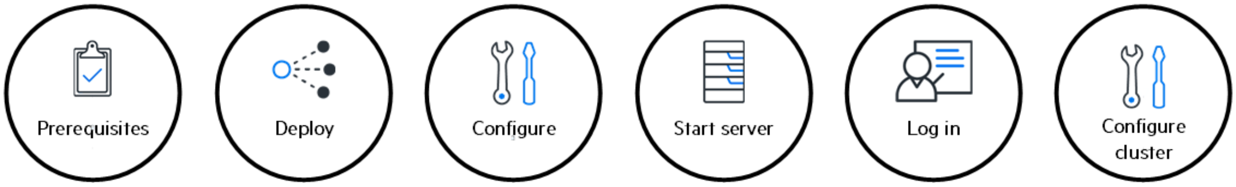
To learn more, see the topic about managing licenses in the *ALM Octane Help Center*.

Next steps:

- "Installation flow" on the next page

Installation flow

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



In this topic:

- "Prerequisites " below
- "Deploy " below
- "Configure " on the next page
- "Start the server" on the next page
- "Log in " on the next page
- "Cluster configuration (optional) " on the next page

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 17 and "Best practices" on page 105.

> **Note:** We recommend you review security considerations in the knowledge base article KM02707977. This article 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 28and "Best practices: Deploying ALM Octane" on page 106.

Configure

Configure ALM Octane by editing these files with your site's settings:

- **setup.xml** for initial configuration
- **octane.yml** for ongoing configuration

The path to these files is **/opt/octane/conf**.

For details, see "Configure initial site settings " on page 30and "Configure other settings" on page 38.

Start the server

Start the ALM Octane server:

```
service octane start
```

For details, see "Start the ALM Octane server" on page 53.

Log in

Verify that ALM Octane was properly installed. For details, see "Checking logs" on page 120.

Log into ALM Octane. For details, see "Log in to ALM Octane" on page 54.

Cluster configuration (optional)

After starting the server on the first machine, configure and initialize each additional cluster node. For details, see "Cluster installation (optional)" on page 55.

See also:

- "Prerequisites" on the next page
- "Deploy ALM Octane" on page 28
- "Configure initial site settings " on page 30
- "Configure other settings" on page 38
- "Cluster installation (optional)" on page 55

Prerequisites

Verify that your system meets the requirements listed below, and that permissions are assigned as necessary, as described under "System Requirements" in the *ALM Octane Help Center*.

For security requirements, see Software Self-solve knowledge base article KM02707977.

In this topic:

- "System requirements" below
- "Checklist" on page 21
- "Permissions" on page 25

System requirements

System requirements are described below.

Hardware

Component	Type	Value
Screen resolutions Screen resolutions between the recommended and minimum values are also supported.	Recommended	1920 x 1080
	Minimum supported	1024 x 768

Component	Type	Value
Production environments: Contact customer support for the most up-to-date be benchmark documentation.	**Recommended**: 2 ALM Octane server machines, minimum **Minimum**: 1 ALM Octane server machine	CPU: 4 RAM: 8 GB Heap: Max 4 GB Disk space: At least 500 GB (network storage recommended)
	1 database server machine	CPU: 8 RAM: 16 GB
	Recommended: 3 Elasticsearch server cluster machines **Minimum**: 1 Elasticsearch server machine	CPU: 4 and higher RAM: 8 GB
	1 load balancing component (load balancer or reverse proxy) to enable cluster	
Pre-production or test environments: **(Recommended values)** Contact customer support for the most up-to-date be benchmark documentation.	1 ALM Octane server machine	CPU: 4 RAM: 8 GB Heap: Max 4 GB Disk space: 200 GB
	1 database server machine	Can be an existing database server. CPU: 8 RAM: 16 GB
	1 Elasticsearch server machine	CPU: 4 and higher RAM: 8 GB
Virtual machines	VMware or any virtual machine is supported, provided it has dedicated resources.	

Software

Component	Type	Version
Server operating system	CentOS	6.5 or later We strongly recommend 7.2 and later.
	Suse	12 with SP1 or SP2
	Red Hat Enterprise Linux (RHEL)	6.5 or later We strongly recommend 7.2 and later.
Browser	Chrome (recommended)	Chrome: The two latest versions Chrome for business
	Firefox (recommended)	Firefox: The two latest versions ESR: 52
	Internet Explorer	11
	Apple Safari	10, 11
JDK		Open/Oracle JDK 8 Java 8 only. Make sure the latest security updates are installed on the ALM Octane server at all times.

Database and Elasticsearch

Component	Type	Version
Database	Oracle	12C Standard or Enterprise edition, with character set AL32UTF8
	SQL Server	2016, 2014 or 2012 SP3 Case-insensitive collations only.
Elasticsearch	N/A	5.6.X • For details on installing Elasticsearch, see knowledge base article KM02494295. • For details on upgrading to a new Elasticsearch version, see knowledge base article KM03207448.

Installation, setup and synchronization

Component	Version
Cloud environments	Amazon Web Services (AWS) Microsoft Azure
LDAP Server	Active Directory, or any LDAP provider supporting the LDAP3 protocol
Synchronizer	Red Hat Enterprise Linux (RHEL) 6.5 and later CentOS 6.5 and later
JIRA synchronization	JIRA 7.2.8 and later
ALM/Quality Center synchronization	ALM/Quality Center 12.60 patch 1, 12.55, 12.53, 12.50, 12.21, 12.01 patch 1 and later
ALM/Quality Center license sharing	ALM 12.60, 12.55, 12.53 (all patch levels), 12.21 patch 6 Quality Center 12.60, 12.55 patch 1, 12.53 (all patch levels), 12.21 patch 6 Note that 12.53 versions require a hotfix.
Upgrade path	Only from 12.53.20

Checklist

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

Category	Tell us...	Your answer...
ALM OCTANE	On which machine will you be installing 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 will use for the installation user?	
	Does the installation user have **sudo** permissions? See "Permissions" on page 25.	
	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 Elasticsearch enables trend reporting and search functionality in ALM Octane.	What is the Elasticsearch version that matches ALM Octane requirements?	
	Do you need to download Elasticsearch? You can download Elasticsearch from https://www.elastic.co/downloads/past-releases/elasticsearch-5-6-5.	
	Did you check Software Self-solve knowledge base articles? • Elasticsearch installation and configuration: KM02494295 • Upgrading to a newer Elasticsearch version: KM03207448	
	On which machine is Elasticsearch installed?	
	What is the Elasticsearch port? Default: 9300 You can modify the port in **setup.xml**.	
	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?	
	Was Elasticsearch configured according to ALM Octane requirements? For details, see the information about "Database and Elasticsearch" in the *ALM Octane Help Center*.	
	Is the Elasticsearch accessible from the ALM Octane server?	

Category	**Tell us...**	**Your answer...**
ORACLE	Does your Oracle version match ALM Octane requirements? For details, see Database and Elasticsearch.For details, see the information about "Database and Elasticsearch" 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 **ConnectionString** field in **setup.xml**.	
	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 "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 92.	

Category	Tell us...	Your answer...
Microsoft	Does your SQL Server version match ALM Octane requirements? For details, see Database and Elasticsearch.	
	On which machine is the database installed?	
	Will you be using 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 "Permissions" on the next page.	
	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 92.	
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? For details, see the JDK system requirements 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.yml**.	
hazelcast	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**.	

Permissions

ALM Octane requires the following permissions for the file system and for the database.

File system

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.

Oracle database

These are the permissions user you will define for the user you will specify in the **DBAdminUser** setting in the **setup.xml** file. For details, see "Configure initial site settings " on page 30.

Permissions vary depending how you work with ALM Octane and how you want to install.

Do you want ALM Octane to create schemas, objects, and tables during the installation?

Yes	Provide ALM Octane with an Oracle power user with the following admin privileges, so that ALM Octane can create schemas and objects automatically during the installation. • 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. If the database at your site is managed by database administrators, and ALM Octane is not authorized to create its own schemas, this power user can 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 the topic about creating spaces for a site n the *ALM Octane Help Center*.

No	Provide ALM Octane with a regular Oracle user with the following permissions. Create the schemas before installation. • CREATE TABLE • CREATE SESSION • CREATE SEQUENCE • The QUOTA clause on the user's default tablespace should be unlimited.

SQL Server Database

These are the permissions user you will define for the user you will specify in the **DBAdminUser** setting in the **setup.xml** file. For details, see "Configure initial site settings " on page 30.

Permissions vary depending how you work with ALM Octane and how you want to install.

Do you want ALM Octane to create databases and the login user during the installation?

Yes	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**: 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.
No	Create an ALM Octane database admin power user for installation purposes. 1. Open the **SQL Server Management Studio**. 2. In the **Object Explorer** pane, under the ALM Octane database server, expand the **Security** directory. 3. Right-click the **Logins** directory, and select **New Login**. 4. Type, for example, **octane_install_power_user** as the user name, and select the authentication type (enter the password if necessary). 5. Click the **Server Roles** tab, and select the **dbcreator** and **securityadmin** options. Click **OK**.

Next steps:

- "Deploy ALM Octane" on page 28

Installation

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

Before installing:

- Verify that your server fulfills all prerequisites. For details, see the prerequisites in the *ALM Octane Help Center*.
- Review security considerations in the knowledge base article KM02707977.

Cluster configuration: If you intend to install ALM Octane in a cluster configuration, review the end-to-end process under "Cluster installation (optional)" on page 55 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.

In this topic:

- "Overview" below
- "Prerequisites" below
- "Deploy" below
- "Deploy in cluster environment" on the next page

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. For details, see the prerequisites in the *ALM Octane Help Center*.
- Review security considerations in the knowledge base article KM02707977.

Deploy

1. Download the ALM Octane RPM package:

   https://www.microfocus.com/en-us/products/application-lifecycle-management-octane-on-prem/download
2. Install the ALM Octane RPM package.
   - To install the ALM Octane RPM package in the default installation directory **/opt/octane**, run:

     ```
     rpm -Uvh <name of the RPM file>
     ```
   - Alternatively, install the ALM Octane RPM package to a different directory:

     ```
     rpm -Uvh --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.

3. 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 that user performing the installation (generally, the **octane** user) can write to the repository.
   - **Single-node configuration**:

     On the ALM Octane server, create a mount directory that points to the file repository directory.
   - **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.
     - It is important that you enter the repository path using the same path name on all nodes. For example, you cannot have the path on the first server node defined as **/opt/octane/repo** and on additional nodes defined as **/server1/opt/octane/repo**.
     - If the repository is not located on a remote, dedicated machine, the repository location cannot be **/opt/octane**.
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

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.yml** file. For details, see "Configure other settings" on page 38.
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.

Next steps:

- "Configure initial site settings " below

Configure initial site settings

You can configure initial site settings using the **setup.xml** file. You must configure the settings in the **setup.xml** file during the ALM Octane installation.

> **Caution:** These settings cannot be changed later.

In this topic:

- "Overview" below
- "Database server settings" on the next page
- "Oracle server settings" on page 34
- "SQL server settings" on page 34
- "Site actions " on page 34
- "Space settings" on page 35
- "Elasticsearch settings" on page 36
- "Site admin credential settings" on page 37
- "Repository settings" on page 37
- "Configure initial site settings " above
- "Additional settings" on page 38

Overview

Configure these settings by editing the **setup.xml** file, for example, with an editor such as nano: `nano /opt/octane/conf/setup.xml`

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 setup.xml`

It is recommended that you save a local copy of the **setup.xml** file before making changes to it.

Also, for security purposes, **setup.xml** should be stored in a secure, off-site location.

Database server settings

The Oracle settings can be used for both Oracle and SQL server.

Oracle settings	Description
DBType	The supported database types are: - ORACLE - MSSQL
SchemaName	The name of the site schema that is created by the **DBAdminUser** during the installation, or supplied by the organization's DBA. Enter the supplied name.
SchemaPassword	**For Oracle**: - The password of the site schema. Enter the supplied password. - When using Oracle, and 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 **SchemaPassword**. **For SQL Server**: The password for the **DBLoginUser** user.
MssqlLoginName ForSetup	ALM Octane uses the **DBAdminUser** both to create objects during installation and also to check that the database server is accessible. **For Oracle:** - The name of the database admin user (**DBAdminUser**). - When using Oracle, and installing using existing site schemas (with the **FILL_EXISTING** site action), enter the **SchemaName**. **For SQL Server:** Login object for logging into the database instance. ALM Octane uses this login for setup, tables, and indexes. - This is either the **sa** user or an SQL Server power user with the correct permissions. - When using SQL Server, and installing using the **FILL_EXISTING** site action, enter the **DBAdminUser** value. For details about **DBAdminUser** permissions, see "Permissions" on page 25. For the **FILL_EXISTING** site action, make sure to also specify **SharedSpaceSchemaName**.

