# ORACLE WEBLOGIC SERVER 12c
# SECURITY TECHNICAL IMPLEMENTATION GUIDE
# (STIG) OVERVIEW

## Version 2, Release 1

## 23 April 2021

## Developed by Oracle and DISA for the DoD

## Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

# TABLE OF CONTENTS

**Page**

# LIST OF TABLES

## LIST OF FIGURES

**Page**

# 1. INTRODUCTION

## 1.1 Executive Summary

The Oracle WebLogic Server 12c Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DoD) information systems.

This document is a requirement for all DoD-administered systems and all systems connected to DoD networks. These requirements are designed to assist Security Managers (SMs), Information System Security Manager (ISSMs), Information System Security Officer (ISSOs), and System Administrators (SAs) with configuring and maintaining security controls. This guidance supports DoD system design, development, implementation, certification, and accreditation efforts.

## 1.2 Authority

DoD Instruction (DoDI) 8500.01 requires that "all IT that receives, processes, stores, displays, or transmits DoD information will be […] configured […] consistent with applicable DoD cybersecurity policies, standards, and architectures" and tasks that Defense Information Systems Agency (DISA) "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DoDI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provide an environment that contributes to the security requirements of DoD systems, applicable NIST SP 800-53 cybersecurity controls need to be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

## 1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

**Table 1-1: Vulnerability Severity Category Code Definitions**

| | **DISA Category Code Guidelines** |
|---|---|
| CAT I | Any vulnerability, the exploitation of which will, **directly and immediately** result in loss of Confidentiality, Availability, or Integrity. |
| CAT II | Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity. |
| CAT III | Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity. |

## 1.4 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Cyber Exchange website at https://cyber.mil/. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DoD Certificates can obtain the STIG from https://public.cyber.mil/.

## 1.5 SRG Compliance Reporting

All technical NIST SP 800-53 requirements were considered while developing this STIG. Requirements that are applicable and configurable will be included in the final STIG. A report marked For Official Use Only (FOUO) will be available for those items that did not meet requirements. This report will be available to component Authorizing Official (AO) personnel for risk assessment purposes by request via email to: disa.stig_spt@mail.mil.

## 1.6 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DoD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

## 1.7 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configurations settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible Authorizing Official. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100% secure.

Security guidance is provided for the Department of Defense. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied both at the device hardening level as well as the architectural level due to the fact that some of the settings may not be able to be configured in environments outside the DoD architecture.

## 1.8 Product Approval Disclaimer

The existence of a STIG does not equate to DoD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DoD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with Cybersecurity controls/control enhancements which supports system Assessment and Authorization (A&A) under the DoD Risk Management Framework (RMF). DoD Authorizing Officials (AOs) may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect vendor's proprietary information.

AOs have the purview to determine product use/approval IAW DoD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (http://www.niap-ccevs.org/) IAW CNSSP #11
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (http://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DoD mandated standards
- DoD Unified Capabilities (UC) Approved Products List (APL) (http://www.disa.mil/network-services/ucco) IAW DoDI 8100.04

