# Java Platform, Standard Edition

## Advanced Management Console Installation and Configuration Guide

2.22
F45992-02
October 2021

ORACLE

Java Platform, Standard Edition Advanced Management Console Installation and Configuration Guide, 2.22

F45992-02

# Contents

## C Troubleshooting Tricks



## D Installing Advanced Management Console in a Clustered Environment — An Example

# Preface

This guide provides information about supported browser platforms and components required for installing and configuring the Advanced Management Console on machines running on Linux, Microsoft Windows, and macOS operating systems.

The AMC is available to enterprise customers within My Oracle Support.

> **Note:**
>
> The Advanced Management Console requires a commercial license for use in production. For information about commercial features and how to enable them, see Oracle Java SE Advanced & Suite Products.

## Audience

This document is intended for system administrators who are responsible for managing the Java desktop environment in their enterprise. The readers are expected to have some knowledge of browser platforms, Oracle WebLogic Server, and databases.

This document is intended for users who are installing any variant of the Java SE platform.

## Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

**Access to Oracle Support**

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

## Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry

standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

# Related Documents

See JDK 17 Documentation.

1

# What's New in Advanced Management Console

The Advanced Management Console (AMC) offers system administrators greater control in managing Java version compatibility and security updates for desktops within their enterprise.

See What's New In Advanced Management Console for the list of important changes and new features in this and previous releases of the Advanced Management Console .

2

# Plan for Advanced Management Console Installation

The Plan for Advanced Management Console Installation describes the Advanced Management Console core components, software requirements, and installation steps.

Read about software requirements and various components of AMC described in this section before you begin installation.

> **Note:**
>
> This release of the Advanced Management Console is primarily a bug fix release. For additional information about AMC releases, see the Advanced Management Console Release Notes.

The Plan for Advanced Management Console Installation contains the following sections:

- About Advanced Management Console
- Software Prerequisites and System Requirements for Advanced Management Console Components
- Installing and Configuring Advanced Management Console
- Migrating Advanced Management Console to the Latest Version

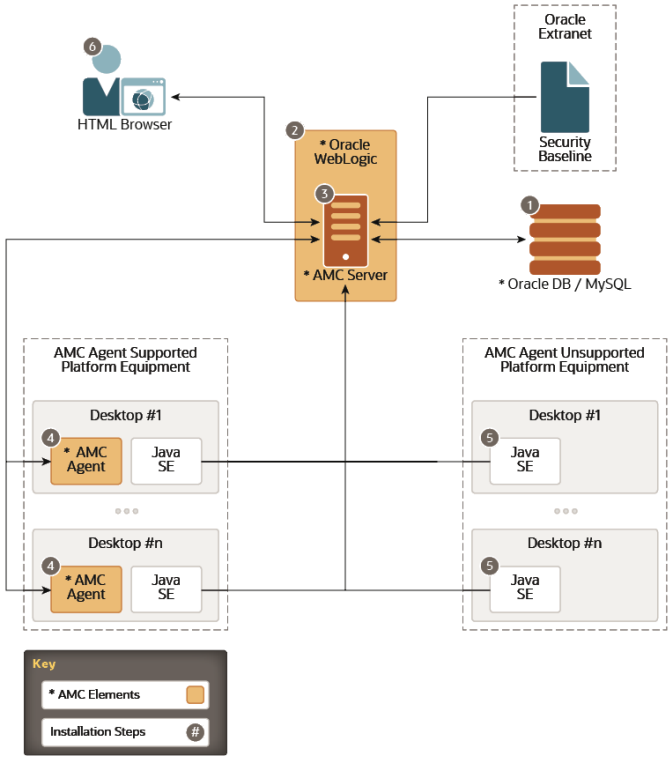
## About Advanced Management Console

The Advanced Management Console provides system administrators with insight into the Java applications that their users run and the versions of the Java Runtime Environment (JRE) that are used in their enterprise.

The Advanced Management Console is packaged as an Enterprise Archive (EAR) file. This file contains the AMC components, such as the Advanced Management Console server, agent, and browser-based user interface. You must provide the WebLogic Server, database, and a JRE for AMC to use.

The Figure 2-1 shows AMC architecture, components, data flow, and the installation sequence. The core components of the AMC are AMC server and AMC agent.

**Figure 2-1 Figure 2-1 Advanced Management Console Components and Installation Steps**




The following topics describe the core components and other elements of AMC:

- Advanced Management Console Server
- Advanced Management Console Agent
- Administration and Monitoring

## Advanced Management Console Server

The Advanced Management Console server uses MySQL or Oracle database to store its internal data and periodically downloads the Java Security Baseline from Oracle extranet. The Advanced Management Console server collects the Java Usage Tracking records of the Java SE runtime on Windows, macOS, and Linux desktops.

The Advanced Management Console server is a Java Platform Enterprise Edition (Java EE) application that must be deployed in Oracle WebLogic Server as shown in Figure 2-1.

## Advanced Management Console Agent

The Advanced Management Console (AMC) agent is another core component, which is deployed on Microsoft Windows and macOS desktops.

The agent automatically enables Java Usage Tracker on installed Java SE runtime. The agent periodically reports data (operating system family, version, and installed Java Runtime Environments) to the Advanced Management Console server. The

agent downloads and applies deployment rule set to the installed Java Runtime Environments (JREs). It automatically enables Java Usage Tracker on installed JREs.

> **Note:**
>
> CPU, memory, disc space, and network capacity requirements are all negligible for the AMC agent provided the appropriate OS and Java version are used.

The AMC agent is supported on desktops running on Windows, macOS, and Linux distributions having `systemd` or `upstart` service management framework. See Figure 2-1. For distributions not supported, the Java Usage Tracker can be configured manually.

## Administration and Monitoring

The Advanced Management Console includes a browser-based user interface for monitoring and administration.

This interface provides the following:

- Access to collect Java Usage Tracker data
- Enables to create and deploy deployment rule sets
- Monitors and configures the AMC

# Software Prerequisites and System Requirements for Advanced Management Console Components

Check the system requirements before setting up the Advanced Management Console to be sure that it runs in your environment.

| Component | Requirements | Supported Platform |
|---|---|---|
| Advanced Management Console Server | Software:<br>• Oracle WebLogic Server 12c R2<br>• Oracle WebLogic Server 14c<br>• Java Runtime Environment (JRE) 8u31 or later; use of the latest Java security update is recommended.<br>Minimum hardware configuration:<br>• Processor = 3 GHz CPU<br>• Memory = 8 GB available, and at least 4GB for WebLogic<br>• Disk Space = 10 GB | For supported configurations of WebLogic Server 14c and 12c R2, see:<br>Oracle Fusion Middleware Supported System Configurations<br>**Note:** AMC is not compatible with Oracle WebLogic Server 14c running on JDK 11 or beyond. |

| Component | Requirements | Supported Platform |
|---|---|---|
| Advanced Management Console Database | One of the following databases:<br>• Oracle Database 11g<br>• Oracle Database 12c<br>• Oracle Database 19c<br>• MySQL 5.6<br>• MySQL 5.7<br>• MySQL 8.0<br>A minimum of 12 GB memory is required for a dedicated Oracle server managing 120 K desktops and 16 GB memory is required if the Oracle server is co-existent with the WebLogic Server. Ensure that you have at least 20 GB free storage space for the Oracle Database. Also, maintain the database regularly as the data in the database might keep increasing over a period of time. | The list of supported platforms:<br>• Oracle Linux 7 (x64)<br>• Ubuntu Linux 14 (x64)<br>• SUSE Linux Enterprise Server 12 (x64)<br>• Windows 8.1 (x64)<br>• Windows Server 2012 R2 (x64)<br>• Windows 10<br>• Red Hat Enterprise Linux 7 (x64)<br>See the following links for information on:<br>• Driver support: WebLogic 12.2.1.3 Driver Support and WebLogic 12.2.1.4 Driver Support<br>• Oracle database requirements: Oracle Database Software Requirements<br>• MySQL requirements: MySQL Database Supported Platforms<br>. |
| Advanced Management Console Agent | | The list of supported platforms:<br>• Windows 8.x (x64, x86)<br>• Windows 10<br>• OS X 10.9 and above<br>• macOS 10.12 and above<br>• Linux: Oracle Linux 6+, RHEL 6+, CentOS 6+, Ubuntu 14.04+, SLES 12, Fedora 9+ |
| Advanced Management Console UI | One of the following browsers, depending on your platform:<br>• Internet Explorer 11 (Compatibility View is not supported)<br>• Firefox<br>• Safari<br>• Chrome<br>To run the Java Web Start applications that Advanced Management Console starts, Java Runtime Environment (JRE) 8u131 or later is required; use of the latest Java security update is recommended. If you use a 32-bit browser on a 64-bit system, then a 32-bit JRE is required. | • AMC UI is based on Oracle JET version 8. See JET FAQ for platform support.<br>• Refer to browser vendor websites for the supported platforms. |

> **Note:**
>
> It's recommended to consider upgrading the Advanced Management Console database to Oracle 12c and WebLogic server to WebLogic Server 12c R2 and later. See the Advanced Management Console downloads page.

The Advanced Management Console uses data collected by Java Usage Tracker. Java Usage Tracker is available for all releases of Java 7 and above, also for the following older Java releases:

- 6u25 and later updates
- 5.0u33 and later updates
- 1.4.2_35 and later updates

> **Note:**
>
> Java Usage Tracking is a feature of Oracle Java runtimes (JDK and JRE). Usage tracking is not available for Open JDK binaries.

# Installing and Configuring Advanced Management Console

The Advanced Management Console installation and configuration consists of the following steps. Complete each step in the process before proceeding to the next step.

1. Oracle Database Installation and Configuration for Advanced Management Console ,

   MySQL Database Installation and Configuration for Advanced Management Console . or

   Installing and Configuring the Oracle Database on Linux
2. Oracle WebLogic Server Configuration for Advanced Management Console
3. Advanced Management Console Server Deployment and Initialization
4. Advanced Management Console Agent Installation and Configuration
5. Java Usage Tracker Setup for Advanced Management Console
6. Browser Setup for Advanced Management Console

# Migrating Advanced Management Console to the Latest Version

The existing users of Advanced Management Console can update to the latest available version of the AMC server, database, and agent. The migration process involves both manual and automatic steps.

Advanced Management Console Migration describes the migration process.

3

# MySQL Database Installation and Configuration for Advanced Management Console

The database for the AMC provides data storage to host all the data. The database stores information about MSI files and applications, deployment rules, and deployment rule sets. The database also stores information about agents, Java Runtime Environment (JRE) statistics, and Java Installer configurations.

The AMC is also supported on Oracle Database.

This topic contains the following sections that describe software requirements and MySQL installation and configuration for the AMC:

- Software Requirements for MySQL Database
- Installing MySQL Database for Advanced Management Console

## Software Requirements for MySQL Database

To use MySQL database with Advanced Management Console , download and install a version of MySQL Server mentioned in Software Prerequisites and System Requirements for Advanced Management Console Components.

## Installing MySQL Database for Advanced Management Console

This topic contains the following sections that describe MySQL installation and configuration setup instructions for Advanced Management Console on different platforms:

- Installing MySQL Database on Windows
- Installing and Configuring MySQL on Linux

### Installing MySQL Database on Windows

To install MySQL database:

1. Install the MySQL database server only and select **Server Machine** as the configuration type.
2. Select the option to run MySQL as a service.
3. Launch the MySQL Command-Line Client. To launch the client, enter the following command in a Command Prompt window: `mysql -u root -p` .

   The `-p` option is needed only if a root password is defined for MySQL. Enter the password when prompted.
4. Create the user (for example, `amc2`) and a strong password:

   ```
   mysql> create user 'amc2' identified by 'amc2';
   ```

To restrict access to a machine (for example, to `localhost` for a user) create the user as follows:

```
mysql> create user 'amc2'@'localhost' identified by 'amc2';
```

5. Create the database (for example, `amc2`) and grant all access to the user (for example, `amc2` user):

   ```
   mysql> create database amc2;
   ```

   ```
   mysql> grant all on amc2.* to 'amc2';
   ```

6. Configure your MySQL installation to handle large BLOB entries, such as AMC Agent (installation) bundle and MSI binaries. To handle BLOB entries, edit the MySQL Option Files.

   MySQL is a Windows Service, so it can be started or stopped from the Windows Service administrator page. Any updates to the `my.ini` MySQL option file must be done by the administrator.

   To edit the `my.ini` file:

   a. Open the `my.ini` file in an editor. You must edit the file with administrator privileges.

      By default, on MySQL 5.6, the option file is located at `%PROGRAMDATA%\MySQL\MySQL Server 5.6\my.ini`.

      > **Note:**
      >
      > As of MySQL 5.7.18, `my-default.cnf` is no longer included in or installed by distribution packages. See Server Configuration Defaults in *MySQL Reference Manual*.

   b. Set the options `max_allowed_packet` and `innodb_log_file_size` in `my.ini` in the `[mysqld]` section to the values shown:

      ```
      [mysqld]
      max_allowed_packet=300M
      innodb_log_file_size=768M
      ```

      > **Note:**
      >
      > Ensure that there are no other values for `max_allowed_packet` and `innodb_log_file_size` that override the set value.

   c. Restart the MySQL service to apply changes.

The MySQL database user credentials provided in this topic are examples. The Advanced Management Console doesn't need to know your MySQL database user credentials. MySQL database user credentials are only required to configure the Data Source connection in the application server.

## Installing and Configuring MySQL on Linux

The following are example instructions to install and configure MySQL database for the Oracle Linux distribution of Linux operating system:

> **Note:**
>
> The MySQL commands might change from one version to another. For the latest commands, see MySQL Reference Manual.

Before you proceed with installation, ensure that the MySQL Yum repository is added to your system's repository list. This is a one-time operation, which can be performed by installing an RPM provided by MySQL.

1. Install the MySQL database server package.

   You can use the Yum tool to install MySQL on Oracle Linux: `sudo yum install mysql-community-server`.

   > **Note:**
   >
   > A password is auto-generated for the root user. Use the following command to extract the auto generated password:
   >
   > ```
   > grep 'A temporary password is generated for
   > root@localhost' /var/log/mysqld.log |tail -1
   > ```

2. Start the MySQL service:

   ```
   sudo systemctl start mysqld
   ```

3. Launch the MySQL Command-Line Client:

   ```
   mysql -u root -p
   ```

   The `-p` option is needed only if a root password is defined for MySQL. Enter the password when prompted.