Oracle settings	Description
DBAdminPassword	**For Oracle:** The password of the database admin user (**DBAdminUser**). - Do not include a pound sign (**#**) or accented characters (such as, **ä**, **ç**, **ñ**). - When installing using existing site schemas (with the **FILL_EXISTING** site action), enter the **SchemaPassword**. **For SQL Server:** Password for **the** sa user or the SQL Server power user defined with the **DBAdminUser** setting. - When installing using existing site database instances (with the **FILL_EXISTING** site action), enter the **SchemaPassword**.

Oracle settings	Description

ConnectionString	The Java Database Connectivity (JDBC) database connection string. It includes the following details: database type, database server name, database server port number, service name.
	The instructions below demonstrate how to set up the string with non-secured database access. However, you can use this connection string to configure secure access to the database. For details, see "Configure secure database access" on page 88.
	Oracle
	• **Syntax using TNS alias names:**
	To use TNS alias names, make sure to provide a value for the **DBServerName** setting.
	`<entry key="ConnectionString">jdbc:mercury:oracle:TNSNamesFile=/<path>/tnsnames.ora;TNSServerName=<server_name></entry>`
	Example:
	`jdbc:mercury:oracle:TNSNamesFile=/etc/tnsnames.ora;TNSServerName=ora12`
	• **Syntax using service names:**
	`<entry key="ConnectionString">jdbc:mercury:oracle://DB_SERVER_NAME:DB_SERVER_PORT;servicename=DB_SERVICE_NAME</entry>`
	Example:
	`jdbc:mercury:oracle://dbserver1.net:1521;servicename=orcl`
	To connect to Oracle RAC, use the Single Client Access Name (SCAN) instead of the database server name.
	SQL
	• **Syntax using port:**
	`<entry key="ConnectionString">jdbc:mercury:sqlserver://DB_SERVER_NAME:DB_SERVER_PORT</entry>`
	Example:
	`jdbc:mercury:sqlserver://dbserver1:1433`
	• **Syntax using instance:**
	`<entry key="ConnectionString">jdbc:mercury:sqlserver://DB_SERVER_NAME/INSTANCE_NAME</entry>`
	Example:
	`jdbc:mercury:sqlserver://dbserver1:my_instance`

Oracle server settings

Oracle settings	Description
TableSpace	The tablespace in the Oracle database where the site schema segment will be created. Case-sensitive.
TempTableSpace	The temporary tablespace in the Oracle database. Case-sensitive.
DBServerName	The TNS alias name for connecting to the Oracle database. Optional. For use with "Configure initial site settings " on page 30. **Example**: **dbserver1.net**
DBServerPort	The port for connecting to the Oracle database.

SQL server settings

SQL Server settings	Description
DbLoginUser	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. Specify the password for this user using the **SchemaPassword** setting. Do not include a pound sign (**#**) or accented characters (such as, **ä**, **ç**, **ñ**). If the **DBLoginUser** user already exists, make sure to use the existing user's password.

Site actions

The **SiteAction** setting determines how the installation should handle databases. Possible values:

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 a **DBAdminUser** 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 admin user does not give permissions to create a schema (for Oracle) or a database (for SQL Server)..
	For SQL Server:
	Two databases are created, one for the site and one for the space. Both are created by the DBA.
	• The default collation is **SQL_Latin1_General_CP1_CI_AS** (must be case-insensitive).
	• Make sure you specify these databases in the **SchemaName** and **SharedSpaceSchemaName** settings, because they are mandatory.
	• Make sure you define the **DbLoginUser** setting.
	For Oracle:
	Two schemas are created, one for the site and one for the space. Both are created by the DBA.
	SharedSpaceSchemaName should have the same password as **SchemaName**.
	Make sure that the passwords that the DBA defines for the site schema and the shared space schema both match the **SchemaPassword** setting.
	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 92.
	For SQL Server: Example of creating a database and granting user access
	`CREATE DATABASE <database_name>`
	`CREATE LOGIN <login_name> WITH PASSWORD = 'thepassword', CHECK_POLICY = OFF`
	`USE` <*database_name*>
	`sp_adduser '<logName>' , 'octane'`
	`GRANT ALL TO octane sp_addrolemember 'db_ddladmin','octane'`

Space settings

Where relevant, the Oracle settings can be used for both Oracle and SQL server. Alternatively, for SQL Server, you can specify the SQL Server settings instead.

Oracle settings	SQL Server settings	Description
SharedSpaceSchemaName	**MssqlSharedspaceDatabaseName**	Relevant only for the **FILL_EXISTING** site action. **For Oracle**: To configure the space, add a **SharedSpaceSchemaName** parameter and set it to the name of the schema that is designated for the space. **For SQL Server**: To configure the space, add a **MssqlSharedspaceDatabaseName** parameter and set it to the name of the database that is designated for the space.

DefaultSpaceMode	*<NA>*	The mode in which the initial space will be created when the ALM Octane server starts. Valid values are:
		• **isolated**. Workspaces associated with the initial space will not share entities or customization settings.
		• **shared**. Workspaces associated with the initial space can share entities or customization settings.
		Examples:
		`<entry key="DefaultSpaceMode">isolated</entry>`
		`<entry key="DefaultSpaceMode">shared</entry>`

Elasticsearch settings

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 the requirements for Database and Elasticsearch.
- For details on installing Elasticsearch, see knowledge base article KM02494295.
- For details on upgrading to a new Elasticsearch version, see knowledge base article KM03207448.

ElasticHost	The name of the host running Elasticsearch. If running an Elasticsearch cluster, all node host names should be separated by semi-colons (**;**). **Example**: **host1;host2;host3**
ElasticPort	The number of the port running the Elasticsearch binary service. This port must be accessible from the ALM Octane server, not just by checking the HTTP connection. **Example**: **9300**
ElasticClusterName	The name of the Elasticsearch cluster.

Site admin credential settings

SiteAdministratorUser	The email of the site admin user that the installation will create. 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).
SiteAdministratorPassword	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.

Repository settings

RepositoryFolder	The full path of the repository directory. **Example**: **/opt/octane/repo** **Cluster configuration**: • The directory specified here must be accessible to all cluster nodes. • If the repository is not located on a remote, dedicated machine, the repository location cannot be **/opt/octane**.

Additional settings

AppURL	The fully-qualified domain name and port for the ALM Octane server. This URL is 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.

Next steps:

- "Configure other settings" below

Configure other settings

You can configure additional site settings using the **octane.yml** file. These settings are configured during installation, and can also be changed any time, whenever necessary.

In this topic:

- "Overview" below
- "Rules for editing the octane.yml file" on the next page
- "General server settings" on the next page
- "LDAP settings" on page 41
- "License settings" on page 45
- "Oracle settings" on page 46
- "Cluster settings" on page 46
- "ALM Octane service provider (SP) settings" on page 47

Overview

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 setup.xml`

If you update any of these settings at a later time, make sure you restart the ALM Octane server. 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.

Configure these settings by editing the **octane.yml**, for example, with an editor such as nano:

```
nano /opt/octane/conf/octane.yml.
```

Rules for editing the octane.yml file

> **Caution:** Correct indentation and formatting is essential when editing **yml** files to avoid unpredictable results during installation.

There are resources available online that describe the exact rules and conventions for formatting **yml** files. We strongly recommend that you familiarize yourself with these rules before editing **octane.yml**.

Here are some important rules when editing settings in **octane.yml**:

- Put a single space after the colon between the parameter name and the value.
- Do not add bullets or any other extra formatting.
- Do not add extra spaces.
- Use double quotes to enclose any values that include special characters, especially the **#**.

  A **#** that is not enclosed in quotes marks the beginning of a comment. Any text after it, until the end of the line, is ignored. The **octane.yml** file is then interpreted incorrectly during installation and causes errors.

If these conventions are not followed, ALM Octane initialization or upgrade can fail.

For an example, see the sample **octaneExample.yml** file.

General server settings

cluster	**Cluster configuration**: Enter a comma-separated list of node host names or IPs in the cluster. **Example: 10.0.0.24,10.0.0.99,10.0.0.23** This is a mandatory setting. By default, the cluster is not configured, and the default value is blank. This indicates a standalone ALM Octane server.

heapSize	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. **heapSize** should be set 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**

server	The value of a Jetty port for HTTP, or a Jetty secure port for HTTPS.
	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.

proxy	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. An example of accessing an external server is when using a Trigger webhook rule. host: <*proxy_host*> port: <*proxy_port*> user: <*user*> password: <*password*>
authenticationType	Whether the ALM Octane installation should use native user management or LDAP authentication for user management. Values are: **sso**. Use SSO authentication. **ldap**. Use LDAP authentication. **internal**. Use internal, native ALM Octane user management. Default.

LDAP settings

LDAP settings can be configured in the ALM Octane Settings UI. As you configure LDAP in Settings, the changes you make are automatically validated and updated in the **octane.yml** file. For details, see the information about configuring LDAP in the *ALM Octane Help Center*.

If you are planning on authenticating users using LDAP, and you prefer to work directly in the **octane.yml** file, set the **authenticationType** setting to **ldap**, and define the following settings. LDAP settings are validated when you start ALM Octane.

Later, after ALM Octane installation, import users from LDAP into ALM Octane. See the information about setting up LDAP user authentication in the *ALM Octane Help Center*.

> **Note:** After updating the **octane.yml** file, 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

connectionTimeout	Connection timeout in seconds. Optional. Default: 30 seconds
adminDn	The user that will log on 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 will not start. Correct the user details and restart the server. This user can be same user as the user entered in the **setup.xml** 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 **setup.xml** 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 **adminDn** is changed and the server is restarted, both the original **adminDn** and the new **adminDn** exist as site admins. Modifying the **adminDn** does not remove the original one.

LDAP server settings

Enter the following settings for each LDAP server separately.

Each LDAP server is defined by a group of settings. The settings for each LDAP server start with a hyphen (**-**) followed by the **host** setting.

> **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. Prefix each host item with a **-** sign: **- host**. This instructs ALM Octane where each host begins, especially if there are multiple LDAP servers.
port	LDAP server connection port. Mandatory.
isSsl	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 84.
description	Description of the LDAP server. Optional.

baseDirectories	Root of the LDAP path to use to search for users when including new LDAP users in ALM Octane spaces. This can be a semi-colon delimited list of common names and domain components (cns and dns), a list of organizational units (ou), and so on.
	Optional. Default: Blank.
	Make sure to put a space after hyphen (**-**) before specifying the filter.
	Example:
	`baseDirectories:`
	`  - ou=Groups,o=organization.com`
	`  - dc=maxcrc,dc=com`

baseFilters	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=*)
	Make sure to put a space after hyphen (**-**) before specifying the filter.
	Example:
	`baseFilters:`
	`  - (objectClass=*)`
	`  - (&(objectClass=user)(objectCategory=person))`

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, **user** and **password**. • **simple**. **user** and **password** are mandatory.
user	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 octane.yml	**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**. **Example** 1. If in LDAP, the **entryDN** attribute value is: **cn=<*common_name*>,ou=<*organizational_unit*>,dc=<*part_of_domain*>** 2. In the **octane.yml**, 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**
	entryDN **(for other LDAP systems)**	

ALM Octane attribute in octane.yml	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)**	
firstName	**givenName**	LDAP attribute for first name, such as **givenName**. Mandatory.
lastName	**sn**	LDAP attribute for last name, such as **sn**. Mandatory.
fullName	**cn**	LDAP attribute for full name, such as **cn**. Optional.
logonName	**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 **logonName**. Mandatory. You can change the **logonName** attribute mapping at any time, but make sure the **logonName** 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.

License settings

Locate the section called **license**, and enter values for the following settings.

Caution: If you plan to install a license for Team Edition at a later stage, you must enter **team** in the **trialEdition** field now.