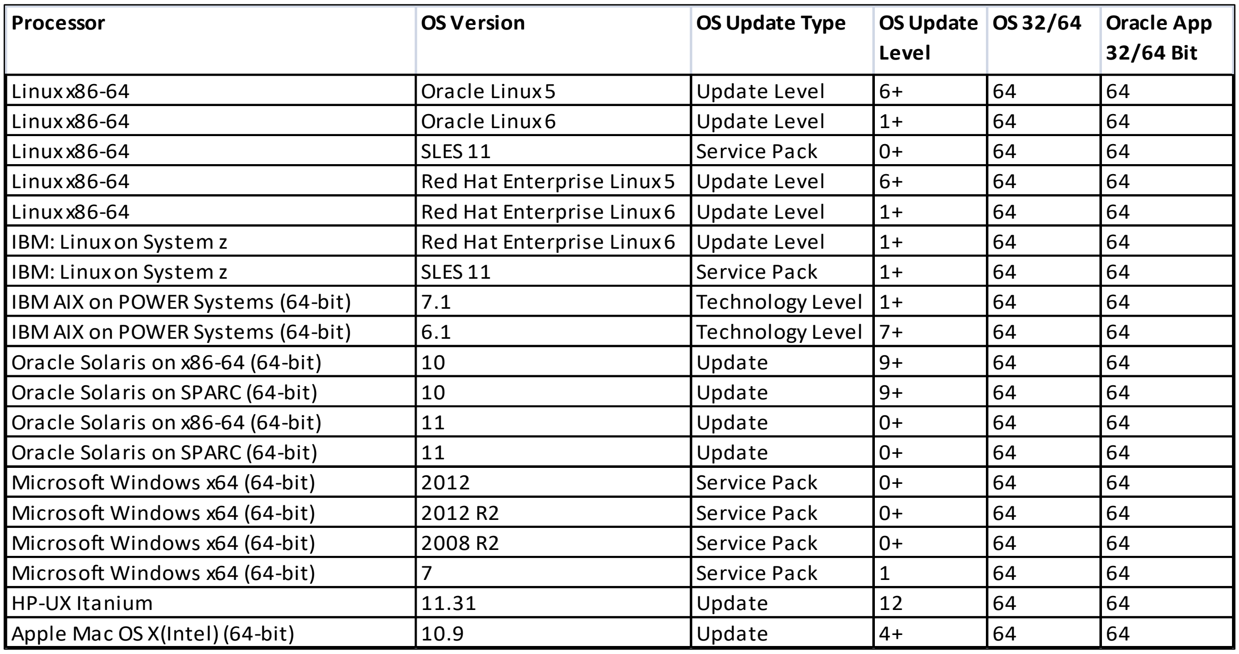
# 2. GENERAL SECURITY REQUIREMENTS

## 2.1 Oracle WebLogic Server 12c Installation Prerequisites

### 2.1.1 Verify Certification and System Requirements

Make sure that you are performing the installation of Oracle WebLogic Server 12c on a supported hardware or software configuration. Refer to the certification matrix below:

**Figure 2-1: Oracle WebLogic Server 12c Certification Matrix**



| Processor | OS Version | OS Update Type | OS Update Level | OS 32/64 | Oracle App 32/64 Bit |
|---|---|---|---|---|---|
| Linux x86-64 | Oracle Linux 5 | Update Level | 6+ | 64 | 64 |
| Linux x86-64 | Oracle Linux 6 | Update Level | 1+ | 64 | 64 |
| Linux x86-64 | SLES 11 | Service Pack | 0+ | 64 | 64 |
| Linux x86-64 | Red Hat Enterprise Linux 5 | Update Level | 6+ | 64 | 64 |
| Linux x86-64 | Red Hat Enterprise Linux 6 | Update Level | 1+ | 64 | 64 |
| IBM: Linux on System z | Red Hat Enterprise Linux 6 | Update Level | 1+ | 64 | 64 |
| IBM: Linux on System z | SLES 11 | Service Pack | 1+ | 64 | 64 |
| IBM AIX on POWER Systems (64-bit) | 7.1 | Technology Level | 1+ | 64 | 64 |
| IBM AIX on POWER Systems (64-bit) | 6.1 | Technology Level | 7+ | 64 | 64 |
| Oracle Solaris on x86-64 (64-bit) | 10 | Update | 9+ | 64 | 64 |
| Oracle Solaris on SPARC (64-bit) | 10 | Update | 9+ | 64 | 64 |
| Oracle Solaris on x86-64 (64-bit) | 11 | Update | 0+ | 64 | 64 |
| Oracle Solaris on SPARC (64-bit) | 11 | Update | 0+ | 64 | 64 |
| Microsoft Windows x64 (64-bit) | 2012 | Service Pack | 0+ | 64 | 64 |
| Microsoft Windows x64 (64-bit) | 2012 R2 | Service Pack | 0+ | 64 | 64 |
| Microsoft Windows x64 (64-bit) | 2008 R2 | Service Pack | 0+ | 64 | 64 |
| Microsoft Windows x64 (64-bit) | 7 | Service Pack | 1 | 64 | 64 |
| HP-UX Itanium | 11.31 | Update | 12 | 64 | 64 |
| Apple Mac OS X(Intel) (64-bit) | 10.9 | Update | 4+ | 64 | 64 |

### 2.1.2 Identify Proper Installation User

The user who installs Oracle WebLogic Server 12c owns the files and has the following permissions on the files:

- Read and write permissions on all non-executable files (for example, .jar, .properties, or .xml). All other users in the same group as the file owner have read permissions only.
- Read, write, and execute permissions on all executable files (for example, .exe, .sh, or .cmd). All other users in the same group as the file owner have read and execute permissions only.