   > **Note:**
   >
   > Reset the password, if required, using the following command:
   >
   > ```
   > ALTER USER 'root'@'localhost' IDENTIFIED BY '<strong password>';
   > ```

4. Create a user (for example, `amc2`) and a strong password:

   ```
   mysql> create user 'amc2' identified by '<strong password>';
   ```

   To restrict the access to a machine (for example, to `localhost` for a user) create the user as follows:

   ```
   mysql> create user 'amc2'@'localhost' identified by '<strong password>';
   ```

5. Create the database (for example, `amc2`) and grant all access to the user, for example, `amc2` as follows:

   ```
   mysql> create database amc2;
   ```

```
mysql> grant all on amc2.* to 'amc2';
```

6. Configure your MySQL installation to handle large BLOB entries, such as AMC Agent (installation) bundle and MSI binaries. To handle BLOB entries, edit the `my.cnf` file. For more information, see MySQL Option Files.

   To edit the `my.cnf` file:

   a. Open the `my.cnf` file in an editor. You can find the `my.cnf` file in one of the following locations:

      - `/etc/my.cnf`
      - `/etc/mysql/my.cnf`
      - `$MYSQL_HOME/my.cnf`
      - `[datadir]/my.cnf`

   b. Set the options `max_allowed_packet` and `innodb_log_file_size` in the `[mysqld]` section to the values shown:

      ```
      [mysqld]
      max_allowed_packet=300M
      innodb_log_file_size=768M
      ```

      > **Note:**
      >
      > Ensure that there are no other values for `max_allowed_packet` and `innodb_log_file_size` that override the set value.

   c. Restart the MySQL service to apply changes.

      ```
      sudo systemctl mysqld restart
      ```

The MySQL database user credentials provided in this topic are examples. The Advanced Management Console doesn't need to know your MySQL database user credentials. MySQL database user credentials are only required to configure the Data Source connection in the application server.

4

# Oracle Database Installation and Configuration for Advanced Management Console

The database for Advanced Management Console provides data storage to host all the data.

The database stores information about MSI files, applications, deployment rules, and deployment rule sets. The database also stores information about agents, Java Runtime Environment (JRE) statistics, and Java Installer configurations. This chapter contains the following sections that describe software requirements for the Oracle Database as well as installation and configuration procedures:

- Software Requirements for Oracle Database
- Installing Oracle Database on Windows
- Configuring Oracle Database on Windows
- Installing and Configuring the Oracle Database on Linux

## Software Requirements for Oracle Database

To use Oracle Database with Advanced Management Console , download and install a supported version of the Oracle database from Oracle Database Software Downloads.

## Installing Oracle Database on Windows

> **Note:**
>
> To install Oracle 11g database, see Oracle 11g Documentation.

This topic describes installation steps for Oracle Database 12c.

To install Oracle database for Windows operating system:

1. Go to Oracle Database Software Downloads in your browser.
2. Download the 64-bit `.zip` file. Select the `.zip` file and right click to select **Extract All**. Extract both the `.zip` files to the same folder.

   Don't extract the archive using `unzip` command, which may result in an unsuccessful run of the `setup.exe`.
3. Run the `setup.exe` and select the installation options according to your database and Windows user requirements.
4. In the **Specify Database Identifiers** screen of the installation process, enter the Global database name (for example, `amc2`) and the Oracle system identifier, SID (for example,

amc2). Don’t select the check box for the option **Create as Container database**. The Install button gets enabled.

5. Click **Install** to install the product.

   Oracle Database is installed on Windows.

6. Start the SQL Plus application. From the command-line, enter the command SQLPLUS to start SQL Plus.

From Windows **Start**, click **Programs**, Oracle-*OraHomeName*, **Application Development**, and **SQL Plus**.

# Configuring Oracle Database on Windows

After installing Oracle database for Advanced Management Console on Windows, you need to configure it.

To configure Oracle database on Windows:

1. Log in to SQL*Plus application with `sys as sysdba` and the password you opt during the installation process in the Schema Password step.
2. Create the user (for example, `amc2`) and grant access to the database (for example, `amc2`). The database name is the one that you set in Installing Oracle Database on Windows.

   ```
   SQL> CREATE USER amc2 IDENTIFIED BY amc2
   DEFAULT TABLESPACE users
   QUOTA UNLIMITED ON users PASSWORD EXPIRE;
   SQL> CREATE ROLE amc2_role;
   SQL> GRANT CREATE SESSION, CREATE TABLE, CREATE SEQUENCE, CREATE VIEW,
   CREATE TRIGGER to amc2_role;
   SQL> GRANT amc2_role TO amc2;
   ```

   Configure your Oracle database `QUOTA` to `UNLIMITED` to ensure that enough database storage is available to support large BLOB entries, such as MSI binaries. If you encounter an issue with the SQL Create User statement, then log out of SQL*Plus application and repeat step 1 and step 2.

3. After you successfully create the user, exit the SQL*Plus application and log back into SQL*Plus as user (for example, `amc2`). You are prompted to set up the password. Set up a strong password.

The Oracle Database user credentials provided in this topic are examples. The AMC doesn’t need to know your database user credentials. Oracle database user credentials are only required to configure the Data Source connection in the application server.

# Installing and Configuring the Oracle Database on Linux

The configuration requires root authority, so make sure that you can get root authority before you begin to install and configure the Oracle database. However, do not start the installer as root user.

To install and configure the Oracle database on Linux:

1. Connect to the server by using SSH or VNC, as appropriate.
2. Unzip your database installer.

3. In your shell, run the `ulimit -s 10240` command . This is the setting for maximum stack size limitation, which is required for the database installation. In addition, edit the `/etc/security/limits.conf` file to set the following `nofile`, `nproc`, `stack`, and `memlock` values for database user deployment:

```
deployment   soft   nofile    1024

deployment   hard   nofile    65536

deployment   soft   nproc    16384

deployment   hard   nproc    16384

deployment   soft   stack    10240

deployment   hard   stack    32768

deployment   hard   memlock    134217728

deployment   soft   memlock    134217728
```

4. Validate that `/etc/pam.d/login` contains the following line:

```
session include system-auth
```

.

If `/etc/pam.d/login` doesn't it, then add the following line:

```
# echo 'session include system-auth' >> /etc/pam.d/login
```

5. Validate that `/etc/pam.d/system-auth` contains the following line:

```
session required pam_limits.so
```

If `/etc/pam.d/system-auth` doesn't it, then add the following line:

```
# echo 'session required pam_limits.so' >> /etc/pam.d/system-auth
```

6. Log in as the database software owner and validate the following shell limits:

```
-bash-4.2$ ulimit -Sn
1024

-bash-4.2$ ulimit -Hn
65536

-bash-4.2$ ulimit -Su
16384

-bash-4.2$ ulimit -Hu
16384
```

```
-bash-4.2$ ulimit -Ss
10240

-bash-4.2$ ulimit -Hs
32768

-bash-4.2$
```

7. Change to the directory where your database installer is unzipped and start the Install wizard by running the `./runInstaller` command. Provide the required information and then click **Next**. Use the default selection in this wizard and then click **Next**.
8. On the Select System Class page, select **Desktop class** and click **Next**.
9. On the Typical Installation page, perform the following:
   a. Specify the install location information.
   b. Verify that the Global database name is `orcl` and then click **Next**.
10. On the Create Inventory page, set the product inventory location and click **Next**.
11. In the Install wizard, click **OK**.

    A summary of the prerequisite checks is displayed. Click **Install** to start the database installation. Ensure that you run the scripts during the installation.
12. Follow the instructions in the wizard and run the scripts.

    The `ENV` scripts are copied to `/usr/local/bin`. You can change the path if you want to.
13. Click **OK** in the Installation wizard to continue with the installation.
14. When installation is completed, click **Close** to close the wizard, and then run the `cat/etc/oratab` command to check the installation information.
15. Run the scripts under `scratch/deployment/app/oraInventory`. If you did not use the default Oracle base location during installation, then change it accordingly.
16. Switch to the database file location and create an `amc2` directory for PDB.
17. Using sqlplus, connect to the database as `sysdba` and enter the following command to create PDB:

```
CREATE PLUGGABLE DATABASE amc2 ADMIN USER amc2 identified by
"amc2" DEFAULT TABLESPACE USERS DATAFILE '/scratch/deployment/app/
deployment/oradata/orcl/amc2/users01.dbf' SIZE 250M AUTOEXTEND ON
FILE_NAME_CONVERT=('/scratch/deployment/app/deployment/oradata/orcl/
pdbseed/', '/scratch/deployment/app/deployment/oradata/orcl/amc2/');
```

18. Change the database session to `AMC2` and make sure that `AMC2` is open:

```
alter session set container=amc2;


alter pluggable database amc2 open;
```

    a. Configure and set the authority for user `AMC2`.

The following is the command to grant authority to amc2:

```
 grant CREATE SESSION, CREATE TABLE, CREATE SEQUENCE, CREATE VIEW to
amc2;
```

The following is the command to set the quota:

```
alter user amc2 quota unlimited on users;
```

b. Save the state of AMC2.

19. Stop the listener and exit sqlplus.

To stop the listener, use the following command:

```
$ORACLE_HOME/bin/lsnrctl stop
```

.

20. Make sure the listener port in the configuration file is set to 1521.

You can edit the configuration file $ORACLE_HOME/network/admin/listener.ora as follows:

```
LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP)(HOST = your_host_name)(PORT = 1521))
      (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC1521))
    )
  )
```

21. Edit the TNS configuration file, $ORACLE_HOME/network/admin/tnsnames.ora:

```
LISTENER_AMC2 =
  (ADDRESS = (PROTOCOL = TCP)(HOST = localhost)(PORT = 1521))
ORCL =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = localhost)(PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = orcl)
    )
  )
AMC2 =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = your_host_name)(PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = amc2)
    )
  )
```

22. After setting the two configuration files correctly, start the listener again by entering the following command:

    ```
    $ORACLE_HOME/bin/lsnrctl start
    ```

23. Make sure that the database listener is running by using the following command:

    ```
    $ORACLE_HOME/bin/lsnrctl services
    ```

If you are a database administrator, then use ORAchk to check for the Oracle database:

1. Download ORAchk from MOS.

    > **Note:**
    >
    > MOS is available at https://support.oracle.com.

2. Copy `orachk.zip` on SRVDB and extract it.
3. Run `./orachk` as a root user to check the Oracle database and generate HTML report. This creates a zip file of the report that contains an HTML file. The report includes any issues that were found along with links to MOS notes or documentation to fix the issues.

5

# Oracle WebLogic Server Configuration for Advanced Management Console

The WebLogic Server instance provides web services to communicate with the agents and the data source to access the database. It also provides a user interface (UI) to configure the Advanced Management Console and the Java Usage Tracker parser as Advanced Management Console server components.

The Oracle WebLogic Server Configuration for Advanced Management Console topic contains the following sections that describe software requirements for installing and configuring Oracle WebLogic Server for AMC:

- Software Requirements for Oracle WebLogic Server
- Installing WebLogic Server
- Configuring WebLogic Server with Databases
- Deploying JAX-RS 2.0 to WebLogic Server Deployment Libraries
- Setting Up WebLogic Server JTA
- Setting Up Java Heap Size and Proxy Servers
- Trusted HTTPS Certificate
- Setting Up WebLogic Server Mail Notification
- Securing WebLogic Server Configuration

## Software Requirements for Oracle WebLogic Server

The Advanced Management Console requires Oracle WebLogic Server and Java SE Development Kit 8 Downloads.

If you're using Oracle WebLogic Server for only the AMC, then in Oracle WebLogic Server Installers for Development, go to Oracle WebLogic Server 12c R2 or later, and then select **Zip distribution for macOS, Windows, and Linux** option. If you have a license for Oracle WebLogic Server, then you can download the packages from Oracle Software Delivery.

## Installing WebLogic Server

There are different ways of installing Oracle WebLogic Server. Oracle WebLogic Server Installation Example provides an example of installing, creating a domain, creating an Administration Server, and creating a Managed Server for Oracle WebLogic Server.

> **Note:**
>
> For production use, it is recommended to deploy AMC onto Managed Servers only.

# Configuring WebLogic Server with Databases

This topic contains the following sections that describe how to configure Oracle WebLogic Server with databases and deploy the JDBC server:

- Configuring WebLogic Server with MySQL Database
- Configuring WebLogic Server with the Oracle Database

## Configuring WebLogic Server with MySQL Database

You can configure Oracle WebLogic Server with MySQL database to provide services to access and modify user data. The database is accessed using JDBC.

To configure WebLogic Server with the database:

1. Open the Oracle WebLogic Server Administration Console in a browser.
   - If the SSL listen port is configured in the WebLogic Server instance, then go to `https://wls-hostname:port/console`. For example:

     ```
     https://localhost:7002/console
     ```

   - If the SSL listen port is not configured in WebLogic Server, then go to `http://wls-hostname:port/console`. For example:

     ```
     http://localhost:7001/console
     ```

2. From the **Domain Structure** block in the left panel, select **Domain**, **Services** and then select **Data Sources**.
3. Create a new Generic Data Source. Set the data source name (for example, `amc2 mysql`).
4. Set the **JNDI Name** to `amc2/db/mysql`. This is the critical value for the AMC to locate the data source object.
5. Select the database type as `MySQL`.
6. For MySQL 5.x, select the database driver as `MySQL's Driver (Type 4) Versions:using com.mysql.jdbc.Driver`. For MySQL 8, you need to use `MySQL's Driver (Type 4) Versions:using com.mysql.cj.jdbc.Driver`.
7. In the **Transaction Options** section, ensure that the **Supports Global Transactions** check box is **not** selected. Advanced Management Console doesn't support global transactions.
8. Set the database name to your MySQL database name you created when performing procedures in MySQL Database Installation and Configuration for Advanced Management Console .
9. Set the database *`host-name`* and `port` to:
   - The host name where Oracle Database resides.
   - Leave `port` as the default or change it to the database port if it is different.
10. Set the database user name and password for your MySQL database (for example, user name as `amc2` and a strong password). The MySQL database user

name and password are the values you configured when performing procedures in MySQL Database Installation and Configuration for Advanced Management Console .

11. In the **Properties** text box, add the following lines to enable Unicode for this JDBC connection:

    `useUnicode=yes`

    `characterEncoding=UTF-8`

12. On the **Select Targets** page, select the servers where you want to deploy the Advanced Management Console.
13. Click **Finish** to save the changes.
14. In **Data Sources**, click the data source that you just created.
15. Click the **Connection Pool** tab.
16. Set **Maximum Capacity** to `50`.
17. Click **Save** to save the changes.