Installing a license for Team Edition after an Enterprise Edition trial is not supported.

trialEdition	Enter **team** or **enterprise**, depending on your trial edition. For details, see the information about ALM Octane editions in the *ALM Octane User Guide*. **Note:** This setting is used the first time the ALM Octane server starts, and cannot be changed retroactively.
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 **almSharing**. You then need to fill in the following fields as described below.
The following fields are mandatory for almSharing mode:	
url	Enter the full path that you use to access ALM. Typically, this includes the suffix **qcbin**.
almIntegrationUser	Enter the user name for accessing ALM. This user was defined in ALM for integration purposes.
almIntegrationPassword	Enter the password for the **almIntegrationUser**. This password is automatically encrypted after you restart the ALM Octane server.

Oracle settings

The following Oracle section and its settings are also available.

Section	Setting	Description and usage

oracle_ database:	**useDefaultSort**	**For Oracle databases**: 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)
		Usage:
		`oracle_database:`
		`  useDefaultSort: no`

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 (optional)" on page 55.

cluster:	Section header. Do not edit.
	`cluster:`
	`    isCluster: true`
	`    nodes:`

isCluster Available with 12.60 CP8 and later.	Whether your server is standalone or in a cluster configuration. Mandatory. For a cluster configuration, set this value to **true**. You must enter node host names in the **nodes** setting. For a standalone server, set this value to false and do not enter any host names using the **nodes** setting. Default: **true**

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. **Examples**: • server1.domain.com,server2.domain.com,server3.domain.com • 120.150.12.12,120.150.80.13,120.150.32.14 Make sure **isCluster** is set to **true**.

ALM Octane service provider (SP) settings

The following service provider (SP) section and its settings are also available. Use these settings to set up SSO authentication for connecting to ALM Octane.

For these settings to take affect, make sure to set the authentication type to **sso** in this **octane.yml** file using the **authenticationType** setting.

For an example of setting these parameters, see the **octaneExample.yml** file.

Main settings

Setting	Description and usage
sso.key-pair.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**
sso.key-pair.pwd	Password for protecting and encrypting the key pair defined with **sso.key-pair.alias**. When ALM Octane starts, it encrypts this password. Mandatory. Example: **my-secret**

Setting	Description and usage
sso.keystore.file	The absolute path to the keystore file identified with **sso.key-pair.alias**. The default format for this file is **PKCS12**. You can change the format to Java KeyStore (JKS) by specifying this type when adding the **sso.oauth-keystore.type** setting to **octane.yml**. The path should be under ALM Octane's configuration folder to avoid permission issues. Mandatory.
sso.keystore.pwd	Password used to protect the keystore file defined with **sso.keystore.file**. When ALM Octane starts, it encrypts this password. Mandatory. Example: **my-password**
sso.login.saml2.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 **sso.login.saml2.idp.metadata** setting. Mandatory, if **sso.login.saml2.idp.metadata** is not defined. Example: **http://my-server.company-infra.net:8080/auth/realms/Dev/protocol/saml/descriptor**

Setting	Description and usage
sso.login.saml2.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. If metadata is provided using this setting, the URL defined in **sso.saml2.idp.metadata-url** is ignored. Mandatory, if **sso.login.saml2.idp.metadata-url** is not defined. You can define the SAML metadata descriptor resource with either this setting or the **sso.login.saml2.idp.metadata-url** setting.
sso.oauth.authentication.timeout.seconds	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 **octane.yml** file. They do not have any affect 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.
sso.oauth.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**

Setting	Description and usage
sso.oauth.client.secret	The OAuth client secret for the integration's client ID defined with **sso.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**
sso.saml.mapping.username	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.

Additional settings

Setting	Description and usage
sso.logging.console.enabled	Whether to log to the console. Log messages are issued to the ALM Octane **wrapper.log** file. Optional. Default: **false**
sso.logging.file.dir	The directory in which to create the SSO log files. Optional. Default: **<*log folder*>/sso**

Setting	Description and usage
sso.logging.file.enabled	Whether to log to the ALM Octane file in the directory defined by the **sso.logging.file.dir** attribute. Optional. Default: **true**
sso.logging.level	Logging level. Possible values are: - **SEVERE** - **INFO** - **WARNING** - **ALL** Optional. Default: **WARNING**
sso.login.saml2.subject.format	The format of the **NameIDPolicy** attribute in the SAML request. Default: **urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified**
sso.oauth.client.redirect-uri.host	The domain name used to redirect back to ALM Octane. Regular expressions are supported, for example, **.*mydomain.*** Optional. in the domain from the **AppURL** setting as defined in the **setup.xml** file, surrounded by wildcards. Example: **.*company-infra.net.*** **Caution**: The redirect URI is a critical part of the OAuth flow. After a user successfully authorizes an application, the authorization server redirects the user back to the application with the authorization code in the URL. Because the redirect URL contains sensitive information, it is critical that the service does not redirect the user to arbitrary locations.

Setting	Description and usage
sso.oauth.client.redirect-uri.schema	The schema (http or https) used to access ALM Octane. Optional. Default: The schema in the AppURL setting defined in the **setup.xml** file. **Caution**: The redirect URI is a critical part of the OAuth flow. After a user successfully authorizes an application, the authorization server redirects the user back to the application with the authorization code in the URL. Because the redirect URL contains sensitive information, it is critical that the service does not redirect the user to arbitrary locations.
sso.saml.mapping.firstName	The attribute in the SAML response's attribute statement that maps to the user's first name. Optional. Default: **firstName**
sso.saml.mapping.fullName	The attribute in the SAML response's attribute statement that maps to the user's full name. Optional. Default: **fullName**
sso.saml.mapping.lastName	The attribute in the SAML response's attribute statement that maps to the user's last name. Optional. Default: **lastName**
sso.saml.mapping.mail	The attribute in the SAML response's attribute statement that maps to the user's email address. Optional. Default: **mail**
sso.saml.mapping.uuid	The attribute in the SAML response's attribute statement that maps to the user's UUID. Optional. Default: **uuid**

Next steps:

- "Start the ALM Octane server" below

Start the ALM Octane server

Now that the initial setup is complete, you can run 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:

```
service octane start
```

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 the topic about trial licenses in the *ALM Octane Help Center*.

Next steps:

- "Log in to ALM Octane" on the next page
- **Cluster configuration**: If you successfully installed and logged into ALM Octane on the first cluster node, continue installing on additional cluster nodes. See:
  Linux: "Cluster installation (optional)" on page 55
  Windows: Cluster installation (optional)
- 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 84.

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 the topic about trial licenses in the *ALM Octane Help Center*.

1. In a browser, navigate 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 **setup.xml** file using settings **SiteAdministratorUser** and **SiteAdministratorPassword**.

> **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 116.

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 (optional)" on the next page.
- Set configuration parameters, such as FORGET_USER_ON_DELETE and SMTP_NOTIFICATION_SENDER_EMAIL. See the topic about configuration parameters in the *ALM Octane Help Center*.
- Create spaces. See the topic about creating spaces in the *ALM Octane Help Center*.
- Once you have logged on as the space admin, you can create other users and workspaces. See the topics on ways to add users and how to create workspaces in the *ALM Octane Help Center*.

Cluster installation (optional)

This section provides end-to-end instructions for installing an on-premises ALM Octane server in a cluster configuration on Linux.

In this topic:

- "Overview" below
- "Install ALM Octane in a cluster configuration" on the next page

Overview

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."

We install ALM Octane in a cluster configuration by:

1. Verifying all requirements and prerequisites for every node in the configuration.
2. After you configured the **setup.xml** and **octane.yml** configuration files in the first node, copy these file to all other cluster nodes.
3. Start ALM Octane on all servers.

See also "Installation flow" on page 15.

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 17.
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	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. If the repository is not located on a remote, dedicated machine, the repository location cannot be **/opt/octane**. 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. For example, you cannot have the path on the first server node defined as **/opt/octane/repo** and on additional nodes defined as **/server1/opt/octane/repo**.
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. For details, see "Prerequisites" on page 17.

2. **Install ALM Octane on the first cluster node**

   Install ALM Octane on the first cluster node, as described under "Installation" on page 27.

   a. "Deploy ALM Octane" on page 28

      Here we deploy the ALM Octane installation files onto the first node.

   b. "Configure initial site settings " on page 30

      We configure ALM Octane by modifying the **setup.xml** configuration file.

      Make sure to set the following settings to values that all cluster nodes can access.

DBServerName	The database server on which the site database schema resides. For cluster environments only.
RepositoryFolder	The shared repository that all cluster nodes can access (read and write).

c. "Configure other settings" on page 38

We configure other ALM Octane cluster settings by modifying the **octane.yml** configuration file.

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

cluster:	Section header. Do not edit.
	`cluster:`
	`    isCluster: true`
	`    nodes:`

isCluster Available with 12.60 CP8 and later.	Whether your server is standalone or in a cluster configuration. Mandatory. For a cluster configuration, set this value to **true**. You must enter node host names in the **nodes** setting. For a standalone server, set this value to false and do not enter any host names using the **nodes** setting. Default: **true**
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. **Examples**: ○ server1.domain.com,server2.domain.com,server3.domain.com ○ 120.150.12.12,120.150.80.13,120.150.32.14 Make sure **isCluster** is set to **true**.

d. "Start the ALM Octane server" on page 53

On the first node only, start the ALM Octane server by running **service octane start**.

3. **Set up a secure configuration on the first cluster node**

   If you want to set up a secure configuration for ALM Octane, follow the instructions in knowledge base article KM02707977.

4. **Make sure** ALM Octane **is running on the first node in the cluster**

   Before installing on remaining cluster nodes, log in to ALM Octane.

   For details, see "Log in to ALM Octane" on page 54.

5. **Only after you successfully log in, deploy ALM Octane installation files on each additional cluster node**

   Download and deploy the ALM Octane package on each cluster node. For details, see "Deploy ALM Octane" on page 28 and "Deploy in cluster environment" on page 29.

   > **Caution:** Do not do the following:
   >
   > - Do not configure the **setup.xml** and **octane.yml** files. You will be copying these files from the first node in the cluster during the next step.
   > - Do not run **connectnode.sh** scripts.

6. **Configure each additional cluster node**

   Copy the **/opt/octane/conf/setup.xml** and **/opt/octane/conf/octane.yml** files from the first cluster node to the **/opt/octane/conf** folder on the cluster node.

7. **Start** ALM Octane **on each additional cluster node**

   Run **service octane start** on each additional node.

8. **Set up a secure configuration on each additional cluster node**

   If you want to set up a secure configuration for ALM Octane in a cluster configuration, follow these instructions on each additional cluster node: Software Self-solve knowledge base article KM02707977.

9. **Log in to make sure** ALM Octane **is running on each additional node in the cluster**

   For details, see "Log in to ALM Octane" on page 54. Use the load balancer URL when you log in.

Upgrade

This section describes how to upgrade an existing installation of an on-premises ALM Octane server on Linux.

In this topic:

Before you upgrade

1. Verify that your server machine, and if relevant, all cluster nodes, meet all prerequisites.

   This includes checking the supported versions for all third party tools, such as Elasticsearch, and upgrading accordingly.

   For details, see "Prerequisites" on page 17.

   > **Note:** If the following are both true, add the CREATE SEQUENCE privilege to the site and shared space schemas:
   >
   > - You are upgrading from an ALM Octane version earlier than 12.55.3.
   > - You are upgrading an installation without a DB admin, for example, your original ALM Octane was installed using the FILL_EXISTING site action.

2. Elasticsearch prerequisites

   This upgrade makes significant changes to Elasticsearch indexes.

   ### Changes to Elasticsearch indexes

   - Updating the Elasticsearch indexes may take a while.

     During this time, users will not be able to use trend graphs, search, use **#** in comments, work in the Pipelines module , or use the Previous Runs tab for tests.

- After upgrading, each space will have multiple Elasticsearch indexes instead of one.

  Each index name will retain a similar prefix convention to prior versions:

  - Prior versions: **MQM-<logical-name>-index**
  - Current version: **mqm_<logical-name>_<index-type>_index**

  The event store index will be one of the indexes associated with the space. It's naming convention will now be: **mqm_sa_<logical-name>_event_store_index**
- If a rollback is needed, all new indexes associated with the space must be deleted.