Below are some additional considerations to make prior to running the installer:

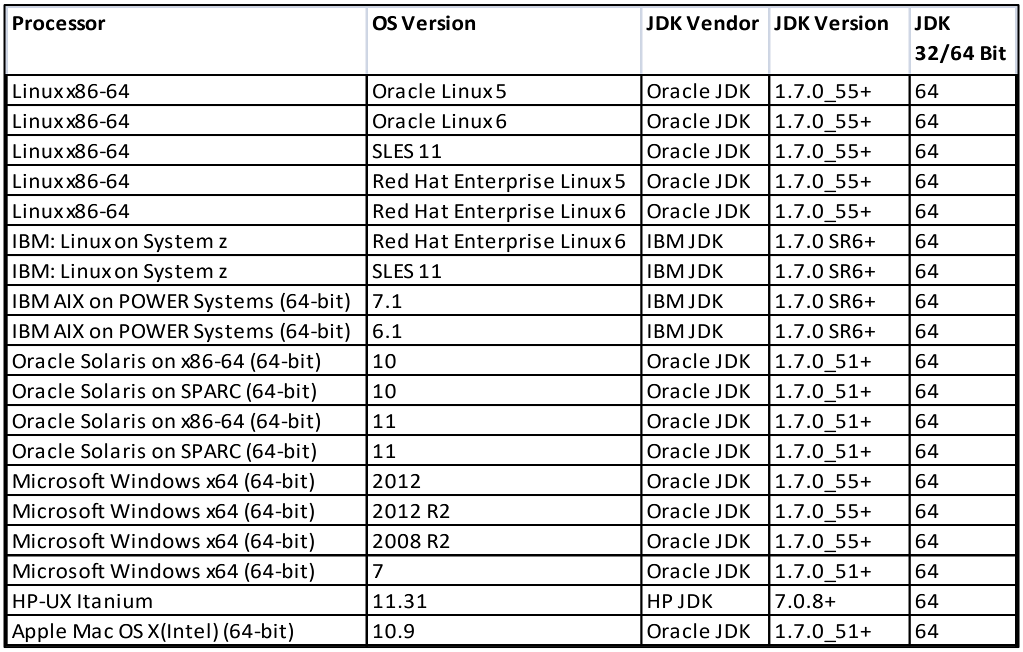
- On UNIX operating systems, Oracle recommends that you set the *umask* to *027* on your system prior to installation. This ensures that file permissions will be set properly during installation.

- You must enter the *umask* command in the same terminal window from which you plan to run the product installer.
- On UNIX operating systems, do not run the installation program as the root user. The installer startup validation will fail, and you will not be able to continue.
- When managing a product installation (for example, applying patches, or starting Managed Servers), you must use the same user ID as was used to perform the initial product installation.
- On Windows operating systems, the user performing the installation must have Administrator privileges.

### 2.1.3 Install Certified JDK

Oracle WebLogic Server 12c requires that a certified JDK is already installed on your system. Refer to the certification matrix below:

**Figure 2-2: JDK Certification Matrix**



| Processor | OS Version | JDK Vendor | JDK Version | JDK 32/64 Bit |
|---|---|---|---|---|
| Linux x86-64 | Oracle Linux 5 | Oracle JDK | 1.7.0_55+ | 64 |
| Linux x86-64 | Oracle Linux 6 | Oracle JDK | 1.7.0_55+ | 64 |
| Linux x86-64 | SLES 11 | Oracle JDK | 1.7.0_55+ | 64 |
| Linux x86-64 | Red Hat Enterprise Linux 5 | Oracle JDK | 1.7.0_55+ | 64 |
| Linux x86-64 | Red Hat Enterprise Linux 6 | Oracle JDK | 1.7.0_55+ | 64 |
| IBM: Linux on System z | Red Hat Enterprise Linux 6 | IBM JDK | 1.7.0 SR6+ | 64 |
| IBM: Linux on System z | SLES 11 | IBM JDK | 1.7.0 SR6+ | 64 |
| IBM AIX on POWER Systems (64-bit) | 7.1 | IBM JDK | 1.7.0 SR6+ | 64 |
| IBM AIX on POWER Systems (64-bit) | 6.1 | IBM JDK | 1.7.0 SR6+ | 64 |
| Oracle Solaris on x86-64 (64-bit) | 10 | Oracle JDK | 1.7.0_51+ | 64 |
| Oracle Solaris on SPARC (64-bit) | 10 | Oracle JDK | 1.7.0_51+ | 64 |
| Oracle Solaris on x86-64 (64-bit) | 11 | Oracle JDK | 1.7.0_51+ | 64 |
| Oracle Solaris on SPARC (64-bit) | 11 | Oracle JDK | 1.7.0_51+ | 64 |
| Microsoft Windows x64 (64-bit) | 2012 | Oracle JDK | 1.7.0_55+ | 64 |
| Microsoft Windows x64 (64-bit) | 2012 R2 | Oracle JDK | 1.7.0_55+ | 64 |
| Microsoft Windows x64 (64-bit) | 2008 R2 | Oracle JDK | 1.7.0_55+ | 64 |
| Microsoft Windows x64 (64-bit) | 7 | Oracle JDK | 1.7.0_51+ | 64 |
| HP-UX Itanium | 11.31 | HP JDK | 7.0.8+ | 64 |
| Apple Mac OS X (Intel) (64-bit) | 10.9 | Oracle JDK | 1.7.0_51+ | 64 |