The AMC doesn't need to know your database user credentials. MySQL database user credentials are only required to configure the data source connection in the application server; therefore, the **JNDI Name** mentioned in step 4 is critical for the setup.

When the WebLogic Server is configured with the database, deploy the JDBC data source for the database to connect to WebLogic Server.

## Configuring WebLogic Server with the Oracle Database

You can configure Oracle WebLogic Server with the Oracle database to provide services to access and modify user data. The database is accessed by using JDBC.

To configure WebLogic Server with the Oracle Database:

1. Open the Oracle WebLogic Server Administration Console in a browser.
   - If the SSL listen port is configured in the WebLogic Server instance, then go to `https://wls-hostname:port/console`. For example:

     `https://localhost:7002/console`

   - If the SSL listen port is not configured in WebLogic Server, then go to `http://wls-hostname:port/console`. For example:

     `http://localhost:7001/console`

2. From the **Domain Structure** block in the left panel, select **Domain Services**, and then select **Data Sources**.
3. Create a new Generic Data Source. Set the data source name. For example, `amc2 oracle`.
4. Set the **JNDI Name** to `amc2/db/oracle` if the database is Oracle 12c or later. If the database is Oracle 11g, then set the JNDI Name to `amc2/db/oracle11`.

   This is the critical value for AMC to locate the Data Source object.
5. Select the database type as `Oracle`.

6. Select the database driver as `Oracle's Driver (Thin) for Instance Connections`, and Versions as `Any`.
7. In the **Transaction Options** section, ensure that the **Supports Global Transactions** check box is **not** selected. Advanced Management Console doesn't support global transactions.
8. Set the database name to the Oracle Database name created when performing the procedures in Oracle Database Installation and Configuration for Advanced Management Console .
9. Set the database *`host-name`* and `port` to:
   - The host name where Oracle Database resides.
   - Leave `port` as the default or change it to the database port if it is different.
10. Set the database user name and password for your Oracle Database.

    The Oracle database user name and password are the values that you configured when performing the procedures in Oracle Database Installation and Configuration for Advanced Management Console . For example, a user name of `amc2` with a strong password.
11. Change the URL so that it contains a backslash (/) instead of a colon (:) after `port`.

    For example:

    ```
    jdbc:oracle:thin:@oracledb-hostname:port/amc2
    ```
12. In the **Properties** text box, add the following lines to enable Unicode for this JDBC connection:

    ```
    user=amc2
    useUnicode=yes
    characterEncoding=UTF-8
    ```
13. Click **Next**.
14. On the **Select Targets** page, select the servers where you want to deploy the Advanced Management Console.
15. Click **Finish** to save the changes.
16. In **Data Sources**, click the data source that you just created.
17. Click the **Connection Pool** tab.
18. Set **Maximum Capacity** to 50.
19. Click **Save** to save the changes.

The AMC doesn't need to know your Oracle Database user credentials. The Oracle Database user credentials are only required to configure the Data Source connection in the application server. The **JNDI Name** mentioned in step 4 is critical for the setup.

After WebLogic Server is configured with the database, deploy the JDBC data source for the database to connect to WebLogic Server.

# Deploying JAX-RS 2.0 to WebLogic Server Deployment Libraries

If the Advanced Management Console needs to use JAX-RS 2.0 RESTful Management API for Web Services, then you must deploy the `jax-rs-2.0.war` file to WebLogic Server deployment libraries.

To deploy the file from the WebLogic Server Administration Console:

1. Log in to the WebLogic Server `Administration` console.
2. From the **Domain Structure** block in the left panel, select **Deployments**.
3. Click the **Install** button.
4. For a Windows operating system, enter the path `%MW_HOME%\wlserver\common\deployable-libraries`.

   For a Linux operating system, enter the path `$MW_HOME/wlserver/common/deployable-libraries`.
5. Select `jax-rs-2.0.war`.
6. Accept the default values for all the rest of the settings and then click **Next**, **Next**, **Next**, and **Finish**.
7. Check in the **Deployments** section for a new entry `Name=jax-rs(2.0)` and `Type=Library`.
8. From the Deployments list, click `jax-rs(2.X.X)`, then the **Targets** tab, and select the servers where you want to deploy the Advanced Management Console .
9. Click **Save**.

# Setting Up WebLogic Server JTA

Errors in WebLogic Server may occur if the Java transaction timeout interval is not set to a long enough value for the database access. You need WebLogic Server administrator credentials to define the timeout interval using the Java Transaction API (JTA).

To define the Java Transaction API (JTA) configuration for the WebLogic Server domain time out to 300 seconds:

1. Log in to the WebLogic Server `Admin` console.
2. From the **Domain Structure** block in the left panel, go to **Services** and select **JTA** from services.
3. Click the **Configurations** tab and then click the subtab **JTA**.
4. On the Java Transaction API (JTA) page, enter the **Timeout Seconds** value as 300.

# Setting Up Java Heap Size and Proxy Servers

If direct access to the Internet from the server is not available, then you should set up the proxy server for the WebLogic Server. The Advanced Management Console requires access to Java Security Baselines. Internet access is also required to introspect JNLP files if they're

outside of the corporate network. For example, when you launch a JNLP application from Oracle Tutorials, in order to display the information correctly, the Advanced Management Console needs to download the JNLP file as well as the referenced jars.

To set up the Java Heap Size and proxy servers:

1. Log in to the WebLogic Server Administration Console.
2. From the Administration Console, go to **Environment**, select **Servers**, and then select the **Managed Server**.
3. Click the **Configuration** tab, and then click the **Server Start** sub tab.
4. Add the following VM options to the `Arguments` text field, which includes heap size and proxy settings (both HTTPS and HTTP proxy settings).

```
-Xmx4G
-Dhttps.proxyHost=<host_name> -Dhttps.proxyPort=<proxy_port>
-Dhttp.proxyHost=<host_name> -Dhttp.proxyPort=<proxy_port>
-Dhttp.nonProxyHosts=<server_hostname|server_IP>
```

**Note:**

- Replace the *<host_name>*, *<proxy_port>*, *<server_hostname>*, and *<server_IP>* with actual values corresponding to your environment. An example configuration values:

  ```
  -Dhttps.proxyHost=proxy.example.com -Dhttps.proxyPort=80
  -Dhttp.proxyHost=proxy.example.com -Dhttp.proxyPort=80
  -Dhttp.nonProxyHosts=localhost
  ```

  See Java Networking and Proxies for more details on the proxy configuration.
- Ensure that you don't specify the JVM properties if your environment does not require a proxy.
- You need to adjust the Java Heap Size as recommended. Oracle recommends 4 GB heap size or higher. The `-Xmx4G` option changes the maximum heap size to 4 GB. A 32-bit JVM cannot be started with 4GB heap size, therefore it is recommended to use a 64-bit JVM.

# Trusted HTTPS Certificate

The Advanced Management Console uses HTTPS only for communication between the AMC server and clients (agent, web UI, Deployment Rule Set tool, and Java installer configuration). The HTTPS setup for AMC requires a valid HTTPS certificate, trusted by the client-side Java Runtime Environment (JRE).

Ensure that a valid HTTP certificate is available and that the Oracle WebLogic Server Identity Keystore is set up with it. See Configuring Keystores in the *Oracle Fusion Middleware Administering Security for Oracle WebLogic Server 12c* guide.

> **Note:**
>
> You can use self-signed certificates only for demonstrations and not in production systems.

# Setting Up WebLogic Server Mail Notification

The Advanced Management Console server optionally sends an email notification to managed desktop users who register agents with their credentials. The AMC server uses JavaMail APIs built into the Oracle WebLogic Server to act as a medium between the AMC and the actual SMTP mail server. The WebLogic Server must be configured to use a specific mail server.

To configure WebLogic Server for mail notification setup in the WebLogic Server console:

1. Log in to the WebLogic Server Administration Console.
2. From the domain structure block, select **Services** and **Mail Sessions**.
3. Click **New** and complete the form.

Complete the form with the following details:

1. Name: Provide an arbitrary name.
2. JNDI Name: Provide the JNDI name as `amc2/mail`. This is a critical value for the mail server setup.
3. Provide your session user name and password.
4. Set up the JavaMail properties.

   ```
   mail.transport.protocol=smtp

   mail.smtp.ssl.enable=true

   mail.smtp.auth=true

   mail.smtp.host=<your email host name>
   ```

5. To trace SMTP sessions, set `mail.debug=true`.
6. Click **Next** and then select the server that AMC is deployed on.
7. Click **Finish**.
8. Restart the server.

In the AMC user interface, the **Settings** sub tab of the Configuration tab has a check box to enable or disable WebLogic Server mail notifications. If no JNDI name is found, then this check box is disabled and you cannot enable WebLogic Server mail notifications.

# Securing WebLogic Server Configuration

You can use the Java Security Manager in WebLogic Server to provide protection for resources running in a Java Virtual Machine (JVM), and to improve the Advanced Management Console security.

6

# Advanced Management Console Server Deployment and Initialization

You can use an HTML browser and the AMC User Interface (UI) for deploying the Advanced Management Console to Oracle WebLogic Server and initializing the product.

This topic contains the following sections that describe the AMC server deployment to WebLogic Server and the initialization process using the AMC UI:

- Deploying Advanced Management Console to WebLogic Server
- Initializing Advanced Management Console

## Deploying Advanced Management Console to WebLogic Server

The Advanced Management Console server is packaged as a J2EE Enterprise Archive (EAR) (`JavaAMC-2_7.ear`). This file contains the AMC components, such as the AMC server, agent, and browser-based user interface.

Ensure that the AMC server is deployed to an existing Oracle WebLogic Server instance as listed in Software Requirements for Oracle WebLogic Server.

Follow this example to deploy the AMC server to Oracle WebLogic Server:

1. Enter `https://`*`wls-hostname`*`:`*`port`*`/console` in the browser, where the *`wls-hostname`* and *`port`* are the DNS name and listen port of the Administration Server.
2. Authenticate using your administrator credentials.
3. Select the **Deployments** option from the **Domain Structure** panel.
4. In the right panel, click **Install**.
5. In the navigation panel, locate `JavaAMC-2_7.ear` file and check it in.
6. Click **Next** and select the server that the AMC is getting deployed on. Then, click **Next** and again **Next**.
7. Click **Finish**.
8. Start the AMC
    a. In the Deployments table, go to the Control tab and select the check box for the AMC application.
    b. Click **Start** and select **Servicing All Requests**.

       A message is displayed that indicates that a start request was sent. When the **State** column for the AMC application shows `Active`, then the application is available to anyone with access to the server.

For alternate deployment methods, see the Installing the Oracle WebLogic Server and Coherence Software in the *Fusion Middleware Installing and Configuring Oracle WebLogic Server and Coherence* guide.

# Initializing Advanced Management Console

Initialize Advanced Management Console after you deploy the AMC server to Oracle WebLogic Server. The initialization process is an interactive process using a web browser and AMC web UI.

The AMC server initialization web page is not protected and can be accessed by any user.

> **Note:**
>
> When the AMC is initialized in an Oracle WebLogic Server cluster, the host name and port in the initialization wizard must match the load balancer, and not any of the back-end servers.

To initialize the AMC server:

1. Enter `https://wls-hostname:port/amcwebui` in the browser, where *`wls-hostname`* and *`port`* are the DNS name and the listen port number of your WebLogic server instance (the default port is 7002). A Welcome screen is displayed, which is the first screen in the initialization process after deployment to WebLogic Server.

   In case of errors, see Troubleshooting Tricks.

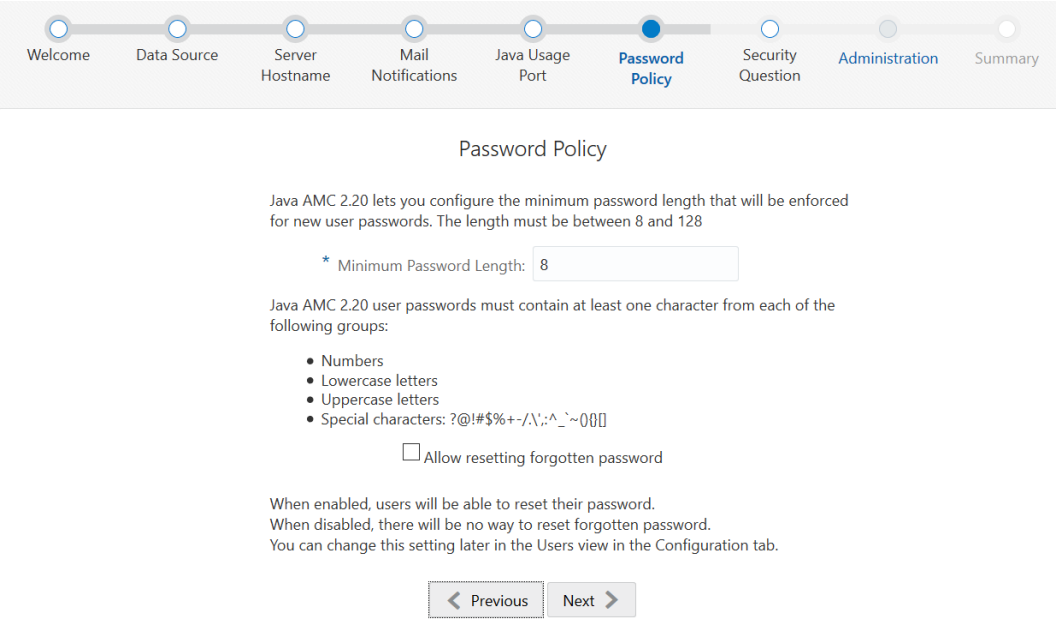
2. Click **Next** on the **Welcome** screen to set up the data source. On this page, the Advanced Management Console reports that it has detected the data source, `amc2/db/mysql` or `amc2/db/oracle` configured in your Oracle WebLogic Server.

3. Click **Next** to set up the Advanced Management Console server host name. The host name specified here is the DNS name that desktops use to connect to the Advanced Management Console server. Do not use `localhost` as the host name. If Oracle WebLogic Server is hosted on a machine with multiple DNS names, then ensure that the name specified on the page enables ***Desktops*** to reach Oracle WebLogic Server.

4. Click **Next** to set up the Advanced Management Console server Java usage port number. Set up a dedicated free port number for collecting Java Usage data sent by a Java Virtual Machine.