Perform the following:

a. Based on the number of cluster nodes for ALM Octane, set the value for the ELASTIC_SPLIT_MAX_WORKERS_PER_NODE. For details, see this parameter in the list of configuration parameters.

b. Review Software Self-solve knowledge base article KM03347999 for up-to-date details about how to upgrade Elasticsearch indexes.

c. The Elasticsearch server by default allows scripting. If you have blocked this option, either enable scripting on the Elasticsearch server by adding **painless** to the **script.allowed_types** property in the **elasticsearch.yml** file, or remove this property altogether.

d. Make sure there is 60% disk availability on the Elasticsearch server. You can run the following command from kibana to check: `GET /_cat/allocation?v`

3. Create backups of:

   - The repository
   - Existing ALM Octane configuration files, including **setup.xml** and **octane.yml**
   - Your database
   - Elasticsearch
   - If you are using ALM Octane Synchronizer, back up :
     - ***/opt/octane/wrapper.conf***
     - **Service.locator.properties (/opt/octane/webapps)**

   For recommendations on making these backups, see "Best practices: Backing up ALM Octane data" on page 107.

4. Take note of any special aspects of your configuration, such as:

Special configuration	**Recommendation**
Did you use a different user, other than the **octane** user, to install?	If you did, the user is set in the **OCTANE_USER** environment variable. Use this user to upgrade.
Did you install ALM Octane to a location other than **/opt/octane**?	Refer to the location you used while upgrading.

Special configuration	Recommendation
What sudoer user did you use to install?	Use the same sudoer user that was used for installation to upgrade.
Did you modifiy the **/opt/octane/webapps/root/WEB-INF/classes/hpssoconfig.xml** file to control session timeouts?	If you modified the **/opt/octane/webapps/root/WEB-INF/classes/hpssoconfig.xml** file to control session timeouts, your updates will be overwritten by the upgrade. After upgrading, control session timeouts by setting the **MINUTES_UNTIL_GLOBAL_SESSION_TIMEOUT** and **MINUTES_UNTIL_IDLE_SESSION_TIMEOUT** configuration parameters instead. For details, see the topic about configuration parameters in the *ALM Octane Help Center*.
Do you want to switch from native user management to LDAP user management with this upgrade?	If you are upgrading from an ALM Octane version using native user management, and want to start using LDAP user management with this new ALM Octane version: a. Realize that once you configure for LDAP user management, you cannot return back to native, internal user management. b. When configuring initial settings in the **setup.xml** file, set the **DefaultSpaceMode** to **isolated**. For details, see "DefaultSpaceMode" on page 36. c. Upgrade ALM Octane without configuring for LDAP. This means, when modifying the **octane.yml** file, do not enter any values in the LDAP Settings section. d. After the upgrade is complete, configure for LDAP. e. Deactivate any native, internal users after LDAP configuration. These users can no longer log into ALM Octane (except for the **adminDN** user).
Did your organization's DBA made changes to database schemas, such as the addition of tables or columns?	Define an exception file. The exception file instructs ALM Octane to ignore manual changes to the database schemas during installation. For details, see "Using exception files for manual database changes" on page 92.

5. Stop the **octane** service on the server, and if relevant, all cluster nodes.

Deploy

Download and deploy the rpm package for the new version of ALM Octane using:

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

For details, see "Deploy ALM Octane" on page 28.

Configure initial settings

Here we describe how to modify settings in the **setup.xml** file.

1. Manually add newly-introduced settings to **setup.xml**

   With each version of ALM Octane, settings are added to support new features. To upgrade to the new version, add the newly-introduced settings as listed in the table below to the **setup.xml** file.

   Give these new settings values.

   Here is a list of introduced settings for **setup.xml**, by version:

Version	New Setting	Example
12.53.20	**AppURL**	`<entry key="AppURL">http://my_octane_server.my_domain.net:8080/</entry>`
Introduced in 12.55.4, but mandatory as of 12.55.17	**DefaultSpaceMode**	`<entry key="DefaultSpaceMode">shared</entry>`
12.60.4	A new section, **oracle_database**, was added. It contains the new **useDefaultSort** setting.	See Oracle settings below.

   a. If not already open, open **/opt/octane/conf/setup.xml** using an editor.

   b. Add any missing settings using this format:

      `<entry key="`*<setting>*`">`*<setting value>*`</entry>`

      Do not modify any text in the <entry> and </entry> tags themselves. Only modify text between these tags.

   c. Save the file.

For a full list of settings for the current ALM Octane installation and their syntax, see "Configure initial site settings " on page 30.

Configure other settings

Here we describe how to modify settings in the **octane.yml** file.

1. Learn the format for **yml** files

   <setting>`:` *<setting value>*

   Caution: Correct indentation and formatting is essential when editing **yml** files to avoid unpredictable results during installation.

There are resources available online that describe the exact rules and conventions for formatting **yml** files. We strongly recommend that you familiarize yourself with these rules before editing **octane.yml**.

Here are some important rules when editing settings in **octane.yml**:

- Put a single space after the colon between the parameter name and the value.
- Do not add bullets or any other extra formatting.
- Do not add extra spaces.
- Use double quotes to enclose any values that include special characters, especially the **#**.

  A **#** that is not enclosed in quotes marks the beginning of a comment. Any text after it, until the end of the line, is ignored. The **octane.yml** file is then interpreted incorrectly during installation and causes errors.

If these conventions are not followed, ALM Octane initialization or upgrade can fail.

For an example, see the sample **octaneExample.yml** file.

2. Determine settings to add to, and remove from, **octane.yml**

   With each version of ALM Octane, settings are added to support new features. To upgrade to the new version, add the newly-introduced settings as listed in the table below to the **octane.yml** file.

   Here is a list of introduced settings, by version:

Version	Added / Removed	Example
12.60.21	**isCluster**	`isCluster: true`
12.53.22	In the LDAP settings section, added all LDAP settings.	See LDAP below.

Version	Added / Removed	Example

12.55.4	In the LDAP settings section, added the following LDAP settings:
	dn
	uid
	baseDirectories
	baseFilters
		dn and uid example:
		`mapping:`
		`  dn: entryDN`
		`  uid: entryUUID`
		method example:
		`authentication:`
		`  method: anonymous`
		baseDirectories example:
		`baseDirectories:`
		`   - ou=Groups,o=organization.com`
		`   - dc=maxcrc,dc=com`
		baseFilters example
		`baseFilters:`
		`   - (objectClass=*)`
		`   - (&(objectClass=user)(objectCategory=person))`

	In the License settings section, added all licenses settings.	See licenses below.
	In the General server settings section removed the **serverDomain** setting.	
12.55.17	In the License settings section, added the **trialEdition** setting.	See licenses below.
12.60.16	For support for SSO in federated environments, added the service provider section. Also added a new authentication type setting for SSO.	See SP Settings below. `authenticationType: sso`

3. Modify settings
   a. Edit the **/opt/octane/conf/octane.yml** file using an editor.
   b. Remove the line with the **serverDomain** setting.
   c. Locate the section for each setting you need to add.
   d. Add any missing settings as listed above using this format:

   <setting>: *<setting value>*

   General server settings

cluster	**Cluster configuration**: Enter a comma-separated list of node host names or IPs in the cluster. **Example: 10.0.0.24,10.0.0.99,10.0.0.23** This is a mandatory setting. By default, the cluster is not configured, and the default value is blank. This indicates a standalone ALM Octane server.
heapSize	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. **heapSize** should be set 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**

server	The value of a Jetty port for HTTP, or a Jetty secure port for HTTPS.
	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.

proxy	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. An example of accessing an external server is when using a Trigger webhook rule. host: <*proxy_host*> port: <*proxy_port*> user: <*user*> password: <*password*>
authenticationType	Whether the ALM Octane installation should use native user management or LDAP authentication for user management. Values are: **sso**. Use SSO authentication. **ldap**. Use LDAP authentication. **internal**. Use internal, native ALM Octane user management. Default.

LDAP settings

Make sure your LDAP system has the corresponding attributes for each mandatory LDAP setting.

connectionTimeout	Connection timeout in seconds. Optional. Default: 30 seconds

adminDn	The user that will log on 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 will not start. Correct the user details and restart the server. This user can be same user as the user entered in the **setup.xml** 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 **setup.xml** 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 **adminDn** is changed and the server is restarted, both the original **adminDn** and the new **adminDn** exist as site admins. Modifying the **adminDn** does not remove the original one.

LDAP server settings

Make sure your LDAP system has the corresponding attributes for each mandatory LDAP setting.

Enter the following settings for each LDAP server separately.

Each LDAP server is defined by a group of settings. The settings for each LDAP server start with a hyphen (**-**) followed by the **host** setting.

> **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. Prefix each host item with a **-** sign: **- host**. This instructs ALM Octane where each host begins, especially if there are multiple LDAP servers.
port	LDAP server connection port. Mandatory.
isSsl	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 84.
description	Description of the LDAP server. Optional.

baseDirectories	Root of the LDAP path to use to search for users when including new LDAP users in ALM Octane spaces. This can be a semi-colon delimited list of common names and domain components (cns and dns), a list of organizational units (ou), and so on.
	Optional. Default: Blank.
	Make sure to put a space after hyphen (**-**) before specifying the filter.
	Example:
	`baseDirectories:`
	`    - ou=Groups,o=organization.com`
	`    - dc=maxcrc,dc=com`

baseFilters	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=*)
	Make sure to put a space after hyphen (**-**) before specifying the filter.
	Example:
	`baseFilters:`
	`    - (objectClass=*)`
	`    - (&(objectClass=user)(objectCategory=person))`

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, **user** and **password**. ○ **simple**. **user** and **password** are mandatory.
user	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

Make sure your LDAP system has the corresponding attributes for each mandatory LDAP setting.

Enter the following mapping settings for each LDAP server separately.

Values used in the mapping section are case-sensitive.

ALM Octane attribute in octane.yml	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**. **Example** i. If in LDAP, the **entryDN** attribute value is: **cn=<*common_name*>,ou=<*organizational_unit*>,dc=<*part_of_domain*>** ii. In the **octane.yml**, the dn value would be mapped to: **entryDN** iii. 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**
	entryDN **(for other LDAP systems)**	
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)**	
firstName	**givenName**	LDAP attribute for first name, such as **givenName**. Mandatory.

ALM Octane attribute in octane.yml	Sample LDAP attribute that can be used	Values and descriptions
lastName	**sn**	LDAP attribute for last name, such as **sn**. Mandatory.
fullName	**cn**	LDAP attribute for full name, such as **cn**. Optional.
logonName	**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 **logonName**. Mandatory. d. You can change the **logonName** attribute mapping at any time, but make sure the **logonName** 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.

License settings

trialEdition	Enter **team** or **enterprise**, depending on your trial edition. For details, see the information about ALM Octane editions in the *ALM Octane User Guide*. **Note:** This setting is used the first time the ALM Octane server starts, and cannot be changed retroactively.
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 **almSharing**. You then need to fill in the following fields as described below.
The following fields are mandatory for almSharing mode:	
url	Enter the full path that you use to access ALM. Typically, this includes the suffix **qcbin**.
almIntegrationUser	Enter the user name for accessing ALM. This user was defined in ALM for integration purposes.

almIntegrationPassword	Enter the password for the **almIntegrationUser**. This password is automatically encrypted after you restart the ALM Octane server.

Oracle settings

Section	Setting	Description and usage

oracle_ database:	**useDefaultSort**	**For Oracle databases**: 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)
		Usage:
		`oracle_database:`
		`  useDefaultSort: no`

ALM Octane service provider (SP) settings

The following service provider (SP) section and its settings are also available. Use these settings to set up SSO authentication for connecting to ALM Octane.

For these settings to take affect, make sure to set the authentication type to **sso** in this **octane.yml** file using the **authenticationType** setting.

For an example of setting these parameters, see the **octaneExample.yml** file.