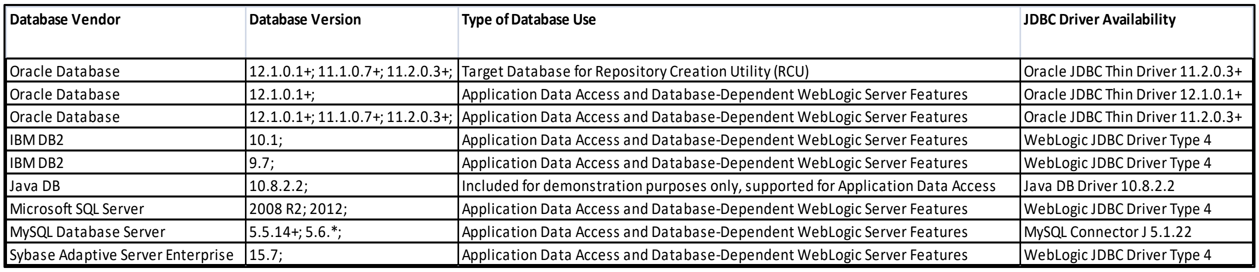
Oracle JDK is available for download from the following page on Oracle Technology Network:

```
http://www.oracle.com/technetwork/java/index.html
```

### 2.1.4 Install or gain access to certified database

Oracle WebLogic Server 12c requires the presence of certain database schemas prior to domain configuration. If you do not already have a database where you can install these schemas, you must install and configure a certified database. Refer to the certification matrix below:

Figure 2-3: Database Schema Certification Matrix



| Database Vendor | Database Version | Type of Database Use | JDBC Driver Availability |
|---|---|---|---|
| Oracle Database | 12.1.0.1+; 11.1.0.7+; 11.2.0.3+; | Target Database for Repository Creation Utility (RCU) | Oracle JDBC Thin Driver 11.2.0.3+ |
| Oracle Database | 12.1.0.1+; | Application Data Access and Database-Dependent WebLogic Server Features | Oracle JDBC Thin Driver 12.1.0.1+ |
| Oracle Database | 12.1.0.1+; 11.1.0.7+; 11.2.0.3+; | Application Data Access and Database-Dependent WebLogic Server Features | Oracle JDBC Thin Driver 11.2.0.3+ |
| IBM DB2 | 10.1; | Application Data Access and Database-Dependent WebLogic Server Features | WebLogic JDBC Driver Type 4 |
| IBM DB2 | 9.7; | Application Data Access and Database-Dependent WebLogic Server Features | WebLogic JDBC Driver Type 4 |
| Java DB | 10.8.2.2; | Included for demonstration purposes only, supported for Application Data Access | Java DB Driver 10.8.2.2 |
| Microsoft SQL Server | 2008 R2; 2012; | Application Data Access and Database-Dependent WebLogic Server Features | WebLogic JDBC Driver Type 4 |
| MySQL Database Server | 5.5.14+; 5.6.*; | Application Data Access and Database-Dependent WebLogic Server Features | MySQL Connector J 5.1.22 |
| Sybase Adaptive Server Enterprise | 15.7; | Application Data Access and Database-Dependent WebLogic Server Features | WebLogic JDBC Driver Type 4 |