5. Click **Next** to display the Password Policy section. Configure the minimum password length for new user accounts. Also, read the Password Rules section in the *Java Platform, Standard Edition Advanced Management Console User's Guide* for the requirements for user account passwords.

**Figure 6-1 Advanced Management Console - Password Length**




6. Click **Next** to setup the Security questions. You can select any three questions from the drop-down and provide your answers.

   These questions will be prompted during password reset and you need to provide correct answer for any one question.

7. Click **Next** to set up the administrator credentials, such as e-mail and a password to access AMC. The administrator has access to all features of AMC Console.

8. Click **Next** to see the summary details of all the AMC credentials. At this step, the MySQL or Oracle database is automatically initialized by the AMC.

9. Finally, click **Initialize** to initialize the AMC server. AMC Successfully Initialized screen is displayed with instructions on the next steps to log in to AMC.

> **Note:**
>
> After you click **Initialize**, the actual time taken to complete the background initialization process may vary. Therefore, don't click **Initialize** again. Wait until you see the status message indicating successful initialization.

> **Note:**
>
> Once the Advanced Management Console has been initialized, you can modify the host name and/or port in the **Configuration** tab. If the Advanced Management Console has been initialized on the WebLogic Server cluster, then ensure that these are values of the load balancer. See Modifying Advanced Management Console Server Host Name.

7

# Advanced Management Console Agent Installation and Configuration

The Advanced Management Console agent runs as a native service with the operating systems (Windows, Linux, and macOS) on a client desktop. The agent finds all the installed Java Runtime Environments (JREs), and then enables and automatically configures Java Usage Tracker. In an enterprise network, the agent enables the Java Usage Tracker on agent-managed desktops. At system startup, the agent reports the data on the AMC client. The agent periodically reports data (operating system family, version, and installed JREs) to the AMC server. The agent downloads and applies the Deployment Rule Set to the installed JREs. It automatically enables the Java Usage Tracker on installed JREs on Windows, Linux, and macOS operating systems.

This topic contains the following sections that describe the AMC agent, agent bundle, agent installation, and agent distribution:



## About Advanced Management Console Agent

The Advanced Management Console agent is a background service.

The Advanced Management Console agent performs the following tasks:

- Identifies all the installed JREs on the desktop and reports the resulting list to the AMC server.
- Enables Java Usage Tracker for each JRE in which Java Usage Tracker is available.
- Downloads deployment rule sets from the AMC server and installs them on each JRE.

Advanced Management Console supports Windows, macOS, and Linux distributions (with `systemd` or `upstart` service management framework). See Software Prerequisites and System Requirements for Advanced Management Console Components for details. For platforms that are not supported, the Java Usage Tracker can be configured manually.

The AMC server and all its components use different protocols to communicate.

## Advanced Management Console Agent Bundle

The Advanced Management Console agent is bundled as a `.zip` file.

The bundle file is configured with Application server URL and Application server certificate chain details. You can download the agent bundle from the Advanced Management Console server through the Advanced Management Console User Interface (UI). The bundle installs the agent on the desktop that must be managed by the Advanced Management Console server.

The Advanced Management Console agent bundle is configured to the Advanced Management Console server that it has been downloaded from.

> **Note:**
>
> If multiple agents from different servers are installed on the same machine, then the earlier configurations will be overwritten by the latest agent installation. The system is configured to communicate with the server from which the latest agent bundle was downloaded.

# Installing Advanced Management Console Agent

The Advanced Management Console agent installation requires administrator privileges and should be performed by a system administrator.

This topic contains the following sections:

- Configuring the Agent Proxy and the Agent Intervals
- Installing Advanced Management Console Agent on Windows
- Installing Advanced Management Console Agent on Linux
- Installing Advanced Management Console Agent on macOS

## Configuring the Agent Proxy and the Agent Intervals

The agent proxy server is included in the bundle. If the bundle is already downloaded and the proxy is changed later, the bundle will not contain the proxy settings.

To configure the agent proxy and the agent intervals:

1. Enter `https://server:port/amcwebui` in the browser and log in to the AMC UI by using administrator credentials to initialize the AMC. See Initializing Advanced Management Console .
2. Configure the agent proxy server host and port.

   > **Note:**
   >
   > Step 2 must be completed before the agent bundle is downloaded. If a proxy server is required to access the AMC Server, then the agent would not be able to reach the server to register without this information.

   a. In the Advanced Management Console UI, click the **Configuration** tab.
   b. Click **Agents Download**.

c. Click **Edit** to display the **Configure AMC Agent Proxy Settings** dialog.

d. Enter the following details for the agent to connect to the Advanced Management Console server:

- **Agent Proxy Host Name**: Specify a proxy server host name.
- **Agent Proxy Port**: Specify a proxy server port number.

e. Click **Save**.

3. Configure the agent intervals.

> **Note:**
>
> If you increase the agent intervals, then the system load is reduced. When the agent intervals are increased, the communication of the agent with the Advanced Management Console server automatically decreases, which reduces the system load.

a. Click the **Configuration** tab.

b. Click **Agent Settings**.

c. Click **Edit** to make the fields editable.

d. Edit any of the following values. You can either edit all of them or just the ones that you want to:

**JUT Processing Interval**
Interval for the agents to report Java Usage Tracker records to the server

**Check Command Interval**
Interval to check if the server has any commands for the agent

**Standard JRE Scan Interval**
Interval to scan Java Runtime Environment (JRE) in the standard location (For example, on Windows it is `C:\Program Files\Java`) and report to server

**Application JRE Scan Interval**
Interval to scan JRE under the application location (For example, on Windows it is C:\Program Files) and report to server

**LocalStorage JRE Scan Interval**
Interval to scan JREs in the entire local storage system (not targeting any particular directory) and report to server

**Agent Auto Update**
Enable or disable the agent auto update

**Agent Log File Max Size (Kb)**
Maximum agent log file size in Kb

**Number of Agent Log Files**
Maximum agent log file number during agent log rotation

**Randomize Interval**
Enable or disable randomize interval

e. Click **Save**.

# Installing Advanced Management Console Agent on Windows

Ensure that the Advanced Management Console server is running and can be accessed by the desktop before you install the AMC agent on a desktop.

To install the agent on Windows:

1. Configure the agent proxy and the agent intervals. See Configuring the Agent Proxy and the Agent Intervals.

   The agent proxy server is included in the bundle. If you change the proxy server settings, you will need to download the agent bundle again and distribute the updated bundle.

2. On the Advanced Management Console UI, click the **Configuration** tab and select **Agents Download**.

   > **Note:**
   >
   > When you select **Agents Download**, you might need to wait for the SHA256 values to finish computing. If the bundle isn't already generated, it takes a short time to build it. Once it's shown, the bundle is ready to download.

3. Click the required bundle link, either `agent-bundle-win32.zip` or `agent-bundle-win64.zip` and save the bundle.

   > **Note:**
   >
   > - The `agent-bundle-win32.zip` bundle should be used for agent installations on 32-bit Windows platform. 32-bit support for Advanced Management Console agent is provided only for Windows operating systems.
   > - When you download an agent bundle, the Advanced Management Console inserts parameters, such as the application server URL and the application server certificate chain into the bundle. This restricts the agent bundle to a specific instance of the Advanced Management Console server at any given time. If you modify the URL or the certificate, then you must download the agent bundle from `https://server:port/amcwebui`.

4. Open the Windows File Explorer, select the `.zip` file, and right click to choose **Extract All**.

   Don’t use the Cygwin utility to extract the agent bundle. The Cygwin extract utility gives improper file permissions that prevents the agent from starting.

5. Move the `AMC_Agent` directory to a location, for example, `C:\Program Files (x86)\Oracle\Java AMC\` (or a directory of your choice, for example,

`C:\AMC_Agent`). In the following steps, `C:\AMC_Agent` represents `%AMC_DIR%`, where the AMC agent gets installed. Ensure that the contents of the folder can be accessed by privileged users only.

6. Starting with Advanced Management Console 2.2, this is an optional step. Copy `%AMC_DIR%\conf\AMCUser.properties.template` to `%AMC_DIR%\conf\AMCUser.properties` and configure the three information values with the user's actual credentials.
7. Open a Windows command prompt with administrator privileges. Run `%AMC_DIR%\bin\AMCAgent.exe -install`.

   The agent is registered with the Advanced Management Console server for the provided user credentials.

> **Note:**
>
> Ensure that the Advanced Management Console server is running and that the desktop can connect to the server. Beginning with Advanced Management Console 2.4, if the server is down or cannot be reached, then the agent service tries to register itself with the server once each hour after the first failure. The next time the agent service is started, it tries again to connect to the server.

8. Select the **Control Panel**, **Administrative Tools** and then select **Services**. Check that the agent service is up and running.
9. If the agent service doesn't start, some log messages may also be available in Windows Event Viewer. Select **Control Panel**, **Administrative Tools**, and **Event Viewer** to view the logs.
10. Log in to Advanced Management Console web UI again. Go to the **Desktops** page and check that the desktop is now registered with the Advanced Management Console server. If the user's credentials were configured in step 6, then the desktop owner now appears as Owner in the Advanced Management Console UI.

## Installing Advanced Management Console Agent on Linux

You can use the `bin/AMCAgent.sh` script file to install and uninstall the Advanced Management Console agent on the Linux operating system. The Advanced Management Console agent is a native service that you can start, stop, or restart from the Linux terminal.

To install the Advanced Management Console agent on the Linux operating system:

1. Configure the agent proxy and the agent intervals. See Configuring the Agent Proxy and the Agent Intervals.

   The agent proxy server is included in the bundle. If you change proxy server settings, you will need to download agent bundle again and distribute the updated bundle.
2. On the Advanced Management Console UI, click the **Configuration** tab and select **Agents Download**.
3. Click the link `agent-bundle-linux64.zip` and save the bundle to a desired location.
4. Start a Linux terminal. Goto the folder where the `zip` file was downloaded. Extract the `zip`. In the following steps, `${AMC_DIR}` represents the `AMC_Agent` directory where the Java Advance Management Agent files are extracted.

5. Starting with Advanced Management Console 2.2, this is an optional step. Rename `${AMC_DIR}/conf/AMCUser.properties.template` to `${AMC_DIR}/conf/AMCUser.properties` and configure the three information values with the user's actual credentials.
6. Excute the `AMCAgent.sh` script from the terminal using the command:

   ```
   sudo bash ${AMC_DIR}/bin/AMCAgent.sh -install
   ```

7. Log in to Advanced Management Console web UI again. Go to the **Desktops** page and check that the desktop is now registered with the Advanced Management Console server. If the user's credentials were configured in step 5, then the desktop owner now appears as Owner in the Advanced Management Console UI.

As part of the installation, the script copies the agent binaries to `/usr/local/Oracle/Java_AMC` directory and starts the daemon. It also registers the native service by placing the registration file in `/etc/systemd/system/` or `/etc/init/` directories for `systemd` or `upstart` frameworks respectively.

# Installing Advanced Management Console Agent on macOS

You can use the `bin/AMCAgent.sh` script file to install and uninstall the Advanced Management Console agent on the macOS operating system. The Advanced Management Console agent is a launched daemon that you can start, stop, or restart by using the `launchctl` command.

To install the Advanced Management Console agent on the macOS operating system:

1. Configure the agent proxy and the agent intervals. See Configuring the Agent Proxy and the Agent Intervals.

   The agent proxy server is included in the bundle. If you change proxy server settings, you will need to download agent bundle again and distribute the updated bundle.
2. On the Advanced Management Console UI, click the **Configuration** tab and select **Agents Download**.

   > **Note:**
   >
   > When you select **Agents Download**, you might need to wait for the SHA256 values to finish computing. If the bundle isn't already generated, it takes a short time to build it. Once it's shown, the bundle is ready to download.

3. Click the link `agent-bundle-macosx.zip` and save the bundle.
4. Open the Finder, select the `.zip` file, right click to select **Open With** and then click **Archive Utility** to unzip all the files. You can also double click the `.zip` file to open the Archive Utility to unzip the files into the current folder.

   The script file doesn't have permissions to execute. Use the `chmod` command to manually set the execute permissions.

5. The files get extracted to `AMC_Agent` directory within the current folder. In the following steps, `${AMC_DIR}` represents the `AMC_Agent` directory where the Java Advance Management Agent files are extracted.
6. Starting with Advanced Management Console 2.2, this is an optional step. Rename `${AMC_DIR}/conf/AMCUser.properties.template` to `${AMC_DIR}/conf/AMCUser.properties` and configure the three information values with the user's actual credentials.
7. Execute the `AMCAgent.sh` script from the terminal using the command:

   ```
   sudo ${AMC_DIR}/bin/AMCAgent.sh -install
   ```

8. A dialog appears stating that the `AMCAgent` app is downloaded. Click **Open**.
9. Log in to Advanced Management Console web UI again. Go to the **Desktops** page and check that the desktop is now registered with the Advanced Management Console server. If the user's credentials were configured in step 6, then the desktop owner now appears as Owner in the Advanced Management Console UI.

After the installation, the script copies the agent binaries to `/Library/Application Support/Oracle/Java_AMC` directory, the `.plist` file to `/Library/LaunchDaemons/`, and starts the daemon.

# Advanced Management Console Agent Logging

The Advanced Management Console agent utilizes the Java logger to log information about tasks performed by the agent as well as any errors that are encountered.

The log files are available in the following directory:

- Windows: `%PROGRAMDATA%\Oracle\Java_AMC`
- macOS: `/Library/Application Support/Oracle/Java_AMC`
- Linux: `/usr/local/Oracle/Java_AMC/`

The logs are rotated according to a policy. Beginning with Advanced Management Console 2.7, the maximum size of the log files and the number of files are configurable through **AMCAgent.properties**. By default, the rotation uses three log files with a maximum size of 64K.  This means that when the first log file grows to a size of 64K, logs are directed to the second log file. When the third log becomes full, the log rotates back to the first file, overwriting any existing contents there. See Configuring the Agent Proxy and the Agent Intervals for procedures you can use to edit logging parameters.

# Unstalling Advanced Management Console Agent

This topic contains the following sections that describe how to uninstall Advanced Management Console Agent:

- Uninstalling the Advanced Management Console Agent on Windows
- Uninstalling the Advanced Management Console Agent on Linux
- Uninstalling the Advanced Management Console Agent on macOS
- Unregistering Desktops

# Uninstalling the Advanced Management Console Agent on Windows

On Windows, you can run the `remove` command to uninstall the Advanced Management Console agent and remove all Java Usage Tracker Properties files from the desktop.