Main settings

Setting	Description and usage
sso.key-pair.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**
sso.key-pair.pwd	Password for protecting and encrypting the key pair defined with **sso.key-pair.alias**. When ALM Octane starts, it encrypts this password. Mandatory. Example: **my-secret**

Setting	Description and usage
sso.keystore.file	The absolute path to the keystore file identified with **sso.key-pair.alias**. The default format for this file is **PKCS12**. You can change the format to Java KeyStore (JKS) by specifying this type when adding the **sso.oauth-keystore.type** setting to **octane.yml**. The path should be under ALM Octane's configuration folder to avoid permission issues. Mandatory.
sso.keystore.pwd	Password used to protect the keystore file defined with **sso.keystore.file**. When ALM Octane starts, it encrypts this password. Mandatory. Example: **my-password**
sso.login.saml2.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 **sso.login.saml2.idp.metadata** setting. Mandatory, if **sso.login.saml2.idp.metadata** is not defined. Example: **http://my-server.company-infra.net:8080/auth/realms/Dev/protocol/saml/descriptor**

Setting	Description and usage
sso.login.saml2.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. If metadata is provided using this setting, the URL defined in **sso.saml2.idp.metadata-url** is ignored. Mandatory, if **sso.login.saml2.idp.metadata-url** is not defined. You can define the SAML metadata descriptor resource with either this setting or the **sso.login.saml2.idp.metadata-url** setting.
sso.oauth.authentication.timeout.seconds	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 **octane.yml** file. They do not have any affect 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.
sso.oauth.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**

Setting	Description and usage
sso.oauth.client.secret	The OAuth client secret for the integration's client ID defined with **sso.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**
sso.saml.mapping.username	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.

Additional settings

Setting	Description and usage
sso.logging.console.enabled	Whether to log to the console. Log messages are issued to the ALM Octane **wrapper.log** file. Optional. Default: **false**
sso.logging.file.dir	The directory in which to create the SSO log files. Optional. Default: **<*log folder*>/sso**
sso.logging.file.enabled	Whether to log to the ALM Octane file in the directory defined by the **sso.logging.file.dir** attribute. Optional. Default: **true**

Setting	Description and usage
sso.logging.level	Logging level. Possible values are: ○ **SEVERE** ○ **INFO** ○ **WARNING** ○ **ALL** Optional. Default: **WARNING**
sso.login.saml2.subject.format	The format of the **NameIDPolicy** attribute in the SAML request. Default: **urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified**
sso.oauth.client.redirect-uri.host	The domain name used to redirect back to ALM Octane. Regular expressions are supported, for example, **.*mydomain.*** Optional. in the domain from the **AppURL** setting as defined in the **setup.xml** file, surrounded by wildcards. Example: **.*company-infra.net.*** **Caution**: The redirect URI is a critical part of the OAuth flow. After a user successfully authorizes an application, the authorization server redirects the user back to the application with the authorization code in the URL. Because the redirect URL contains sensitive information, it is critical that the service does not redirect the user to arbitrary locations.
sso.oauth.client.redirect-uri.schema	The schema (http or https) used to access ALM Octane. Optional. Default: The schema in the AppURL setting defined in the **setup.xml** file. **Caution**: The redirect URI is a critical part of the OAuth flow. After a user successfully authorizes an application, the authorization server redirects the user back to the application with the authorization code in the URL. Because the redirect URL contains sensitive information, it is critical that the service does not redirect the user to arbitrary locations.

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

e. Save the file.

Upgrade

1. Start the ALM Octane server.

```
service octane start
```

2. Check the **/opt/octane/log/wrapper.log** file. If you do not see the "Server is ready!" message, correct the errors shown in the log.

   Instructions for troubleshooting upgrade errors and warnings:

   - ""The wrapper.log has Java-related warnings (Linux)"" on page 118

Caution: Do not use ALM Octane until you have completed "Upgrade spaces in ALM Octane" on the next page.

Upgrade cluster nodes

Caution: Do not use ALM Octane until you have completed "Upgrade spaces in ALM Octane" below.

After the upgrade on the first node has completed successfully, you can then upgrade the remaining nodes in a cluster.

1. Copy **setup.xml** and **octane.yml** files to each node.
2. Start the ALM Octane server on each node.

```
service octane start
```

For details, see "Cluster installation (optional)" on page 55.

Upgrade spaces in ALM Octane

After upgrading, log into ALM Octane as the site admin to upgrade each space.

1. In a browser, navigate to **<*ServerURL*>:<*port*>/ui?site**.
2. Log in as the space admin, with the user name and password you provided in the **setup.xml** file.
3. Click **Site** and then click the **Spaces** tab.
4. Select the space and click **Upgrade**.

   Upgrade is available only if the space needs to be upgraded.

   Click **Refresh** to see the updated status for the space.

   Note: Upgraded spaces are, by default, isolated. To work with shared spaces, create new spaces.

5. Individual workspaces are upgraded in the background. In **Settings > Spaces**, click **Background Jobs** to track the progress of the workspace upgrades.

   Note: Until all of the background jobs have completed, some data may be unavailable in trend graphs.

For details on upgrading the space, see the topic about upgrading spaces in the *ALM Octane Help Center*.

Restart all Jetty servers

After upgrading the spaces in ALM Octane Settings, clear caches:

1. Stop all Jetty servers.
2. Make sure all post upgrade jobs and background jobs completed for all spaces.

   This includes jobs that run maintenance on Elasticsearch indexes. To check if these jobs have completed, In ALM Octane **Settings** ⚙ **> Site > POST UPGRADE JOBS**, and make sure that each space's "Split Elastic Index" job has the status **SUCCESS**.
3. Restart each Jetty server.

> **Note:** Make sure all Jetty servers are stopped at the same time before restarting even one of them.

After the upgrade

After the upgrade has completed successfully:

- The space status becomes **Active**.
- The space version is updated to the current version.

Bulk update data access control

> **Note:** This section is relevant only if you want to apply data access control for the first time to an upgraded system.

For data access control to work properly, both roles and entities must be assigned with data access control categories. After an upgrade, entities do not yet have a data access control category assigned to them. This means that roles that already have data access restrictions, will not be able to access these entities.

We recommend using the bulk update functionality to update entities efficiently.

Follow the instructions in the *Set up data access* topic in the *ALM Octane Help center*. When you reach the *Assign data access categories to items* section, use the **Bulk Update** option to assign data access categories to items, so that all the items are accessible only to the relevant roles.

Next steps:

- Update mandatory configuration parameters, such as SMTP_NOTIFICATION_SENDER_EMAIL. See The topic about configuration parameters in the *ALM Octane Help Center*.
- Download the newest IDE plugins for this ALM Octane version. See the topic about IDE integrations in the *ALM Octane Help Center*.
- If you work with the REST API, you might want to check if any API resources have been deprecated. While the deprecated resources are supported for a while, we recommend that you start updating your code so that you use the resource aliases instead. To see deprecated resources for a particular version, see the corresponding REST API example and how to use the interactive API client in the *ALM Octane Developer Help*

- Monitor the progress of post-upgrade background jobs. See the topic about upgrading spaces in the *ALM Octane Help Center*.
- "Rollback" below

Rollback

This section describes how to roll back after upgrading an on-premises ALM Octane server. This may be necessary if for some reason the upgrade fails or performance is slow.

Depending on when you want to roll back, there are different steps to perform.

In this topic:

- "After the upgrade's setup validation phase" below
- "After a site schema has been upgraded" below
- "After space schema has been upgraded" on the next page
- "After upgrade completed" on page 81
- "After upgrading cluster nodes" on page 81

After the upgrade's setup validation phase

You can roll back after the upgrade's setup validation phase, whether it passed or failed.

If the upgrade reached setup validation, the following have been modified:

- Previously-deployed files
- **setup.xml** and **octane.yml** configuration files

To roll back the deployed files, including setup.xml, and octane.yml files

1. Revert to the previous rpm file: `rpm -Uvh --oldpackage <`*filename*`>`
2. Revert to the backups of the **setup.xml** and **octane.yml** configuration files.
3. Re-initialize the ALM Octane server (the octane service). For details, see "Start the ALM Octane server manually" on page 83.

After a site schema has been upgraded

You can roll back after the upgrade's site schema have been upgraded.

If the upgrade upgraded the site schema, the following has been modified:

- The RPM file
- **setup.xml** and **octane.yml** configuration files
- The site schema

To roll back the site schema

1. Stop the ALM Octane server (the octane service).
2. Revert to a backup of the site schema.
3. Revert to the previous rpm file: `rpm -Uvh --oldpackage <`*filename*`>`
4. Revert to backups of **setup.xml** and **octane.yml** configuration files.
5. Re-initialize the ALM Octane server (the octane service). For details, see "Start the ALM Octane server manually" on page 83.

After space schema has been upgraded

If the upgrade upgraded the site schema, the following have been modified:

- The space schema
- Elasticsearch indexes
- ALM Octane repository files

Follow the steps for one of the following options.

Rollback option	**Steps**
To roll back changes to the space schema	1. Open the backup of the space schema. 2. Open the repository backup for this specific space. 3. Delete the additional Elasticsearch indexes and the event store index that were created after the upgrade. When rolling back, you need the original index only. 4. Fix what caused the upgrade to fail. 5. Reset the following for the space within the site schema: a. Open the **SHARED_SPACE** table. b. Find the record for the shared space. You can search for the **SP_NAME**. c. Set the **SP_STATUS** to **ACTIVE**. d. Set the **SP_VERSION** to the original version number before upgrading. 6. Upgrade again.
To roll back the entire upgrade	Follow the steps for "To roll back the site schema" above.

After upgrade completed

If the upgrade completed successfully, the following have been modified:

- The RPM file
- **setup.xml** and **octane.yml** configuration files
- The site schema
- The space schema
- Elasticsearch indexes
- ALM Octane repository files

To roll back the entire upgrade

1. Follow the steps for "To roll back the site schema" on the previous page.
2. Follow the steps for "To roll back changes to the space schema" on the previous page for each space.

After upgrading cluster nodes

If you upgraded additional cluster nodes, the following has been modified on the cluster nodes:

- Previously-deployed files
- **setup.xml** and **octane.yml** configuration files

To roll back to the **rpm** package

1. Revert to the previous **rpm** file on each cluster node: `rpm -Uvh --oldpackage` <*filename*>
2. Re-initialize the ALM Octane server (the octane service) on each cluster node. For details, see "Cluster installation (optional)" on page 55 and "Start the ALM Octane server manually" on page 83.

See also:

- "Management" on the next page

Management

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

This section includes:

Including these management tasks, you can also set configuration parameters to define how your site operates. Configuration parameters for the site are set using Settings. For details, see the topic about configuration parameters in the *ALM Octane Help Center*.

See also:

- Linux "Prerequisites" on page 17 or Windows Prerequisites
- Linux "Architecture" on page 7 or Windows Architecture
- Linux "Installation flow" on page 15 or Windows Installation flow

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:

```
service octane restart
```

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.

See also:

- "Management" on the previous page

Handle database-related issues

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

In this topic:

- "Change site schema settings and reinitialize" below

Change site schema settings and reinitialize

If you need to make changes to the site schema settings, make the changes in the **setup.xml** file.

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.

   ```
   services octane start
   ```

See also:

- "Management" on page 82

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 **service octane start**.

In this topic:

- "Configure trust" below

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. If the ALM Octane service (**octane**) is running, restart it.

Next steps:

- "Management" on page 82

Configure a secure connection to the ALM Octane server (Jetty)

This topic describes how to configure a secure connection to the ALM Octane server with Jetty.

We recommend that you always run ALM Octane in production with a secure connection.

> **Note:** ALM Octane uses the TLS version 1.2 secure protocol.

In this topic:

- "Configure the connection" below
- "Limitations" below

Configure the connection

Perform the following to configure a secure connection using TLS (SSL).

1. Obtain the server certificate issued to the name of this server in java keystore format (.jks) issued to the fully qualified domain name of ALM Octane server. It must contain a private key and the certificate authority that issued it. For details on creating certificates using the Certificate Authority, see Software Self-solve knowledge base article KM02707977.
2. Copy your keystore file to the **/opt/octane/conf/** directory. Name the file **keystore.jks**.
3. Run `/opt/octane/install/enablessl.sh`, supplying the certificate password as a parameter to the script.

Limitations

Note the following limitations:

- 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.

See also:

- "Management" on page 82

Advanced ALM Octane server configuration

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

This section includes:

- "Redirect http to https" below
- "Configure number of allowed open files (Linux)" on the next page
- "Configure secure database access" on page 88
- "Configure redirection when using SSL offloading" on page 90
- "Dedicate a cluster node for background jobs – 12.60 CP8 and later" on page 91

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:

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, or is protected only with Oracle Native Network encryption.