### 2.1.5 Obtain the appropriate distribution

The Oracle Weblogic 12c STIG was developed on version 12.1.3.0.0. While the STIG may be able to be applied to other minor releases of 12c, STIG requirements checks and fixes have only been tested on version 12.1.3.0.0. Ensure software is acquired in accordance with applicable licensing guidelines. For development purposes, Oracle WebLogic Server 12.1.3 may be downloaded from the link below:

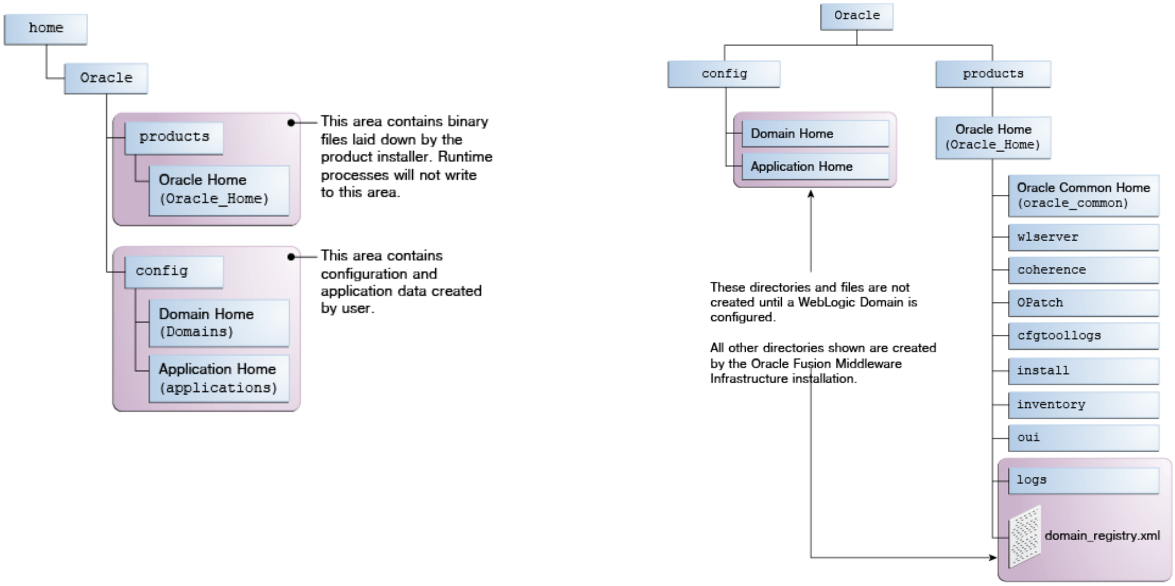
```
http://www.oracle.com/technetwork/developer-tools/adf/downloads/index.html
```

**Note**: When your browser asks if you want to download the file fmw_12.1.3.0.0_infrastructure_Disk1_1of1.zip, download this file onto your system. Extract the contents of this .zip file onto your system. One of the files extracted will be fmw_12.1.3.0.0_infrastructure.jar; this file will be used to run the product installer and install the software onto your system.

### 2.1.6 Determine installation directories

Oracle recommends a directory structure similar to the one shown here:

**Figure 2-4: Example of Recommended Directory Structure**


home
Oracle
products
Oracle Home
(Oracle_Home)
This area contains binary files laid down by the product installer. Runtime processes will not write to this area.
config
Domain Home
(Domains)
Application Home
(applications)
This area contains configuration and application data created by user.
Oracle
config
products
Domain Home
Application Home
Oracle Home
(Oracle_Home)
Oracle Common Home
(oracle_common)
wlserver
coherence
OPatch
cfgtoollogs
install
inventory
oui
logs
domain_registry.xml
These directories and files are not created until a WebLogic Domain is configured.
All other directories shown are created by the Oracle Fusion Middleware Infrastructure installation.

A base location (**Oracle base**) should be established on your system (for example, /home/Oracle) and from there, two separate branches should be created. The products directory should contain the product binary files and all of the Oracle home directories. The config directory should contain your domain and application data.

It is recommended that you do not keep your configuration data anywhere underneath the Oracle home; if you upgrade your product to another major release, you will be required to create a new Oracle home for binaries. You must also make sure that your configuration data exist in a location to which the binaries in the Oracle home have access.