To uninstall the Advanced Management Console agent:

1. Open the Windows Command Prompt with administrator privileges.
2. Run `%AMC_DIR%\bin\AMCAgent.exe -remove` to uninstall the agent.

   `%AMC_DIR%` is the directory where the Advanced Management Console agent is installed.
   The agent attempts to unregister itself on the Advanced Management Console server before uninstalling. After the agent is unregistered on the server, all Java Usage Tracker configuration files (`usagetracker.properties`) on the desktop are also removed.

   If the Advanced Management Console server is not reachable, this could cause the uninstallation to stall or fail. In this case, `%AMC_DIR%\bin\AMCAgent.exe -forceremove` can be used to force the agent to uninstall without unregistering first. However, `AMCAgent.exe -forceremove` does not perform the cleanup of `usagetracker.properties` files.

   Run the `AMCAgent.exe -forceremove` command in the following scenarios:

   - If `%AMC_DIR%\bin\AMCAgent.exe -remove` fails to uninstall agent service, then run the `%AMC_DIR%\bin\AMCAgent.exe -forceremove` command to force uninstall the agent.
   - If the agent was never successfully registered on the server, then execute `AMCAgent.exe -forceremove` command to uninstall the agent. The `AMCAgent.exe -remove` doesn't work in such a scenario.

> **Note:**
>
> See Unregistering Desktops to unregister the agent from the User Interface.

# Uninstalling the Advanced Management Console Agent on Linux

On Linux, you can run the `remove` command to uninstall the Advanced Management Console agent and remove all Java Usage Tracker Properties files from the desktop.

To uninstall the agent, open the Linux terminal and execute the command:

```
sudo bash ${AMC_DIR}/bin/AMCAgent.sh -remove
```

The agent attempts to unregister itself on the Advanced Management Console server before uninstalling. After the agent is unregistered on the server, all Java Usage Tracker configuration files (`usagetracker.properties`) on the desktop are also removed.

If the Advanced Management Console server is not reachable, this could cause the uninstallation to stall or fail. In this case, you can use the `sudo bash ${AMC_DIR}/bin/AMCAgent.sh -forceremove` command to force the agent to uninstall without unregistering first. However, `AMCAgent.exe -forceremove` does not perform the cleanup of `usagetracker.properties` files.

You need to run the `AMCAgent.sh -forceremove` command in the following scenarios:

- If using the `AMCAgent.sh -remove` command fails to uninstall the agent service, then run the `AMCAgent.sh -forceremove` command to force uninstall the agent.
- If the agent was never successfully registered on the server, then you need to execute `AMCAgent.sh -forceremove` command to uninstall the agent. The `AMCAgent.sh -remove` command doesn't work in such a scenario.

> **Note:**
>
> See Unregistering Desktops to unregister the agent from the User Interface.

After the agent is uninstalled, the script stops the daemon and deletes the service registration file based on the service management framework from either:

- `/etc/systemd/system/`
- `/etc/init/`

## Uninstalling the Advanced Management Console Agent on macOS

On macOS, you can run the `remove` command to uninstall the Advanced Management Console agent and remove all Java Usage Tracker Properties files from the desktop.

To uninstall the agent, open the terminal and execute the command:

```
sudo ${AMC_DIR}/bin/AMCAgent.sh -remove
```

The agent attempts to unregister itself on the Advanced Management Console server before uninstalling. After the agent is unregistered on the server, all Java Usage Tracker configuration files (`usagetracker.properties`) on the desktop are also removed.

If the Advanced Management Console server is not reachable, this could cause the uninstallation to stall or fail. In this case, you can use the `${AMC_DIR}/bin/AMCAgent.sh -forceremove` command to force the agent to uninstall without unregistering first. However, `AMCAgent.exe -forceremove` does not perform the cleanup of `usagetracker.properties` files.

You need to run the `AMCAgent.sh -forceremove` command in the following scenarios:

- If using the `${AMC_DIR}/bin/AMCAgent.sh -remove` command fails to uninstall the agent service, then run the `${AMC_DIR}/bin/AMCAgent.sh -forceremove` command to force uninstall the agent.
- If the agent was never successfully registered on the server, then you need to execute `AMCAgent.sh -forceremove` command to uninstall the agent. The `AMCAgent.sh -remove` command doesn't work in such a scenario.

> **Note:**
>
> See Unregistering Desktops to unregister the agent from the User Interface.

After the agent is uninstalled, the script stops the daemon and deletes the `.plist` file from the following directories:

- `/Library/LaunchDaemons/`
- `/Library/Application Support/Oracle/Java_AMC`

## Unregistering Desktops

You can use the Advanced Management Console to remove any desktops that cannot contact the Advanced Management Console server.

Follow these steps to remove the desktops that cannot contact the Advanced Management Console server:

1. In the Advanced Management Console UI, click the **Desktop** tab.
2. Ensure that the **Desktop** is selected in the **Display** drop-down list.

   The **Other Actions** button is available only with the **Desktop** display option.
3. Ensure that the **Table** icon is selected.
4. (Optional) Set the filter criteria to show only the desktops that you want to unregister.
   a. Click **Add Criteria**.
   b. Select the filters and set the values for each filter that you select.
5. In the **Desktop** table, select the check boxes adjacent to the desktops that you want to unregister.
6. Click **Other Actions** and then select **Unregister Desktop(s)** to display the **Unregister Desktop(s)** dialog.
7. Select the target desktops by selecting either of the following options:
   - **Selected Desktops**: Shows the number of desktops selected.
   - **All Filtered Desktops**: Shows the number of filtered desktops included.
8. Click **Confirm**.

   The selected desktops or all filtered desktops are unregistered.

The selected desktop(s) are unregistered on the server.

# Distributing Advanced Management Console Agent

In an enterprise environment, deploying Advanced Management Console agent requires installation and configuration of AMC agent on each client desktop. Distribution of the AMC agent bundle is not handled by the Advanced Management Console and has to be taken care separately.

Consider using a desktop as a host to stage the agent bundle. From this host, distribute and install the agent bundle on multiple client desktops.

Follow these steps to install the AMC agent in multiple client desktops:

1. Download the Advanced Management Console agent bundle from the AMC web UI to the host desktop. To download the agent bundle, select **Configuration** and then **Agent Download**.

   > **Note:**
   >
   > Ensure that you do **NOT** run the install command (for example, `%AMC_DIR%\bin\AMCAgent.exe -install`). By doing so, the host desktop will get registered as an agent with the AMC server.

2. For distribution of the downloaded agent bundle:
   a. To distribute the agent bundle to client desktops in your enterprise, use a Software Management System (such as Microsoft SCCM). The Software Management System that you choose must be capable of providing customized options to support secure Advanced Management Console agent distribution. This system must also handle the following operations using administrator privileges:
      i. Extraction of the agent bundle. Incorrect extraction may cause improper file permissions that prevent agent from starting.
      ii. Configuration of the bundle based on the client desktop owner's user credentials.
      iii. Installation of the agent using the install command. See Installing Advanced Management Console Agent.
   b. If the agent bundle is distributed to the client desktops through other means, ensure that extraction of bundle and installation steps are followed as described in Installing Advanced Management Console Agent.

After the agent is installed, each client desktop is registered with the Advanced Management Console server. The agent then periodically reports data, such as operating system family and version, and installed JREs to the Advanced Management Console server.

To view the client desktops that are registered with the Advanced Management Console server, log in to the Advanced Management Console web UI and click the **Desktops** tab.

8

# Java Usage Tracker Setup for Advanced Management Console

You can set up the Java Usage Tracker for the Advanced Management Console on Windows, macOS, and Linux operating systems. The Advanced Management Console agent automatically enables Usage Tracker on agent-managed Windows, macOS, and Linux desktops. On unsupported platforms, Java Usage Tracker can be manually configured. This topic contains the following sections describe the Java Usage Tracker configuration for the Advanced Management Console on Windows, macOS, and Linux operating systems:

- Setting Up Java Usage Tracker on Windows, macOS, and Linux Desktops
- Setting up Java Usage Tracker on Unsupported Agent Platforms

## Setting Up Java Usage Tracker on Windows, macOS, and Linux Desktops

The Advanced Management Console agent automatically configures Java Usage Tracker on agent-managed desktops on supported platforms.

See Software Prerequisites and System Requirements for Advanced Management Console Components for the list of supported platforms.

Starting from Advanced Management Console version 2.5, agents configure Java Usage Tracker to report records to Advanced Management Console agents instead of sending them directly to the Advanced Management Console server over the User Datagram Protocol (UDP). Agents then re-send the records to the Advanced Management Console server over `https`. The Java Usage Tracker ensures that every JRE located on the desktop sends its Java usage data to the Advanced Management Console server.

> **Note:**
>
> When Advanced Management Console is running in a cluster, the agent communicates with the load balancer and the UDP listener for the Java Usage Tracker records may not be supported.

## Setting up Java Usage Tracker on Unsupported Agent Platforms

The Advanced Management Console supports Linux distributions having `systemd` or `upstart` service management framework. For distributions not supported, the Java Usage Tracker can be configured manually.

1. Enter `https://`*`wls-hostname`*`:`*`port`*`/amcwebui` in the browser, where *`wls-hostname`* and *`port`* are the DNS name and listen port number of Oracle WebLogic Server.
2. Log in to the AMC UI using your administrator credentials.

3. Click the **Configuration** tab and then click the **Settings** sub tab.
4. Click **Download usagetracker.properties file** to download the file.
5. Enable Java Usage Tracker by copying this `usagetracker.properties` file to `{JRE_HOME}/lib/management` for each JRE installed on the desktop.

The downloaded `usagetracker.properties` file has the Java Usage Tracker parameters (port number, separators) required by the AMC. If you prefer to create the `usagetracker.properties` file yourself, then specify the parameters displayed in the AMC **Settings** tab.

> **Note:**
>
> The Advanced Management Console doesn't incorporate data from the `com.oracle.usagetracker.additionalProperties` setting of the `usagetracker.properties` file.

9

# Browser Setup for Advanced Management Console

You need to ensure the operating systems and browser version compatibility for the Advanced Management Console . You also need a browser set up and the AMC user interface for monitoring and administering the server.

The Browser Setup for the Advanced Management Console topic contains the following sections that describe compatibility and browser set up for the AMC:

- Advanced Management Console Browser Supported Versions
- Browser Setup for the Advanced Management Console User Interface (UI)

## Advanced Management Console Browser Supported Versions

The Advanced Management Console user interface is provided through a browser.

If you use Internet Explorer as your supported browser as listed in Software Prerequisites and System Requirements for Advanced Management Console Components, then ensure that **Display Intranet Sites in Compatibility View** is not selected in Compatibility View Settings.

## Browser Setup for the Advanced Management Console User Interface (UI)

The Advanced Management Console provides a web user interface (UI) to connect to the server.
See step 6 of Figure 2-1. The Advanced Management Console UI enables the user to monitor and administer the server.

Some commands in the Advanced Management Console start Java Web Start applications by using the JRE versions listed in Software Prerequisites and System Requirements for Advanced Management Console Components are needed to run these applications.

The commands in the **Installers** tab use Java Web Start applications, which also run on Windows operating systems.

10

# Advanced Management Console Migration

The migration of the Advanced Management Console to the latest available version involves redeploying the latest Enterprise Archive (EAR) file over the previous Advanced Management Console version within the WebLogic Server Administrator Console. The migration process is facilitated by an update wizard, where the Advanced Management Console server updates the database either manually or automatically. The Advanced Management Console agent is then updated to the latest version to be consistent with the redeployed Advanced Management Console server.

> **Note:**
>
> - Migration of higher version of Advanced Management Console to lower version is not supported.
> - As a best practice, always ensure to take a back up or a snapshot of the existing database before you continue with the upgrade process. If there is no back up, then you can't go back and try to upgrade subsequently, in case an error occurs at any point.

During the migration process, the Advanced Management Console server stops processing requests from the agent, processing Java Usage Tracker records, and updating security baseline records.

This topic contains the following sections that describe the Advanced Management Console server upgrade to the latest version, the Advanced Management Console database update, and the Advanced Management Console agent update:

- Uploading a New Version of Advanced Management Console Server
- Updating the Advanced Management Console Database
- Setting up Security Questions
- Updating the Advanced Management Console Agent

> **Note:**
>
> Ensure to always clear browser cache and cookies, after the Advanced Management Console is updated to a new version.

# Uploading a New Version of Advanced Management Console Server

The Advanced Management Console migration process begins with redeploying the latest Enterprise Archive (EAR) file over the previous Advanced Management Console version within the WebLogic Server administration console. You need WebLogic Server administrator credentials to perform this migration task.
To upload the Advanced Management Console over the previous version:

1. Enter `https://wls-hostname:/port/console` in a web browser, where *`wls-hostname`* and *`port`* are the DNS name and SSL listen port number of the Administration Server.
2. Authenticate using your administrator credentials.
3. Select the **Deployments** option from the **Domain Structure** panel.
4. In the right panel, select the check box for the Advanced Management Console application.
5. Click **Update**.
6. In the navigation panel, locate the EAR file for the latest version of the Advanced Management Console file and check it in. For example, the EAR file for the 2.20 version is `JavaAMC-2_20.ear`.
7. Click **Next**. Use the default values.
8. Click **Finish**.
9. Restart the WebLogic Server after Advanced Management Console is deployed.

# Updating the Advanced Management Console Database

After you have uploaded a new version of the Advanced Management Console EAR file, for example, `JavaAMC-2_20.ear` to WebLogic Server, the Advanced Management Console administrator must update the Advanced Management Console database.

> **Note:**
>
> You need not update the database if there are no changes to the database between the previous and the later AMC versions.

To update the database, load the `/amcwebui` and check whether or not the Advanced Management Console Database Update screen (update wizard) is displayed. If the screen is not displayed, then no changes are required, and the Advanced Management Console is fully operational. If the screen is displayed, then it guides you to perform database updates.