This section includes:

- "Before securing database access..." below
- "To configure a secure database connection for a previously-unsecured database " on page 90
- "To configure a secure database connection for a new ALM Octane installation" on page 90

Before securing database access...

Before configuring secure database access, determine the following:

- For SQL Server databases, determine if TLS 1.2 is required.
- For Oracle databases, determine if the database requires SSL/TLS or only Native Oracle protection.

Does the Oracle database require SSL/TLS?	**Instructions**
Yes	• Place the Oracle client wallet file in a location on the ALM Octane server into a directory accessible to all, such as **/tmp/ewallet.p12**. • Get the port number for secure access.
No	Get the following, for use later: • Determine if native Data Integrity is configured in **sqlnet.ora** on the Oracle server as **SQLNET.CRYPTO_CHECKSUM_SERVER**. • Determine if native Network Encryption is configured on the Oracle server. If yes, get the algorithm as defined in **sqlnet.ora** on the Oracle server as **SQLNET.ENCRYPTION_TYPES_SERVER**, and see if the key is larger than 128 bits.

- Prepare the connection string for the database

  This connection string will be used later.

  SQL Server

SQL Server Scenario	ConnectionString
SSL/TLS is required	Add the encryption method to the end of the **ConnectionString** value. **jdbc:mercury:sqlserver://<server>:<port>;EncryptionMethod=SSL**
TLSv1.2 is required	Add the encryption method and the TLS version to the end of the **ConnectionString** value. **jdbc:mercury:sqlserver://<server>:<port>;EncryptionMethod=SSL;CryptoProtocolVersion=TLSv1.2**

  Oracle

  Perform the following, based on your scenario.

Oracle scenarios	ConnectionString and other instructions
SSL/TLS required	Add the encryption method, the trust store, and the trust store password to the end of the **ConnectionString** value. **jdbc:mercury:oracle://<server>:<port>;servicename=<serviceName>;EncryptionMethod=SSL;TrustStore=<path to client wallet file> ;TrustStorePassword=<wallet password>**
Oracle Native Data Integrity	Add **;DataIntegrityLevel=accepted** or **;DataIntegrityLevel=required** to the end of the **ConnectionString** value.
Oracle Native Encryption	Add **;EncryptionLevel=accepted** or **;EncryptionLevel=required** to the end of the **ConnectionString** value. For encryption algorithms with keys longer than 128 bits, replace the Java security policy files in **\opt\octane\java\jre\lib\security\**. For details on Java security policy files, see http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html.

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 **setup.xml** file. The default location is **/opt/octane**):
   a. Set the value of **SiteAction** to **CONNECT_TO_EXISTING**:

      `SiteAction=`**CONNECT_TO_EXISTING**

   b. Edit the line with **ConnectionString**. For details, see "Prepare the connection string for the database" on the previous page.
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 84.
3. Run the service to start the ALM Octane server.

```
service octane start
```

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

1. After installing ALM Octane, start the server:

```
service octane start
```

2. In the Database Server step, select the **ConnectionString** option and set the values for your database. For details, see "Prepare the connection string for the database" on the previous page.
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 84.

Configure redirection when using SSL offloading

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

For details, see knowledge base article KM03286744.

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 (optional)" on page 55.
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 the overview for developers in the Developer Help in the *ALM Octane Help Center*.
5. Start the ALM Octane server.

See also:

- "Management" on page 82

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.

In this topic:

- "Overview" below
- "Define exception files" below
- "Set up use of the exception file" on page 94

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.

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 **setup.xml** file.

1. During installation, when configuring the **/opt/conf/setup.xml** 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 **C:\octane\conf\setup.xml** 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 the topic about creating spaces for a site in the *ALM Octane Help Center*.
3. Check that you have proper access to the space.

See also:

- "Configure initial site settings " on page 30
- Troubleshooting: ""My FILL_EXISTING installation failed, indicating that I have extra tables, view, indexes, and so on."" on page 119

Set up SSO authentication (on-premises)

This topic describes how to set up SSO authentication for connecting to ALM Octane.

In this topic:

- "Overview" below
- "Prerequisites" on page 98
- "Configure ALM Octane and its SP" on page 98
- "Establish SAML trust between the ALM Octane's SP and the IdP" on page 99
- "Map IdP attributes" on page 100
- "Test SSO authentication" on page 104
- "Import users " on page 104

Overview

This topic describes how SSO access to ALM Octane can be authorized in a federated environment. This way, users can use single sign-on for logging into ALM Octane as they do with other SSO applications at the site.

To facilitate single sign-on, the ALM Octane service provider (SP) sends an authentication request to the IdP, which is an online service that authenticates users using security tokens.

It is essential that the ALM Octane service provider (SP) can identify users uniquely when communicating with the Identity Provider (IdP). This is a two-step process.

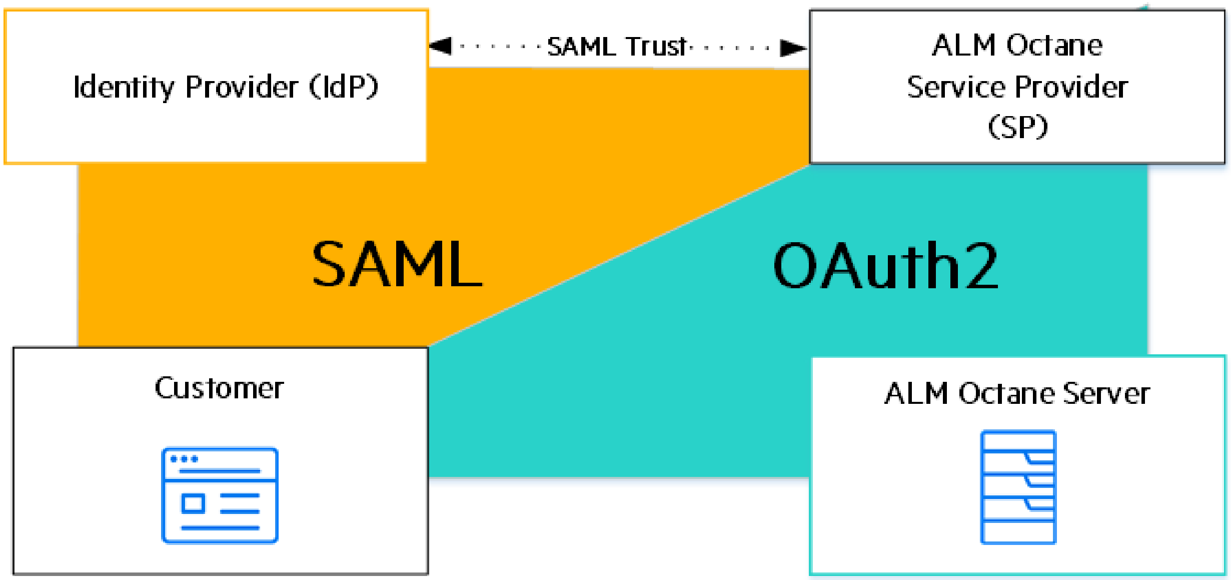
1. **Authorization**. When a user logs in, ALM Octane attempts to locate a matching user in the IdP. For details, see "About authorizing users" below.
2. **Identification**. After a user is authorized to log in, ALM Octane identifies which user it is. For details, see "About identifying users" on the next page.

Service providers and protocols

ALM Octane has its own built-in service provider (SP) for this purpose.

ALM Octane's SSO integration uses the SAML2 protocol for authentication with identity providers (IdPs).

ALM Octane uses the OAuth2 protocol for creating access tokens and validating them.



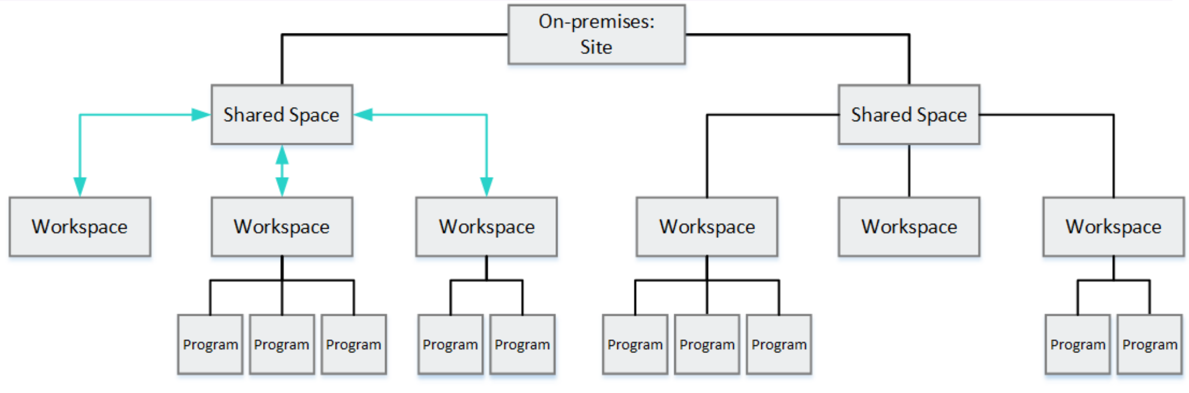
About authorizing users

When a user logs in, ALM Octane attempts to locate a matching user in the IdP.

Scenario	Description and result
A matching user exists	ALM Octane checks by uuid, and then by name. If either of these is located successfully, the user is authorized. If the details of the user do not match, the details are updated in ALM Octane and the user is authorized.

Scenario	Description and result
No matching user exists	The user is not authorized and cannot log in. Users can be imported from the IdP into ALM Octane using a CSV file. After the import, the user can log in. For details on importing, see Import IdP users for SSO authentication into a workspace (on-premises).

Example: Assume the following users are defined in the IdP and the ALM Octane SP:



- A user named Carlos with uuid 100 attempts to log in.

  Carlos is authorized.
- A user named Svetlana with uuid 300 attempts to log in.

  The user is authorized. The name in ALM Octane is updated to Lee.
- A user named Sally with uuid 400 attempts to log in.

  Sally is authorized. The uuid in ALM Octane is updated to 200.
- A user named George with uuid 900 attempts to log in.

  Authorization fails.

For details, see "Set up SSO authentication (on-premises)" on page 95.

About identifying users

For identification, the ALM Octane SP uses the **sso.saml.mapping.username** setting in the **octane.yml** file to determine how to map the ALM Octane **username** attributes to the corresponding IdP attribute after receiving the SAML response from the IdP. The mapping is based on the following:

Setting in octane.yml	SAML Response	Description
'{$id}'	**<saml2:NameID>** attribute, in the **<saml2:Subject>**	ALM Octane identifies users by mapping the ALM Octane **username** to the **NameID** in the SAML subject. This is the default.
userName	The FriendlyName **username** in the **<saml2:Attribute>** in the **<saml2:AttributeStatement>**	ALM Octane identifies users by mapping the ALM Octane **username** to the **username** attribute in the SAML attribute statement.

For details, see "Map IdP attributes" on page 100.

> **Tip:** Other **octane.yml** settings that you can define for mapping purposes include: **sso.saml.mapping.uuid, sso.saml.mapping.lastName**, **sso.saml.mapping.firstName**, **sso.saml.mapping.fullName**, and **sso.saml.mapping.mail**. For details, see the information about configuring additional ALM Octane SP settings in the installation help for Windows or Linux.

Handling existing internal users

Existing internal users defined in ALM Octane from before switching to SSO authentication already have passwords. These passwords are not overridden when the user is mapped to IdP users. However, the users cannot use these original ALM Octane passwords to log into ALM Octane once configured for SSO, even when directly navigating to the ALM Octane login page. They are defined, but the SSO passwords are the only ones in use.

For details, see "Import users " on page 104.

Prerequisites

If you are using SSL with a self-signed or internal certificate, add the certificate to the CA store of the JVM runtime used to run ALM Octane for authentication to succeed.

Configure ALM Octane and its SP

Configure ALM Octane and its service provider (SP) for SSO integration.

Verify that the initial admin is available in the IdP

The first user created in ALM Octane has superuser permissions and is allowed to perform any action in the system. In effect, the initial user is a site admin, a space admin, and a workspace admin for all default spaces.

This user is defined using the **SiteAdministratorUser** setting in the **setup.xml** file.

Make sure that this admin already exists in the IdP.

Later, you can import additional IdP users. For details, see "Import users " on page 104.