The */home/Oracle/products* (for the Oracle home) and */home/Oracle/config* (for the application and configuration data) directories are referred to throughout the STIG remediation steps; be sure to replace these directories with the actual directories on your system.

The Oracle home directory is referenced as **ORACLE_HOME** in the STIG remediation steps.

The Domain home is the directory where the domains you configure will be created. The default Domain home location is *ORACLE_HOME/user_projects/domains/domain_name*; however, Oracle strongly recommends locating your Domain home outside of the Oracle home directory; if you upgrade your product to another major release, you will be required to create a new Oracle home for binaries.

The Domain home directory is referenced as **DOMAIN_HOME** in the STIG remediation steps and includes all folders up to and including the domain name. For example, if you named your domain *exampledomain* and you locate your domain data in the */home/Oracle/config/domains* directory, DOMAIN_HOME would be used in the documentation to refer to */home/Oracle/config/domains/exampledomain*.

The Application home is the directory where selected applications related to the domains you configure will be created. The default Application home location is *ORACLE_HOME/user_projects/applications/domain_name*; however, Oracle strongly recommends locating your Application home outside of the Oracle home directory; if you upgrade your product to another major release, you will be required to create a new Oracle home for binaries.

The Application home directory is referenced as **APPLICATION_HOME** in the STIG remediation steps and includes all folders up to and including the domain name. For example, if you named your domain *exampledomain* and you locate your application data in the */home/Oracle/config/applications* directory, APPLICATION_HOME would be used in the documentation to refer to */home/Oracle/config/applications/exampledomain*.

## 2.2 Oracle WebLogic Server 12c Software Installation

### 2.2.1 WebLogic Server 12c Installation

To start the installation program, perform the following steps:

1. Log into the target system.
2. Navigate to the directory where the installation program has been downloaded.
3. Launch the installation program by invoking java -jar from the JDK directory on your system, as shown in the examples below:

   On UNIX operating systems:

   ```
   /home/Oracle/jdk7_15/jdk1.7.0_55/bin/java -jar fmw_12.1.3.0.0_infrastructure.jar
   ```

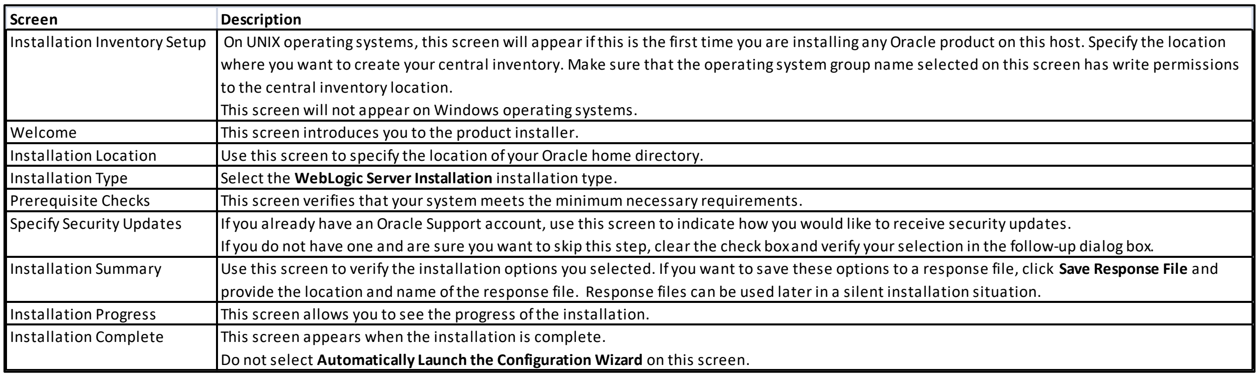
   On Windows operating systems:

   ```
   C:\Program Files\Java\jdk1.7.0_55\bin\java -jar fmw_12.1.3.0.0_infrastructure.jar
   ```

   Replace JDK location in these examples with the actual JDK location on your system.