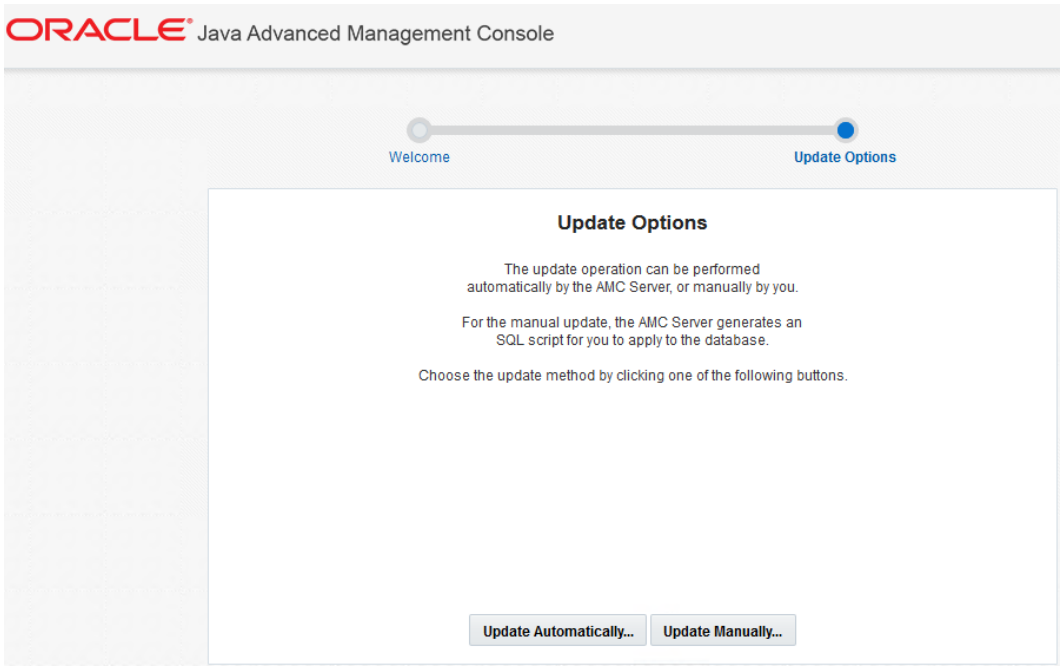
The database can be updated either manually or automatically using administrator credentials. If no database updates are required from the current AMC version to the latest one, then the update wizard is not displayed and you do not need to explicitly perform any task. Follow these topics to update the Advanced Management Console :

# Automatic Update of the Database

To do an automatic update of the Advanced Management Console database:

1. Enter `https://wls-hostname:port/console` in a web browser where *`wls-hostname`* and *`port`* are the DNS name and the SSL listen port the WebLogic server instance (the default port is 7002) to start the WebLogic Server Administration Console. A Welcome screen is displayed that indicates a database update.
2. Click **Next** on the Welcome screen to choose between automatic or manual database update as shown in Advanced Management Console Database Update — Welcome Screen.

**Figure 10-1 Advanced Management Console Database Update — Welcome Screen**




3. Click **Update Automatically** for the AMC server to update the database for you.
4. Click **Update** to complete the process. Or, click **Cancel** to cancel the automatic database update.

When the update is completed, a screen is displayed indicating that the AMC database is successfully updated.

# Manual Update of the Database

To do a manual update of the Advanced Management Console database:

1. Enter `https://wls-hostname:port/console` in a browser where *`wls-hostname`* and *`port`* are the DNS name and the SSL listen port the WebLogic server instance (the default port

is 7002) to start the WebLogic Server Administration Console. A Welcome screen is displayed that indicates a database update.

2. Click **Next** on the Welcome screen to select between an automatic or manual database update.
3. Click **Update Manually** to update the database using a SQL script.
4. Click the **SQL script** link to download the SQL script.

   The SQL script is saved as `amc_mysql_update.sql`. Connect to AMC database to apply it.
5. Click **Continue** after applying the SQL script on your database. Or, click **Cancel** to cancel the manual database update.

After the update is completed, a message is displayed to indicate that the AMC database is successfully updated.

# Setting up Security Questions

After setting up the database successfully, access Advanced Management Console . You will be prompted to set up the security questions. Select any three questions from the drop-down and provide your answers. You will then be redirected to the login page.

# Updating the Advanced Management Console Agent

After you update the database, update the Advanced Management Console agent to the latest release to be consistent with the redeployed Advanced Management Console server.

You can update the Advanced Management Console agent manually or automatically. However, Oracle recommends automatic updates.

- Manually Updating the Advanced Management Console Agent Version 2.0
- Manually Updating the Advanced Management Console Agent Version 2.1 and later
- Automatic Update of Advanced Management Console Agent

## Manually Updating the Advanced Management Console Agent Version 2.0

Learn more about how to manually update Advanced Management Console version 2.0 to be consistent with the Advanced Management Console server.

To manually update Advanced Management Console agent version 2.0:

1. Don’t remove the old agent. At the Windows command prompt, enter `sc stop "AMC Agent"` or `net stop "AMC Agent"` to stop the agent service.

   You need administrator privileges for this command to work.
2. Ensure that `%programData%\Oracle\Java_AMC_2` folder is preserved. The new agent picks the settings automatically from this folder.
3. Remove the contents of <*existing amc agent root directory*>. Download the latest agent bundle from the server after you have updated the server to the latest

release of the Advanced Management Console. Extract the `.zip` file for the new agent bundle to the same <*existing amc agent root directory*>.

4. At the Windows command prompt, enter `sc start "AMC Agent"` or `net start "AMC Agent"` to start the agent service again.

   You need administrator privileges for this command to work.

5. After you have started the new agent and verified that it works, you can remove `%programData%\Oracle\Java_AMC_2"`.

## Manually Updating the Advanced Management Console Agent Version 2.1 and later

Learn more about how to manually update Advanced Management Console agent version 2.1 and later to be consistent with the Advanced Management Console server.

To manually update Advanced Management Console agent version 2.1 and later:

1. Don't remove the old agent. At the Windows command prompt, enter `sc stop "AMC Agent"` or `net stop "AMC Agent"` to stop the agent service.

   You need administrator privileges for this command to work.

2. Backup `conf\AMCServer.properties` and `conf\AMCUser.properties` if these files exist.

3. Remove the contents of <*existing amc agent root directory*>. Download the latest agent bundle from the server after you have updated the server to the latest release of the Advanced Management Console. Extract the `.zip` file for the new agent bundle to the same <*existing amc agent root directory*>.

4. Restore the `conf\AMCServer.properties` and `conf\AMCUser.properties` files that you saved in step 2.

5. At the Windows command prompt, enter `sc start "AMC Agent"` or `net start "AMC Agent"` to start the agent service again.

   You need administrator privileges for this command to work.

## Automatic Update of Advanced Management Console Agent

Starting version 2.1, when you update the Advanced Management Console to a higher release, the agent automatically updates itself to that specific version.

When you upgrade the Advanced Management Console agent to version 2.17 or later, and **Agent Auto Update** is enabled, you need to validate the Keystore certificate. Follow these steps to accommodate the change in the signing certificates:

1. Download the `AMCSigning.jks` file from **Configuration**, **Agents Download** and then **AMC Signing Keystore** section.

2. Distribute this file to all the agent machines.

3. Stop the agent service manually.

4. Replace the `AMCSigning.jks` file in <*existing amc agent root directory*>`/conf` folder with the distributed file.

5. Start the agent service manually.

A

# Oracle WebLogic Server Installation Example

There are different ways of installing Oracle WebLogic Server. This topic contains an example to install Oracle WebLogic Server.

This topic contains the following sections that describe software requirements and WebLogic Server installation and configuration:



## Installing WebLogic Server

The Advanced Management Console requires Java SE Development Kit 8 Downloads, update 65 or later, and WebLogic Server supported versions 12c R2 or 14c. See Software Prerequisites and System Requirements for Advanced Management Console Components.

> **Note:**
>
> The version of WebLogic Server as mentioned in Installing the Oracle WebLogic Server in the *Oracle Fusion Middleware Installing and Configuring Oracle WebLogic Server and Coherence* guide may not be the default one. Ensure to download the correct version.

## Setting Up the Environment for WebLogic Server

The Advanced Management Console server initialization web page is not protected and can be accessed by any user.

> **Note:**
>
> This section is based on using Oracle WebLogic Server version 12c R2. Other versions may need different configurations.

To set up the required environment variables for WebLogic Server version 12c R2:

1. Define the environment variable, JAVA_HOME, and set it to JDK 8.

   For example, `C:\Java\jdk1.8.0_131`.

2. Run the command, `java -jar extracted_jar_file` from the Command Prompt (Admin).

   For example,

   ```
   java -jar fmw_12.2.1.3.0_wls_quick.jar
   ```

# Creating a WebLogic Server Domain

To create a WebLogic Server domain:

1. Define `JAVA_HOME`. See Setting Up the Environment for WebLogic Server.
2. For a Windows operating system, run the `config.cmd` file from the WebLogic Server installed directory, `%MW_HOME%\oracle_common\common\bin\config.cmd`.

   For a Linux operating system, run the `config.sh` file from the WebLogic Server installed directory, `%MW_HOME%/oracle_common/common/bin/config.sh`.
3. Ensure that **Create a New Domain** is selected, and then select the folder for the new domain. The default folder is `%MW_HOME%\user_projects\domains\base_domain`. The domain name is `base_domain`, which can be changed.
4. Click **Next**.
5. In the Templates step, select **Create Domain Using Product Templates**, and then select the Basic WebLogic Server Domain template. Click **Next**.
6. In the Administrator Account step, configure the administrative manager `admin` account. Click **Next**.
7. In the Domain Mode and JDK step, click the domain mode option as **Production** and specify the JDK if it is different from the bootstrap JDK. Click **Next**.
8. In the Advanced Configuration step, ***do not*** select any of the check boxes for **Administration Server**, **Node Manager**, and **Managed Servers, Clusters, and Coherence**. Click **Next**.
9. For all the **Views** in Deployment, Application, and Service screens, ***do not*** change the default folder options.
10. Click **Create** to create the domain.
11. When the Domain Created Successfully message is displayed, select **Next**.
12. In the Configuration Success step, click the check box for **Start Admin Server** to start the server. Click **Finish**.

In the AMC documentation, the directory `%MW_HOME%\user_projects\domains\domain1` represents `DOMAIN_HOME`.

# Starting a WebLogic Server Administration Server

To log in to the WebLogic Server administration server:

1. For a Windows operating system, start the administration server with `%DOMAIN_HOME%\startWebLogic.cmd`.

   For a Linux operating system, start the administration server with `%DOMAIN_HOME%/startWebLogic.sh`.

2. If the SSL port is configured for the WebLogic Sever Administration Server, then in the browser, go to the default URL *`https://localhost:7002/console`*. Otherwise, in the browser, go to the default URL *`http://localhost:7001/console`*.

3. Use your administrative credentials to log in to the server.

# Creating and Configuring a WebLogic Server Managed Server

Domains include a special Oracle WebLogic Server instance called the Administration Server, which is the central point from which you configure and manage all resources in the domain. Typically, you configure a domain to include additional Oracle WebLogic Server instances called Managed Servers.

Follow this example method to create a Managed Server for the WebLogic Server:

1. Define the environment variable, `JAVA_HOME`. See Setting Up the Environment for WebLogic Server.

2. For a Windows operating system, run `%DOMAIN_HOME%\bin\setDomainEnv.cmd`, which is required to set the environment.

   For a Linux operating system, run `%DOMAIN_HOME%/bin/setDomainEnv.sh`, which is required to set the environment.

3. For a Windows operating system, start the node manager with `%DOMAIN_HOME%\bin\startNodeManager.cmd`. If the node manager does not start, then edit `%DOMAIN_HOME%\nodemanager\nodemanager.properties` and set `NativeVersionEnabled=false`.

   For a Linux operating system, start the node manager with `%DOMAIN_HOME%/bin/startNodeManager.sh`. If the node manager does not start, then edit `%DOMAIN_HOME%/nodemanager/nodemanager.properties` and set `NativeVersionEnabled=false`.

4. Start the administrative server and log in to the server as described in Starting a WebLogic Server Administration Server.

5. From the **Domain Structure** block in the left panel, go to **Environment** and select **Machines**. Create a new machine. Enter any unique name in the **Name** field and then enter the host name (for example, `localhost`) and server listen port that matches the node manager settings. Click **Finish** to create the machine.

6. From the **Domain Structure** block in the left panel, go to **Environment** and select **Servers**. Create a new server. Enter any unique name in the **Name** field and then enter the host name and server listen port. Ensure that the new server listen port is different from the existing Administration Server listen port. Click **Finish** to create the server.

7. From the **Domain Structure** block in the left panel, go to **Environment** and select **Servers**. Click the server you created in step 6. In the **Configuration** tab associate this server to the new machine you created in step 5.

8. Click the **Control** tab and then click the check box for the associated server and machine. Then click **Start** to start the server.

9. In the browser, go to *https://hostname:port* and verify that the server is running. The Advanced Management Console uses HTTPS only for communication between the Advanced Management Console server and clients. See Trusted HTTPS Certificate.

# Configuring the Corporate LDAP Server

Groups in the corporate LDAP server are used to access AMC.

The following groups should be created in the corporate LDAP server:

- **cn=groups**
  - **cn=AMCAdminGroup**
  - **cn=AMCDRSGroup**
  - **cn=AMCJICGroup**
  - **cn=AMCReportsGroup**

Any user who needs access to AMC (with LDAP integration) should be assigned to at least one or all of the roles listed above. After this is completed, you may have to follow the instructions provided in Configuring LDAP Security Server in WebLogic Server to complete the LDAP integration process. See Using a WebLogic Deployment Plan for Customizing LDAP Group Names if you need to customize the name of the user groups that AMC will access for LDAP authentication.

# Using a WebLogic Deployment Plan for Customizing LDAP Group Names

You can create and use a WebLogic deployment plan if you intend to use descriptor values other than default settings during deployment. This enables you to customize the name of user groups that AMC has access to for LDAP.

To create and use a WebLogic deployment plan:

1. Set the required CLASSPATH by navigating to the `wlserver/server/bin` folder in your WebLogic installation and running the following script from the command line:

   > **Note:**
   >
   > The CLASSPATH is required to run the PlanGenerator application.

   ```
   setWLSEnv.cmd
   ```

2. Generate the deployment plan by navigating to the folder where your `amc.ear` application is located and running the following command:

   ```
   java weblogic.PlanGenerator -all amc.ear
   ```

> **Note:**
>
> You might get some unresolved references. That is alright. Just check for these lines at the end
>
> "Saving plan to *folder*\plan.xml.
>
> Saved configuration for application, amc.ear"

This generates the deployment plan based on the `amc.ear` file.