Enable the ALM Octane SP

Modify the **octane.yml** file to configure the ALM Octane SP.

For these settings to take affect, make sure to set the authentication type to **sso** in this **octane.yml** file using the **authenticationType** setting.

Not all settings are required. Make sure to comment out unnecessary settings using the hash (**#**) at the beginning of a line.

These available settings include:

Keystore settings	Include settings that provide the SP with the certificates needed to sign and encrypt authentication messages.
OAuth settings	For configuring internal OAuth authentication details.
Logging settings	For changing the SP's logging level.
SAML metadata settings	For establishing trust.
Redirect URI settings	Which contain the allowed addresses for redirection. This is used to validate that an authenticated user is not redirected to an incorrect place.

For details on the settings to add to the **octane.yml** file, see the *ALM Octane Installation Help*: Linux Windows

Restart ALM Octane.

Establish SAML trust between the ALM Octane's SP and the IdP

Establishing trust between the ALM Octane service provider (SP) and the IdP requires sharing metadata between the providers.

- Share the IdP's metadata with ALM Octane

  While enabling the SP, the IdP’s metadata was already shared.

  The metadata can be supplied with a URL or by a file. For details, see Linux settings or Windows settings.

Tip: During the authentication process, the ALM Octane SP sends a SAML request that contains the **NameIDPolicy**. The **NameIDPolicy** specifies constraints on the name identifier that represents the requested subject. By default, the requested **NameIDPolicy** is **urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified**. This value can be changed by setting the **sso.login.saml2.subject.format** setting in the **octane.yml** file. For details, see the description of the **sso.login.saml2.subject.format** setting in the **octane.yml** file under Linux settings or Windows settings.

- Share ALM Octane's metadata with the IdP

  To obtain ALM Octane's metadata, navigate to:

  <protocol>://<host>:<port>/osp/a/au/auth/saml2/sp-metadata

  The metadata is available only after the ALM Octane server starts. For details, see "Enable the ALM Octane SP" on the previous page.

  Any additional IdP configuration is not covered here. See the documentation for the IdP. Generally, however, depending on your individual IdP, you either provide this URL in the IdP's configuration screens, or save the XML and import it into the IdP. This configures the ALM Octane SP as a client for your IdP.

Map IdP attributes

Map the user attributes that are returned by the IdP in a SAML assertion to the equivalent ALM Octane attributes.

The attributes are case-sensitive.

The SAML response must be signed. Encryption is optional.

Note: ALM Octane overrides the built-in attributes with the ones supplied by the IdP, keeping them up-to-date with your IdP definitions.

ALM Octane Attribute	IdP Friendly Name	Description
User name	username	If set to **'{$id}'**, the ALM Octane **username** is mapped to the **NameID** in the SAML subject. If set to **username**, the ALM Octane **username** is mapped to the **NameID** in the SAML AttributeStatement section. The value may be changed to the name of any other attribute sent in the SAML response.

ALM Octane Attribute	IdP Friendly Name	Description
UUID	uuid	The uuid of the user. If the IdP sends updated information in the SAML assertion, the updates override existing information in ALM Octane. If the Friendly Name for this attribute is different in the IdP, you can specify the correct Friendly Name using the optional **sso.saml.mapping.uuid** setting in the **octane.yml** file.
Email	mail	The email of the user. If the IdP sends updated information in the SAML assertion, the updates override existing information in ALM Octane. If the Friendly Name for this attribute is different in the IdP, you can specify the correct Friendly Name using the optional **sso.saml.mapping.mail** setting in the **octane.yml** file.
Full name	fullName	The full name of the user if it is different from the **firstName** and the **lastName** together. If the IdP sends updated information in the SAML assertion, the updates override existing information in ALM Octane. If the Friendly Name for this attribute is different in the IdP, you can specify the correct Friendly Name using the optional **sso.saml.mapping.fullName** setting in the **octane.yml** file.
Last name	lastName	The last name of the user. If the IdP sends updated information in the SAML assertion, the updates override existing information in ALM Octane. If the Friendly Name for this attribute is different in the IdP, you can specify the correct Friendly Name using the optional **sso.saml.mapping.lastName** setting in the **octane.yml** file.
First name	firstName	The first name of the user. If the IdP sends updated information in the SAML assertion, the updates override existing information in ALM Octane. If the Friendly Name for this attribute is different in the IdP, you can specify the correct Friendly Name using the optional **sso.saml.mapping.firstName** setting in the **octane.yml** file.

> **Tip:** Mapping by **uuid** is not required, but recommended.
>
> To facilitate automatic synchronization of user details from the IdP to ALM Octane, the uuid (the user identifier, similar to the user name) should be unique and stable. This means the attribute should not be something that is likely to change, such as email.
>
> (Using the **uuid** as the user identifier allows you to change the user name, if necessary.)
>
> If the **uuid** is not provided for mapping, ALM Octane tries to synchronize user details based on the mapped **userName** or the subject in the SAML response. However, if this value is later changed on the IdP side, ALM Octane will not be able to identify the user.
>
> For details, see "Set up SSO authentication (on-premises)" on page 95.

Example

Here is a sample SAML response.

```
</saml2p:Response>

        </saml2:Assertion>

...

...

...

                <saml2:Subject>
                       <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
NameQualifier="https://idp.hpsso.com/idp/shibboleth" SPNameQualifier="http://myd-
vm04876.hpeswlab.net:8081/osp/a/au/auth/saml2/metadata">ostap</saml2:NameID>
                       <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                               <saml2:SubjectConfirmationData Address="10.14.82.165"
InResponseTo="idQYsxpd8LajekIxpc2SIlsCLwJpo" NotOnOrAfter="2018-05-06T13:17:45.303Z"
Recipient="http://myd-vm04876.hpeswlab.net:8081/osp/a/au/auth/saml2/spassertion_
consumer"/>
                       </saml2:SubjectConfirmation>
               </saml2:Subject>
               <saml2:Conditions NotBefore="2018-05-06T13:12:45.291Z" NotOnOrAfter="2018-05-
06T13:17:45.291Z">
                       <saml2:AudienceRestriction>
                               <saml2:Audience>http://myd-
vm04876.hpeswlab.net:8081/osp/a/au/auth/saml2/metadata</saml2:Audience>
                       </saml2:AudienceRestriction>
               </saml2:Conditions>
               <saml2:AuthnStatement AuthnInstant="2018-05-06T13:12:45.210Z" SessionIndex="_
279a5220e4450d141a5ae8838c05c650">
                       <saml2:SubjectLocality Address="99.99.99.999"/>
                       <saml2:AuthnContext>

<saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedT
ransport</saml2:AuthnContextClassRef>
                       </saml2:AuthnContext>
               </saml2:AuthnStatement>
               <saml2:AttributeStatement>
                       <saml2:Attribute FriendlyName="phoneNumber"
Name="urn:oid:0.9.2342.19200300.100.1.1"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                               <saml2:AttributeValue>+972(54)911 1011</saml2:AttributeValue>
                       </saml2:Attribute>
                       <saml2:Attribute FriendlyName="fullName" Name="urn:oid:2.16.840.1.113730.3.1.24
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                               <saml2:AttributeValue>Ostap Suleyman Berta Maria Bender
Bey</saml2:AttributeValue>
                       </saml2:Attribute>
                       <saml2:Attribute FriendlyName="firstName" Name="urn:oid:2.5.4.42"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                               <saml2:AttributeValue>Ostap</saml2:AttributeValue>
                       </saml2:Attribute>
                       <saml2:Attribute FriendlyName="lastName" Name="urn:oid:2.5.4.4"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                               <saml2:AttributeValue>Bender</saml2:AttributeValue>
                       </saml2:Attribute>
                       <saml2:Attribute FriendlyName="uuid" Name="uuid"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">

<saml2:AttributeValue>MWY3ZTg2YWEtODIzZC00NDgyLTgyMTYtOGZjODAzYzVhMTRh</saml2:Attribu
teValue>
                       </saml2:Attribute>
                       <saml2:Attribute FriendlyName="mail" Name="urn:oid:0.9.2342.19200300.100.1.3"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                               <saml2:AttributeValue>obender@hpe.com</saml2:AttributeValue>
                       </saml2:Attribute>
                       <saml2:Attribute FriendlyName="username" Name="username"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                               <saml2:AttributeValue>obender@hpe.com</saml2:AttributeValue>
                       </saml2:Attribute>
               </saml2:AttributeStatement>

       </saml2:Assertion>

</saml2p:Response>
```

Test SSO authentication

Test authentication for the ALM Octane UI and APIs:

To log in to ALM Octane using SSO, navigate to ALM Octane's URL. You should be redirected to your IdP's login screen.

Log in with the ALM Octane admin credentials.

You are redirected to ALM Octane and you can now use the application.

For information on non-browser-based authentication for the REST API, see "Set up SSO authentication (on-premises)" on page 95

Import users

Import users and assign their permissions in the ALM Octane Settings area.

For details on importing users, see Import IdP users for SSO authentication into a workspace (on-premises).

Once imported into ALM Octane, these users can log in with SSO.

See also:

- Linux: "Configure other settings" on page 38
- Windows: Configure other settings
- Import IdP users for SSO authentication into a workspace (on-premises)

Best practices

Here are some best practices you may want to consider adopting during or after installation.

This section includes:

See also:

- Installation flow for Linux or Windows in the *ALM Octane Installation Guide*
- Information about managing spaces in the *ALM Octane Help Center*
- Information about managing workspaces in the *ALM Octane Help Center*

Best practices: Deploying ALM Octane

This topic describe the main components of the ALM Octane architecture and provides best practices and recommendations for enterprise deployment of ALM Octane on-premises.

In this topic:

- "Overview " below
- "Architecture" below
- "General guidelines" below
- "Minimal and suggested requirements" on the next page

Overview

ALM Octane is available:

- As a service offered by Micro Focus SaaS.
- As an on-premises installation as a compressed package (**rpm** or **zip**).

Architecture

ALM Octane includes the following main components:

- Database
- Elasticsearch
- ALM Octane server

Each component should reside on separate, dedicated machine. Each component can be scaled using clustering to provide better performance, load balancing, and fault tolerance.

For details on the ALM Octane architecture, see the architecture diagrams in the *ALM Octane Installation Guide* or the *ALM Octane Help Center*.

General guidelines

While planning the enterprise deployment, consider the following:

- The capacity for production environments is hard to assess due to unknown patterns of behavior. Will testing be manual or automatic? Will there be a large backlog witha vonsiderable or minimal number of tasks? How many workspaces are needed? And so on.

- Our recommendations are based on Micro Focus generic assumptions. Reassess the environment after 1-2 years of full production usage.
- The specifications provided here do not relate to the installation and configuration of 3rd party software. See vendor documentation to prepare clustered installations of the database and Elasticsearch.
- While each component can be clustered, clustering does not necessarily improve performance linearly. This is because performance depends on the types of operations your users perform. However, it is important to design the environment in such a way that you can add more cluster nodes later.

Minimal and suggested requirements

For the most up-to-date list of requirements, see the system requirements provided in the *ALM Octane Help Center*.

See also:

- "Best practices" on page 105

Best practices: Backing up ALM Octane data

This topic provides best practices and recommendations for backing up ALM Octane and all its components.

In this topic:

- "Overview " below
- "The process" on the next page
- "Best practices" on page 109

Overview

ALM Octane stores its information in the following components:

- **Your relational database (either Oracle or SQL Server)**. This is where the most important system data are located. The relational database is the most important component of the backup.

  Database systems support hot backup procedures and provide the ability to restore operations to the last second before the system crash.
- **Elasticsearch**. Elasticsearch stores trend data, audit information, run history, search information, and additional miscellaneous items.

  You can take periodic snapshots of Elasticsearch data.

- **The repository folder on your file system**. ALM Octane includes its own file system repository where attachments, manual scripts and other artifacts are kept. The default location for this folder is:
  - Linux: **/opt/octane/repo**
  - Windows: **C:\octane\repo**

  You can take periodic snapshots of repository data.

The process

To fully back up ALM Octane, back up all its components: the relational database, Elasticsearch, and the repository folder. Store each backup in a separate location to allow for (disaster) recovery.

Order matters

- Time may elapse as you back up each of these components. In terms of time difference tolerance, the time as specified in the relational database is used as the determining factor. When you restore ALM Octane, it is the data and timestamps stored in the relational database that users see. Keep this in mind when restoring.
- If you backed up your relational database, added files, and only then backed up the repository, the files exist after restore, but ALM Octane does not see any associations to them, and eventually deletes them.

  Conversely, if you backed up the repository, added files, and only then backed up the relational database, ALM Octane might report that you have some broken associations, as the files do not exist in the repository while ALM Octane tries to find them.

Frequency of backups

While database systems, such as Oracle and SQL Server, support hot backup procedures and provide the ability to restore operations to the last second before the system crash, it is only possible to take a periodic snapshot of the Elasticsearch and ALM Octane repository.

Therefore, how often you should back up is determined by the amount of down time your site can tolerate. If the amount of tolerated time is one day (meaning, the company is fine with the ability to restore the operation to the state of 24 hours ago), the suggested backup frequency could be defined as one day. If the amount of tolerated time is 12 hours, backups should run every 12 hours.

> **Example:** ALM Octane operations on SaaS are backed up every 4 hours. In most cases, hot backups and dumps/snapshots should then be either moved to a separate location or put on removable media for storage.

Backing up the relational database

Use the database's backup mechanism and save the resulting files and folders.

Open files do not pose a problem during the backup, as most files are not locked by ALM Octane.

Best practices

The relational database is the most important component in the backup.

General

- Back up each component as closely as possible, one after the other.
- Back up ALM Octane during quiet times to minimize missing files, broken file associations, and time inconsistencies between the three components.

Recommended order for backing up components

Here are suggested guidelines and the sequence of backup actions to take.

1. Always back up the database first. Use the database vendor's, or commercially-available, tools to perform a hot backup (such as Oracle RMAN). We recommend that you take a snapshot (dump) before performing any major operations on the database, such as an upgrade, data migration (such as from Agile Manager to ALM Octane), massive import, and so on.
2. Back up Elasticsearch next. Elasticsearch is a NoSQL database geared toward fast textual indexing and search. You can take a snapshot of the Elasticsearch indexes periodically using REST API commands from any programming language (for example, JavaScript). Kibana is one tool recommended by Elasticsearch for issuing REST API commands.

   See https://www.elastic.co/guide/en/elasticsearch/reference/current/modules-snapshots.html on the Elasticsearch site.

   To back up properly in a clustered Elasticsearch environment, attach shared storage to which snapshots from each node can be saved.
3. Lastly, back up the ALM Octane repository. Make a complete backup using operating system capabilities (**tar**, **zip**) or commercially-available tools.

See also:

- "Best practices" on page 105
- "Disaster recovery" on the next page

Best practices: Maintenance

To maintain uninterrupted operations, we recommend you follow the following best practices for the ALM Octane production environment.

In this topic:

- "Overview" on the next page
- "Periodic maintenance" on the next page
- "Disaster recovery" on the next page

Overview

These best practices help maintain the following main components that are necessary for proper functioning of ALM Octane:

- The ALM Octane application server
- The Elasticsearch server
- The database server

Periodic maintenance

Periodic maintenance includes upgrading to new versions of the product, including patches. This involves:

- Downloading the appropriate version build from Micro Focus Software Self-service Online.
- Deploying the package.
- Performing database upgrade steps.

Before upgrading to a new build or patch, make sure to:

1. Back up the database.
2. Back up (meaning, take a snapshot of) the Elasticsearch index.
3. Back up the ALM Octane repository file system.
4. Back up the ALM Octane configuration files (which are located at **/opt/octane/conf** by default).

For details on backing up, see "Best practices: Backing up ALM Octane data" on page 107.

For details on upgrading, see the upgrade procedure in the *ALM OctaneInstallation Guide*.

Disaster recovery

ALM Octane can be deployed in a cluster to allow for uninterrupted operation. In fact, each component can be scaled out:

- Database and Elasticsearch, according to vendor instructions.
- ALM Octane cluster guidelines can be found in the *ALM Octane Installation Guide*.

Having backup procedures in place allows for data integrity and completeness.

In addition, ALM Octane does not lose data at a time of crash, because data is kept in database. All asynchronous jobs are persistent.

See also:

- "Best practices" on page 105
- "Best practices: Backing up ALM Octane data" on page 107

Best practices: Setting up spaces and workspaces

This topic provides best practices and recommendations for setting up spaces and workspaces in ALM Octane.

In this topic:

- "Overview " below
- "Planning how to set up spaces" on the next page
- "Planning how to set up spaces" on the next page

Overview

This overview provides basic information about the various types of spaces in ALM Octane and how to work with them.

Terms

Site	Top level container. Allows the management of the different spaces created in ALM Octane as well as a place to carry administrative tasks and manage users.
Space	Top level logical container. Provides absolute isolation of data. A space is the highest container level that allows data sharing and interaction. A space allocates its own resources when created, such as relational database schema, Elasticsearch indexes, and the repository location.
Workspace	A working container. A user always works in the context of a specific workspace. A workspace is always contained in a shared space and provides logical isolation of data and settings. The level of isolation is defined by the type of shared space created.

For details about the site and spaces, see the information about spaces in the *ALM Octane Help Center*.

Types of spaces

ALM Octane Enterprise edition provides the following types of spaces: Shared and Isolated.

Shared space (Enterprise edition)	Workspaces share customization and can share data. Cross workspace reporting is possible. Some entities may be defined as global and be viewed across all workspaces.

Isolated space (Pro and Enterprise editions)	Each workspace defines its own customization. No sharing between workspaces. A user can be assigned to multiple workspaces and seamlessly switch between them. **Note:** Pro edition only allows creation of isolated spaces. Shared spaces are an enterprise level feature.

Planning how to set up spaces

This topic provides strategies for planning spaces (both isolated and shared) in your ALM Octane deployment.

Space strategy overview

When planning your ALM Octane deployment, it is important to plan how to break down your projects into a structure that provides you with the best experience for your teams.

Generally, unless there is an actual need for complete isolation of workspaces, use shared spaces (instead of isolated spaces). The use of shared spaces allows you to better scale out ALM Octane as your projects grow.

Consider the following factors.

Amount of interaction and data-sharing between projects

If you have projects that have close interaction and work together frequently, consider putting them either in the same workspace or in different workspaces under the same shared space.

This best practice is relevant in both this use case, sharing data, and also the use case for having similar processes and shared customization. For more suggestions about working with similar process and shared customization, see "Projects that have shared processes and policy" on the next page.

When trying to evaluate and understand interaction level between the projects, and the need to share data, relate to factors such as team collaboration level, dependencies among teams, common releases, integration among the applications, and so on.

The level of interaction between teams is the most major factor for deciding whether teams and products should be in the same workspace. For details, see "Planning how to set up spaces" above.

If you define teams and products in separate workspaces, knowing that the teams and products need some level of interaction that require dependencies between entities and sharing of data, these workspaces should reside within the same shared space. Workspaces that reside within the same shared space are able to more easily share entities and set dependencies between entities in the following ways:

- Define shared entities at the shared space level.
- Move entities from one workspace to another.
- Define dependencies between entities on different workspaces within the same shared space.

Projects that have shared processes and policy

If you are an enterprise customer, you can enforce your process and align organizational standards to all workspaces within a shared space by customizing at the shared space level. This customization is achieved using business rules, common fields, workflow, lists, and so on.

ALM Octane also provides customization on the workspace level, so the teams and products don’t have to be fully aligned. However, defining the main processes and standards at the shared space level is advantageous because not only does it apply to all workspaces, you can also add additional processes, definitions, and standards for specific projects in specific workspaces. This provides flexibility.

If you have sets of workspaces that do not need any interaction, the recommendation is to separate the sets of workspaces into different shared spaces, and manage the common customizations on the different shared spaces accordingly.

> **Note:** Managing common customization for large number of workspaces might result in a very complicated customization at the shared space level that is hard to manage and eventually can also cause performance degradation. If the shared space admin does want to have a significant portion of the customization shared, the more workspaces there are with greater variance, the more work the shared space admin needs to do to manage the variance.

Make sure that the customization at the shared space level is relevant and needed for all workspaces. Additional flexibility can be done at the customization of each workspace, but if there is a need for common customization for partial set of workspaces within the same shared space, then probably these workspaces should be in a different shared space.

> **Note:** Same applies also to management of shared assets. If there are too many variations between the workspaces and the need for different shared entities, it results in a large number of shared assets which are hard to manage.

Cross-workspace reporting

If there is a need to track projects managed in different workspaces, having these workspaces on the same shared space enables cross-workspace reporting, which reflects the data from different workspaces in the ALM Octane dashboard. For example, if two projects share the same release and you want to understand the progress of each project in the release, put each project in its own workspace, and make sure both workspaces are under the same shared space,

Cross-workspace reporting is also possible even if the workspaces are under different shared spaces. You can do this by using OData, which extract workspaces data to external BI tools. For details, see the information about OData support for extended reporting in the *ALM Octane Help center*.

Data isolation

If a project requires absolute data isolation, define the project in a workspace in its own isolated space. This ensures that there is no way to inadvertently expose confidential information between projects.

Disaster recovery planning (DRP)

Each space is stored in a different database schema (Oracle) or database (SQL Server).

> **Note:** For the purposes of this discussion, we will use the Oracle terminology.

Workspaces within the same space share the same database schema as the space. This means that backup and recovery can be done over an entire space, and it includes all its workspaces.

Recovery therefore recovers all workspaces in a space. You cannot recover just one workspace in a space.

Planning how to set up workspaces

This topic provides strategies for planning workspaces in your ALM Octane deployment.

Workpace strategy overview

Similar to the strategy for setting up spaces, consider how to partition projects within a space. The factors to consider are similar to the space strategy parameters, but on a smaller scale.

If the projects are tightly intertwined, and a large portion of the data needs to be used by different teams in these projects, the projects should reside within the same workspace to allow ease of sharing of data.

You can make sure that each project member only sees the information that is relevant in the following ways:

- Use basic filtering to partition data within a workspace. For example, you can filter by program.
- Assign and customize roles.
- Customize module access.
- Set up data access.

Consider the following factors.

Sharing of data between teams

The main factor for deciding whether teams and projects should be in the same workspace or separate workspaces is the level of shared data that is common for the teams. If teams share the same release planning and content, or have strong dependencies on different entities, these teams and projects should probably share the same workspace.

Data isolation

Different workspaces provide data isolation. If there is a need to isolate data between the different teams and projects, this probably indicates that these teams and projects should be managed in different workspaces.

ALM Octane provides data access capabilities, but these should be used for specific cases when some entities need to be hidden for certain users and teams, and not in the case of most data needing to be hidden. If most data needs to be hidden between teams, use different workspaces.

Different processes

All workspaces within the same shared space inherit the common customization from the shared space level.

You can customize each workspace even further, on top of the shared customization for the space. This enables you to define additional processes relevant for the workspace level only. If there is a need for different customization at the workspace level for compliance with different processes, and there is no need to share data, we recommend that you define these projects and teams in different workspaces.

Performance considerations

Try to break down your spaces into as many workspaces as possible as this helps ALM Octane perform better and makes searching for data, and concentrating on your tasks, easier. The best practice is to have many small workspaces in the same space instead of a few, very big workspaces.

See also:

- "Best practices" on page 105

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 Micro Focus Software Self-solve 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:

```
service octane restart
```

The service runs in the background.

"ALM Octane does not open in Internet Explorer."

If you encounter problems opening ALM Octane in Internet Explorer, check that the domain is configured correctly:

1. Edit the **octane.yml** and provide the correct the domain.
2. Restart the ALM Octane server.

"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`
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.

"Session timeout a few minutes after login."

If session timeout occurs within a few minutes after login, check that the required domains are configured in the list of authorized domains in the **hpssoconfig.xml** file. For details, see Configure access to from multiple domains.

"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 **services octane start** 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 83.

"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 92.

If you still have problems:

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

"Either ALM Octane cannot fetch Jetty files or Internet Explorer 11 does not connect to SSL"

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 Micro Focus Software Self-solve knowledge base article KM03310408.

See also:

- "Management" on page 82

Checking logs

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

In this topic:

- "Log files" below
- "Checking logs" above

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 82

Uninstall

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 27

Send Us Feedback

Let us know how we can improve your experience with the Installation Guide for Linux.
Send your email to: docteam@microfocus.com

MICRO® FOCUS

Java™ COMPATIBLE