3. Customize the required parameters in the `plan.xml` file.
   a. Open the generated `plan.xml` file in a text editor.
   b. In the `<variable-definition>` section, search for the following variable names and replace each of the corresponding `<value xsi:nil="true"> </value>` for the variable name with the respective values configured in LDAP server.

> **Note:**
>
> The *XXXX* suffix below is a timestamp and can vary.

- `ApplicationSecurityRoleAssignment_admin_PrincipalNames_XXXXX`
- `ApplicationSecurityRoleAssignment_reports_PrincipalNames_XXXX`
- `ApplicationSecurityRoleAssignment_drs_PrincipalNames_XXXX`
- `ApplicationSecurityRoleAssignment_jic_PrincipalNames_XXXX`

For example, if your LDAP server group names are **app_AMCAdminGroup, app_AMCDRSGroup, app_AMCJICGroup, app_AMCReportsGroup** then after change they should look like this

```
<variable>
<name>ApplicationSecurityRoleAssignment_admin_PrincipalNames_XXXXX</
name>
<value>app_AMCAdminGroup</value>
</variable>

<variable>
<name>ApplicationSecurityRoleAssignment_drs_PrincipalNames_XXXXX</
name>
<value>app_AMCDRSGroup</value>
</variable>

<variable>
<name>ApplicationSecurityRoleAssignment_jic_PrincipalNames_XXXXX</
name>
<value>app_AMCJICGroup</value>
</variable>

<variable>
```

```
<name>ApplicationSecurityRoleAssignment_reports_PrincipalNames_XX
XXX</name>
<value>app_AMCReportsGroup</value>
</variable>
```

c. In the `<module-override>` section, search for the variable names listed in **step b** and add the line`<operation>replace</operation>`.

   For example, a section should look like this before adding the line:

```
<variable-assignment>

<name>ApplicationSecurityRoleAssignment_admin_PrincipalNames_XXXX
X</name>
    <xpath>/weblogic-application/security/security-role-
assignment/[role-name="admin"]/principal-name</xpath>
</variable-assignment>
```

   After adding the line`<operation>replace</operation>` , the section would look like this:

```
<variable-assignment>

<name>ApplicationSecurityRoleAssignment_admin_PrincipalNames_XXXX
X</name>
    <xpath>/weblogic-application/security/security-role-
assignment/[role-name="admin"]/principal-name</xpath>
    <operation>replace</operation>
</variable-assignment>
```

d. Repeat **step c** for the variable assignments in `_drs`, `_jic`, and `_reports`.

4. Deploy the customized plan.
   a. Open the WebLogic administration console.
   b. Under Domain Structure, click Deployments.
   c. Select the checkbox for the "JavaAMC" application, and click the Update button.
   d. Click the Change Path button associated with the Deployment plan path.
   e. Select the radio button for the new plan.xml file, and click Next.
   f. Select the radio button “Redeploy this application using the following deployment files” and then click Finish.

   Verify that the success message is displayed at the top of console. The message should be similar to:

```
All changes have been activated. No restarts are necessary.
Message icon - Success Selected Deployments were updated.
```

**Related Topics**

- https://www.oracle.com/webfolder/technetwork/tutorials/obe/fmw/wls/12c/09-DeployPlan--4464/deployplan.htm
- https://docs.oracle.com/cd/E24329_01/web.1211/e24443/

# Configuring LDAP Security Server in WebLogic Server

You can configure your Oracle WebLogic server to connect to Lightweight Directory Access Protocol (LDAP) server, so that the Advanced Management Console can communicate with the WebLogic Server, without having to connect to the LDAP

This topic contains sample instructions to configure the LDAP security provider in the WebLogic server, so that the WebLogic server gets connected to the LDAP server. The type of LDAP being configured in this example is OpenLDAP. This means OpenLDAP (external provider) server runs on localhost or on a remote server. If a different type of LDAP server is used, then there are chances of these instructions varying.
To configure WebLogic server to connect to the LDAP server:

1. Add a new security provider in the WebLogic server:
   a. Log in to WebLogic server admin console.
   b. Click **Domain**, and select **Security realms**, and then **myrealm**.
   c. Click **Providers** tab and then select **New**.
   d. Enter a name for the new provider, for example, LDAP.
   e. Set **Provider Type** to LDAPAuthenticator.
   f. Click **Save**.

      A Provider is created.
2. Configure the provider:
   a. Select the Provider that you just created.
   b. Click **Provider Specific** tab.
   c. Enter the following details in the following sections:

      Note that these are sample values only. You need to enter these values, based on the values configured on the LDAP server. Therefore, these values vary based on how the LDAP is set up.

   - **Connection** section:
     - **Host**: `localhost`
     - **Port**: <*portnumber*>
     - **Principal**: `cn=admin,dc=oracle,dc=com`
     - **Credential**: `welcome0`
   - **Users** section:
     - **User Base DN**: `cn=users,ou=amc,dc=oracle,dc=com`

       > **Note:**
       >
       > This value is based on the configuration of the LDAP server. You can set other values for the **User Base DN** field based on the LDAP server configuration.

     - **All Users Filter**: `(objectclass=person)`

  - **User Name Attribute**: `uid`
  - **User Object Class**: `person`
- **Groups** section:
  - **Group Base DB**: `cn=groups,ou=amc,dc=oracle,dc=com`

    > **Note:**
    >
    > This value is based on the configuration of the LDAP server. You can set other values for the **User Base DN** field based on the LDAP server configuration.

  - **All Groups Filter**: `(objectclass=groupOfNames)`
  - **Group From Name Filter**: `(&(cn=%g)(objectclass=groupOfNames))`
- **Static Groups** section:
  - **Static Group Name Attribute**: `cn`
  - **Static Group Object Class**: `groupOfNames`
  - **Static member DN attribute**: `member`
  - **Static Group DNs from Member DN Filter**: `(&(member=%M)(objectclass=groupOfNames))`

3. Click **Save**.
4. Restart the Admin server as well as all the managed servers.
5. Login to the Advanced Management Console UI, and click the **User** sub tab in the **Configuration** tab and ensure that the **Enable Container based authentication** checkbox is selected. By default, you aren't authenticated by the external LDAP server. If you want to enable the LDAP authenticatation, then you need to enable it by selecting the checkbox.

B

# Security Compliance for Advanced Management Console

The security recommendations help in improving the processes of installing, configuring, and deploying the Advanced Management Console server and its components.

All the security recommendations are applicable to Windows, macOS, and Linux operating systems. The following sections list the recommendations for each component of the AMC:

- Security Recommendations for Advanced Management Console Server
- Security Recommendations for Advanced Management Console WebLogic Server
- Security Recommendations for Advanced Management Console Agent
- Security Recommendations for Advanced Management Console Databases: MySQL or Oracle

## Security Recommendations for Advanced Management Console Server

Follow these security recommendations for the Advanced Management Console server installation, configuration, and deployment:

- **Protocol**: The AMC uses HTTPS for communication between the AMC server and clients (agent, web UI, Deployment Rule Set tool, and Java installer configuration).
- **Server deployment protection**: The AMC server deployment and initialization web page is not protected and does not require a password to set up. Therefore, the initialization page can be accessed by any user. Administrators should restrict access to the server or lock the server behind a firewall until initialization is complete.
- **Java Usage Tracker communication protection**: The Advanced Management Console should be run behind a firewall, which should be supported by the administrators. Administrators need to run the agent and server communication within the same intranet segment behind the firewall. The Advanced Management Console agents send Java Usage Tracker data to the server over https.

## Security Recommendations for Advanced Management Console WebLogic Server

Follow these security recommendations for the Advanced Management Console WebLogic Server installation, configuration, and deployment:

- **Java Security Manager**: Consider enabling the Java Security Manager in WebLogic Server to provide protection for resources running in a Java Virtual Machine (JVM) and to improve the AMC security. See Java Security Manager.

- **WebLogic Server Logs**: AMC leverages WebLogic Server logs to report all the security errors and warnings. Check the WebLogic Server domain logs for any reported errors.
- **Critical Patch Updates**: AMC requires that you keep your WebLogic Server instance up-to-date with security patches. We also recommend that you subscribe to receive Oracle's Critical Patch Update Advisories and Security Alerts notifications. See Instructions for subscribing to email notifications.

# Security Recommendations for Advanced Management Console Agent

Follow these security recommendations for the Advanced Management Console agent installation, configuration, and deployment:

- **Secure file permissions**: The AMC doesn't restrict the locations where system administrators can install the agents in a Windows environment. However, agents should be installed in a protected location, such as Program Files (x86), where regular users cannot make changes. In addition, system administrators should ensure that all installed files have secure permissions.
- **Agent logs**: Check the AMC agent service logs for reported logins, events, and errors located in the following Windows directory: `%PROGRAMDATA%\Oracle\Java_AMC\agent.log`. In a macOS environment, locate the agent logs here:`/Library/Application Support/Oracle/Java_AMC/agent.log.0`.

# Security Recommendations for Advanced Management Console Databases: MySQL or Oracle

Follow these security recommendations for Advanced Management Console installation, configuration, and deployment of Oracle database or MySQL database:

- **Secure database setup** : This installation guide does not provide details about secure database configuration and database security management.
- **User credentials**: The user credentials provided for MySQL or Oracle databases in the sections are examples. Oracle highly recommends that you use a different name and strong password for production use.

C

# Troubleshooting Tricks

This topic contains a few known issues in the Advanced Management Console and how to troubleshoot them.

This topic contains the following sections:



## Agent

Tips and Tricks to Ensure that the Advanced Management Console Agent Runs Efficiently:

1. Verify that the Advanced Management Console agent is running.
    a. From the Windows Control Panel, open **Services**, locate `AMC Agent` and verify whether it's running. If not, right click the **AMC Agent** and select **Start**.
2. Verify that the Advanced Management Console agent is communicating. Do the following to verify:
    a. Open `C:\ProgramData\Oracle\Java_AMC\agent.log.0`.
    b. Check the log file to validate that the agent does not have any communication errors to the server. For example:

```
2016-06-14 14:54:19 Communication: sending
com.oracle.amc.agent.client.GetCommandMessage@1c00735
2016-06-14 14:54:19 Communication: exception:
java.net.UnknownHostException: <amc-server-host>
16-06-14 14:54:19 com.oracle.amc.agent.task.GetCommandTask: got
communication error; rescheduling try #1
```

    c. Check the log file to validate that the Agent is posting Java Runtime Environment (JRE) installs to the server and that the server is delivering updates to the Agent (for example, (DRS)). To initiate the agent to communicate with the server, right click the **AMC Agent** in the **Services** dialog box of the Windows Control Panel, and select **Restart**.

> **Note:**
>
> Starting Advanced Management Console 2.7, the updated Native Launcher has changed the number of times the agent restarts as well as the delay between each retries. For example, if you retry 3 times, reset on the 4th time, and wait for an hour, then it goes back to the 3 retries again. The interval between the 3 retries is 30 seconds. However, agents that have been updated from an older release version of Advanced Management Console don't reflect this behavior.

3. Verify that the desktop hosting the agent shows up in the **Desktops** tab of the Advanced Management Console .
4. Verify that Advanced Management Console Server has pushed a Deployment Rule Set (DRS). Do the following to let the Advanced Management Console update `DeploymentRuleSet.jar`.
   a. Check the status of DRS pushing command to the desktop in the **Status** tab of the Advanced Management Console .
   b. Check the agent log in `C:\ProgramData\Oracle\Java_AMC\agent.log.0` for messages relating to DRS upload.
   c. From the Java Control Panel, open the Security Tab, and click **View the Active Deployment Rule Set** to ensure that the most current version of the rules are shown.
   d. If the rules are not updated, then check `C:\Windows\Sun\Java\Deployment` to locate a `DeploymentRuleSet.tmp` file. If you see `DeploymentRuleSet.tmp` in this location, then ensure that all applets and Java Web Start applications are terminated. Restart the **AMC Agent** service from the **Services** dialog box of the Windows Control Panel.

      Once the agent is restarted, ensure that the `DeploymentRuleSet.tmp` file is no longer available and the `DeploymentRuleSet.jar` is updated to the latest version.
5. Verify DRS processing:
   a. Set the deployment logging properties in the `<USER_DIR>\AppData\LocalLow\Sun\Deployment\deployment.properties` as follows:

      ```
      deployment.trace=true
      deployment.trace.level=ALL
      ```

   b. Check the log files in `<USER_DIR>\AppData\LocalLow\Sun\Deployment\log`. (Verify both `plugin*` and `javaws*` trace files.) Usually, there are two paired trace files produced for an application. One is the log message for the Main plugin Java Version and the other is the trace file for the Java Version defined from the Deployment Rule.
   c. Locate the word ruleset in the log file to debug the ruleset processing and find all the ruleset logging.

i. Verify that the Deployment Rule can be read by the plugin. If there is a certificate error, then ensure that the `deployment.properties` file is available in the following location: `C:\Windows\Sun\Java\Deployment`. Also, ensure that the `deployment.properties` contains the following property: `deployment.user.security.trusted.cacerts=C:\\Windows\\Sun\ \Java\Deployment\\drscacerts`. The Advanced Management Console agent should automatically update this file.

ii. If only one trace file is produced and you expected more, there is an issue with the browser bits compared to the Java versions installed. For example, the browser is a 32 bit, but only a 64 bit Java is installed. Look for the word Exception in the log file.

6. Verify Internet Explorer (IE) and Java Bits: IE 11 32 bit and 64 bit is the same application in Windows. To swap between 32 bit and 64 bit, in the **Advanced Options** tab of the Internet Options dialog box, select the **Enable Enhanced Protection Mode*** for 64 bit, and ensure that the check box is not selected for 32 bit.

   In Internet Options of IE 11, you can set it as follows:

   a. Go to the Control Panel and open the Action Center. Click **Change User Account Control Settings** and verify that the slider is not set to **Never notify**. If User Account Control is set to **Never notify**, then the Enhanced Protected Mode can't be enabled.

   b. In the **Security** tab of Internet Options, verify that the **Enable Protected Mode** check box is selected.

   c. In the **Advanced** tab of Internet Options, verify that **Enable Enhanced Protection Mode*** is enabled.

7. Reinstall the agent: When you want to re-install Advanced Management Console agent, either keep its `\conf` folder intact or run `AMCAgent -remove`. This also saves you from hitting the agent registration limit from the same IP address.

# Server

Tips and Tricks to Ensure that the Advanced Management Console Server Runs Efficiently:

1. You may encounter error messages, such as `404`, `HTTP_NOT_FOUND` while initializing the AMC:

   - If you get error messages, such as, `Connection refused` or `Cannot connect to the server` while trying to load `/amcwebui` in the browsers, then the WebLogic server where AMC is deployed to is either not started, or is unreachable.
   - If you get a warning message indicating that the page or the server is not trusted by the host, then it means that an unknown SSL certificate is used by the WebLogic Server.
   - If an HTTP Page Not Found (404) error is displayed, then it means that one of the following can be the issue:
     - WebLogic Server is started, but Advanced Management Console is not installed.
     - WebLogic Server is started and Advanced Management Console is installed (deployed), but the Advanced Management Console is not targeted to the correct managed server.
   - If the Advanced Management Console server has been already initialized, but loading `/amcwebui` still shows the initialization wizard, then there may be a broken database connection. Verify that you can connect to the database from the Advanced

Management Console server and that the data source is configured correctly (check whether or not the user credentials are valid), and then restart the Advanced Management Console or the Managed Server, where the Advanced Management Console is deployed to.

- If the WebLogic Server is started and the Advanced Management Console is installed, but the dependencies, such as the Data Source or JAX-RS 2.0 library are not deployed to the managed servers, then `/amcwebui` fails to be loaded and an HTTP Page Not Found (404) error is displayed.
- If you deploy the Advanced Management Console on an unsupported version of the Oracle WebLogic server, then the page gets redirected to the initialization page when loading `/amcwebui` and a `Datasource Cannot be Found` error message gets displayed when you continue to initialize the Advanced Management Console manually.

2. Ensure the following: agent desktops should get registered with the Advanced Management Console and also the Java Usage Tracker records should get registered with the Advanced Management Console . If not, check the WebLogic Server log in the following location: `<WebLogicHome>\user_projects\domains\base_domain\servers\AMCServer\logs\AMCServer.log`.
3. If you have an Out of Memory (OOM) exception, then you need to increase the Java Heap Space. By default the WebLogic Server uses 512 m. Set this to at least 4 GB. Set `USER_MEM_ARGS=-Xmx4g` before you invoke `setDomainEnv.cmd`.
4. Certificate issues can occur if system proxy is not defined. To define proxy servers:
   a. If connection to Internet requires proxy server, then set the following properties: `http.proxyHost`, `http.proxyPort`, `http.nonProxyHosts`, `https.proxyHost`, `https.proxyPort`. See Setting Up Java Heap Size and Proxy Servers.
5. At times, there is a very slow network connection to the server and some Advanced Management Console threads can be marked as Stuck by the Oracle WebLogic Server. For example, if you download an agent bundle from the Advanced Management Console UI, it can take more than 10 minutes. It can take a long time, if agents download JREs to install as well.
   - As a workaround to this issue, you need to configure the WebLogic Server to use a greater timeout than (default) 600s, in case you see a lot of threads marked as Stuck. To configure the timeout, in the WebLogic Administration Console, go to the **Server**, expand **Configuration**, and then select **Overload**, and then update **Max Stuck Thread Time** to a greater value.

# Important Directory Locations in a Windows Environment

The following is a list of important directory locations:

- `C:\Windows\Sun\Java\Deployment\`: If you want to use self-signed certificates, then ensure that the following files are available in the `C:\Windows\Sun\Java\Deployment\` location:
  - `deployment.properties`:

The content of this file is as follows:

```
#Updated by AMC   #Fri Aug 19 08:15:55 EDT 2016
deployment.user.security.trusted.cacerts=C\:\\windows\\Sun\\Java\
\Deployment\\drscacerts
```

  - `drscacerts`: The Keystore pointed to in the `deployment.properties` file containing the self-signed certificate.
  - If you have a signing certificate from a certificate authority, then it's sufficient if you have the `DeploymentRuleSet.jar` file in your Windows directory, for example, `C:\Windows\Sun\Java\Deployment\DeploymentRuleSet.jar`.

- `C:\Users\user\AppData\LocalLow\Sun\Java\Deployment\`: The client log files and the `deployment.properties` file are located in this directory. You can capture additional information by adding the following properties to the `deployment.properties` file:

  ```
  deployment.trace=true
  deployment.trace.level=all
  ```

- `$JRE_HOME%\lib\management\usagetracker.properties`: To troubleshoot the Java Usage Tracker, add the following in the `usagetracker.properties` file:

  ```
  com.oracle.usagetracker.logToFile = ${user.home}/.java_usagetracker
  com.oracle.usagetracker.verbose = true
  ```

  If you still find issues, then add the properties to `C:\Program Files\Java\conf`.

- `%ProgramData%\Oracle\Java_AMC\`: The Advanced Management Console log conversations with the Advanced Management Console server are available here. The content of the log file is as follows:

  ```
  %AMC_HOME%
  \Middleware\Oracle_Home\user_projects\domains\base_domain\servers\AdminSer
  ver\logs\{base_domain.log and AdminServer.log}
  %AMC_HOME%
  \Middleware\Oracle_Home\user_projects\domains\base_domain\servers\AMC-
  Server\logs\AMC-Server.log
  ```

# Important Directory Locations in a macOS Environment

The following is a list of important directory locations:

- `/Library/Application Support/Oracle/Java`: The Desktop-wide Java settings, such as the Java Usage Tracker configuration file (`usagetracker.properties`) are stored here. The Deployment rule set is in `Deployment/<sub-folder>`.
- `/Library/Application Support/Oracle/Java_AMC`: This is the Advanced Management Console agent folder that also contains log files apart from other folders.
- `~/Library/Application Support/Oracle/Java/Deployment`: This is the user-specific-deployment home directory. Settings from the Java Control Panel are stored for each user in this folder.

- `/Library/Internet Plug-Ins/JavaAppletPlugin.plugin`: This folder contains the system-wide JREs that are used to run Java applets in browsers. In a macOS environment, typically, there maybe just one JRE installed.

# Important Directory Locations in Linux Environment

The following is a list of important directory locations:

- `/usr/local/Oracle/Java_AMC`: The Advanced Management Console agent is installed into this folder. The agent logs are also located in this folder.
- `/etc/.java/deployment directory`: The install location for signed `DeploymentRuleSet.jar`.
- `/etc/oracle/java/`: Centralized location where the Java Usage Tracker configuration file (`usagetracker.properties`) is placed by AMC.
- `/usr/java, /usr/lib/jvm`: Default paths for locating Java installations depending on the Linux variant.

D

# Installing Advanced Management Console in a Clustered Environment — An Example

This section describes an example to install the Advanced Management Console on a Linux platform. You can deploy the Advanced Management Console in a WebLogic cluster environment to improve the performance. Multiple Managed servers running on different hosts, which are managed by the WebLogic cluster can work together to serve all requests in a round-robin mode.

This appendix contains the following:



The following is an overview of the process followed when installing the Advanced Management Console in a clustered environment:

1. Ensure that all machines are available.
2. Ensure that you can login with shell access and you have root credentials.
3. Install setup on the first server, for example SRV1.
4. Install setup on the 2nd server, for example, SRV2.
5. Install setup on the database server (SRVDB).
6. Deploy the Advanced Management Console application. You need to have the WebLogic Admin server running on SRV1 to access console and Node managers running on SRV1 and SRV2.
7. Install the Advanced Management Console agents using SCCM or manual steps.

## Installing and Configuring WebLogic Server

You need to install the WebLogic server on each host on which, the target managed server is running. A domain needs to be created on the first host.

To install the Advanced Management Console in a WebLogic cluster, you need at least 4 machines – 2 of which are required for setting up the WebLogic servers and one machine for setting up the database. The load balancer is shared across multiple setups.

To install WebLogic server and create a domain:

1. See Installing WebLogic Server.
2. Create and configure a WebLogic server domain.

# Configuring Machines and Server (SRV1) on a WebLogic Server Console

To configure the WebLogic server, you need to configure the required machines and servers on the WebLogic server console.

This topic mainly details how to create first machine in the cluster (SRV1). To configure machines and servers on a WebLogic server console:

1. Edit the nodemanager properties to start the Node manager on DNS name instead of localhost. In this guide, `${MW_HOME}` represents the WebLogic Server home directory.

   ```
   [deployment@SRV1 nodemanager]$ pwd
   ${MW_HOME}/user_project/domains/base_domain/nodemanager
   [deployment@SRV1 nodemanager]$ vi nodemanager.properties
   Set ListenAddress=SRV1.yourdomain.com
   ```

2. Start the WebLogic console:

   ```
   [deployment@SRV1 bin]$ pwd
   ${MW_HOME}/user_projects/domains/base_domain/bin
   [deployment@SRV1 bin]$ nohup ./startWebLogic.sh &
   [1] 7820
   [deployment@SRV1 bin]$
   ```

3. Start the Node Manager:

   ```
   [deployment@SRV1 bin]$ pwd
   ${MW_HOME}/bin
   [deployment@SRV1 bin]$ nohup ./startNodeManager.sh &
   [2] 7991
   [deployment@SRV1 bin]$
   ```

4. Login to the WebLogic console with the WebLogic administration user: `http://SRV1.yourdomain.com:7001/console/login/LoginForm.jsp`.
5. Click **Environment** and click **Machines** from the left panel.
6. Click **New** and enter SRV1 DNS name and select **Unix** from the drop-down list, and then click **Next**.
7. Enter `SRV1` DNS name and click **Finish**.
8. Similarly, repeat step 6 and 7 to create machine for SRV2.
9. Navigate to **Environment** and then click **Servers** from the left panel.
10. Click **New** and enter server details, with the listen address as DNS name and a port number. Make sure to select **Yes, create a new cluster....**, and then click **Next**.
11. Name new cluster, for example, `cluster-0` and click **Finish**.

12. Click the server name and associate this server with SRV1 and enable SSL and click **Save**.
13. Configure server for SRV2 following steps 9 through 12. Make sure to associate this server with existing cluster you created earlier.
14. Click on servers again and configure a heap size by navigating to **Server Start** from configuration page.
15. Click **Services** and then click **JTA** from the left panel.
16. Update the **Timeout Seconds** and then click **Save**. See Setting Up WebLogic Server JTA .

# Creating Domain Pack

To create a domain pack, in SRV1, update as follows:

```
[deployment@SRV1 Oracle_Home]$ java -version
java version "1.8.0_121"
Java(TM) SE Runtime Environment (build 1.8.0_121-b13)
Java HotSpot(TM) 64-Bit Server VM (build 25.121-b13, mixed mode)
[deployment@SRV1 ]$ export PATH=${MW_HOME}/oracle_common/common/bin:$PATH
[deployment@SRV1 ]$ export DOMAIN=${MW_HOME}
[deployment@SRV1 ]$ pack.sh -managed=true -domain=$DOMAIN -template=/tmp/
template.jar -template_name="/tmp/template_name"
<< read domain from ${MW_HOME}
  succeed: read domain from ${MW_HOME}
<< set config option Managed to "true"
  succeed: set config option Managed to "true"
<< write template to "/tmp/template.jar"
.............................
 >> succeed: write template to "/tmp/template.jar"
<< close template
  succeed: close template
[deployment@SRV1 base_domain]$
```

# Configuring a Second Machine in Cluster (SRV2)

To configure a second machine:

1. Install the WebLogic server. See Installing WebLogic Server. Click **Cancel** when asked to create domain.
2. Check if the pack was created by using **Create Domain Pack**.
3. Copy the pack file from SRV1 to SRV2.

   ```
   [deployment@SRV2 base_domain]$ scp /tmp/template.jar
   deployment@SRV2:/tmp/.
   ```

4. Unpack the domain by ssh onto SRV2:

   ```
   [deployment@SRV2 Oracle_Home]$ java -version
   java version "1.8.0_121"
   Java(TM) SE Runtime Environment (build 1.8.0_121-b13)
   ```

```
Java HotSpot(TM) 64-Bit Server VM (build 25.121-b13, mixed mode)
[deployment@SRV2 Oracle_Home]$ export DOMAIN=${MW_HOME}
[deployment@SRV2 Oracle_Home]$ unpack.sh -domain=$DOMAIN -
template=/tmp/template.jar
<< read template from "/tmp/template.jar"
  succeed: read template from "/tmp/template.jar"
<< set config option DomainName to "base_domain"
  succeed: set config option DomainName to "base_domain"
  validateConfig "KeyStorePasswords"
  succeed: validateConfig "KeyStorePasswords"
<< write Domain to ${MW_HOME}
.................................................
<< close template
  succeed: close template
[deployment@SRV2 Oracle_Home]$
```

5. Start the Node Manager on SRV2:

```
[deployment@SRV2 bin]$ pwd
${MW_HOME}/bin
[deployment@SRV2 bin]$ nohup ./startManagedWebLogic.sh
second_server_name admin_url &
[1] 10632
[deployment@SRV2jb bin]$
```

> **Note:**
>
> You may have to set up a `boot.properties` file with the username and password for the *`admin_url`*.

# Configuring Load Balancer

A load balancer sits in front of the backend WebLogic servers. Any load balancer can be used. As the load balancer is a transfer station for each packet between the clients and the backend servers, it could be a single point bottleneck. Therefore a hardware load balancer is highly recommended.

# Deploying Java Advanced Management Console Application

To deploy the application:

1. Check if you have completed installation and configuration steps for SRV1 and SRV2.
2. Check if the WebLogic Server is started on SRV1. If not, then you need to start it.
3. Login to WebLogic console on SRV1.
4. Click **Deployments** from the left panel.
5. Click **Install** and Install `jax-rs-2.0.war` from WebLogic deployment libraries. Click **Next** and then **Next**.

6. In the Deployment targets page, select **All servers in the cluster** to deploy this library for all servers and then click **Next**.
7. Click **Next** and **Finish** on next screens to accept defaults.
8. To deploy the Advanced Management Console application, click **Deployments** from the left panel.
9. Click **Install** and select `JavaAMC` deployment package. Click **Next** and then **Next**.
10. In the Deployment Targets page, select **All servers in the cluster** to deploy this library for all servers and click **Next**.
11. Click **Next** and **Finish**.
12. Click **Deployments** from left panel to make sure deployment is done.

# Installing and Configuring Oracle Database

Before you begin to install and configure the Oracle database, make sure you can get root authority as the configuration requires root authority.

See Configuring Oracle Database on Linux.

# Configuring Data Source in WebLogic Server

To Configure Data Source in WebLogic server, see Configuring WebLogic Server with Oracle Database.

> **Note:**
>
> The data source needs to be deployed on the cluster instead of the single WebLogic server.
> Automatic Update of Advanced Management Console Agent