4. When the installation program appears, you are ready to begin the installation. The installation program displays a series of screens, in the order listed below:

**Figure 2-5: Installation Screens**



| Screen | Description |
|---|---|
| Installation Inventory Setup | On UNIX operating systems, this screen will appear if this is the first time you are installing any Oracle product on this host. Specify the location where you want to create your central inventory. Make sure that the operating system group name selected on this screen has write permissions to the central inventory location.<br>This screen will not appear on Windows operating systems. |
| Welcome | This screen introduces you to the product installer. |
| Installation Location | Use this screen to specify the location of your Oracle home directory. |
| Installation Type | Select the **WebLogic Server Installation** installation type. |
| Prerequisite Checks | This screen verifies that your system meets the minimum necessary requirements. |
| Specify Security Updates | If you already have an Oracle Support account, use this screen to indicate how you would like to receive security updates.<br>If you do not have one and are sure you want to skip this step, clear the check box and verify your selection in the follow-up dialog box. |
| Installation Summary | Use this screen to verify the installation options you selected. If you want to save these options to a response file, click **Save Response File** and provide the location and name of the response file. Response files can be used later in a silent installation situation. |
| Installation Progress | This screen allows you to see the progress of the installation. |
| Installation Complete | This screen appears when the installation is complete.<br>Do not select **Automatically Launch the Configuration Wizard** on this screen. |

### 2.2.2 Database Schema Creation

The following schemas must be installed on a certified database for use with Oracle WebLogic Server 12c:

- Metadata Services (MDS)
- Audit Services (IAU)
- Audit Services Append (IAU_APPEND)
- Audit Services Viewer (IAU_VIEWER)
- Oracle Platform Security Services (OPSS)
- WebLogic Services (WLS)
- Service Table (STB)

This can be done using the Repository Creation Utility (RCU). Perform the following steps:

1. Obtain SYS or SYSDBA privileges and valid authentication credentials for database access.
2. Log in to the target system.
3. Navigate to the *ORACLE_HOME/oracle_common/bin* directory.
4. Start RCU:

   On UNIX operating systems:

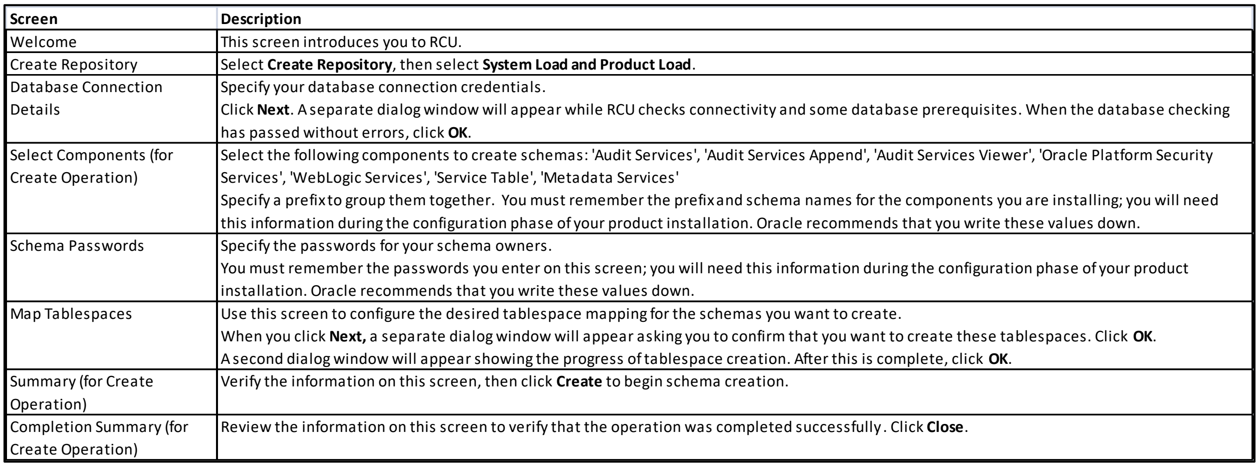
   ```
   ./rcu.sh
   ```

   On Microsoft Windows operating systems:

   ```
   rcu.bat
   ```

5. When the RCU configuration program appears, you are ready to begin. The configuration program displays a series of screens, in the order listed below:

**Figure 2-6: Database Schema Configuration Screens**



| Screen | Description |
|---|---|
| Welcome | This screen introduces you to RCU. |
| Create Repository | Select **Create Repository**, then select **System Load and Product Load**. |
| Database Connection Details | Specify your database connection credentials.<br>Click **Next**. A separate dialog window will appear while RCU checks connectivity and some database prerequisites. When the database checking has passed without errors, click **OK**. |
| Select Components (for Create Operation) | Select the following components to create schemas: 'Audit Services', 'Audit Services Append', 'Audit Services Viewer', 'Oracle Platform Security Services', 'WebLogic Services', 'Service Table', 'Metadata Services'<br>Specify a prefix to group them together.  You must remember the prefix and schema names for the components you are installing; you will need this information during the configuration phase of your product installation. Oracle recommends that you write these values down. |
| Schema Passwords | Specify the passwords for your schema owners.<br>You must remember the passwords you enter on this screen; you will need this information during the configuration phase of your product installation. Oracle recommends that you write these values down. |
| Map Tablespaces | Use this screen to configure the desired tablespace mapping for the schemas you want to create.<br>When you click **Next,** a separate dialog window will appear asking you to confirm that you want to create these tablespaces. Click **OK**.<br>A second dialog window will appear showing the progress of tablespace creation. After this is complete, click **OK**. |
| Summary (for Create Operation) | Verify the information on this screen, then click **Create** to begin schema creation. |
| Completion Summary (for Create Operation) | Review the information on this screen to verify that the operation was completed successfully. Click **Close**. |

**Note**: The **IAU_*** schemas created in this step will store the Security Audit records.

### 2.2.3 WebLogic Domain Creation

To begin domain configuration, perform the following steps:

1. Log in to the target system.
2. Navigate to the *ORACLE_HOME/oracle_common/common/bin* directory.
3. Start WebLogic Server Configuration Wizard:

   On UNIX operating systems:

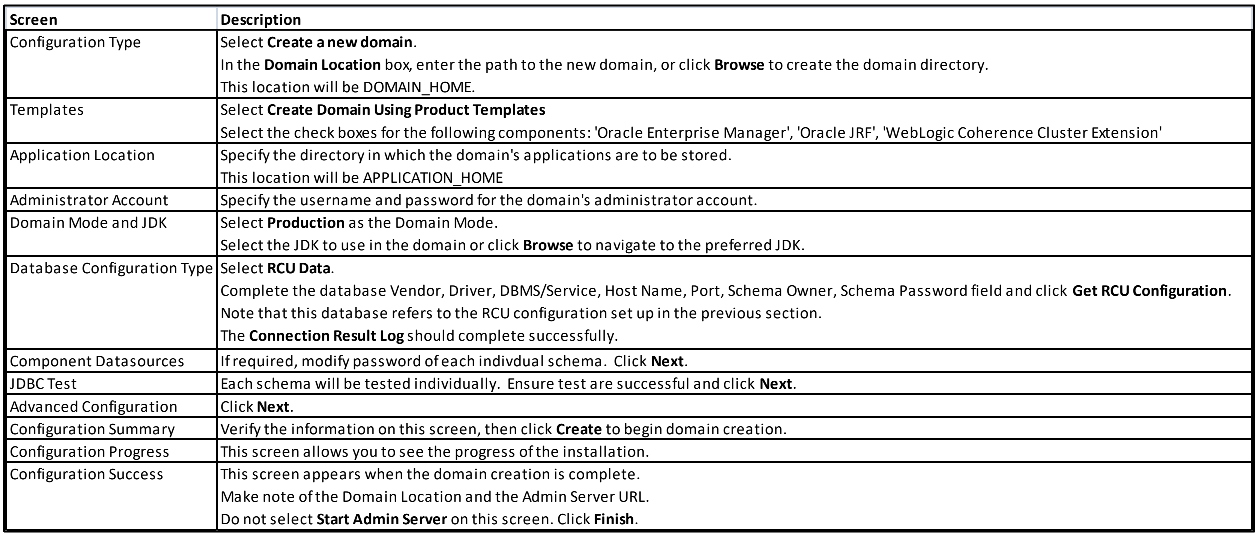
   ```
   ./config.sh
   ```

   On Microsoft Windows operating systems:

   ```
   config.cmd
   ```

4. When the Domain Configuration program appears, you are ready to begin. The configuration program displays a series of screens, in the order listed below:

### Figure 2-7: Domain Configuration Screens



| Screen | Description |
|---|---|
| Configuration Type | Select **Create a new domain**.<br>In the **Domain Location** box, enter the path to the new domain, or click **Browse** to create the domain directory.<br>This location will be DOMAIN_HOME. |
| Templates | Select **Create Domain Using Product Templates**<br>Select the check boxes for the following components: 'Oracle Enterprise Manager', 'Oracle JRF', 'WebLogic Coherence Cluster Extension' |
| Application Location | Specify the directory in which the domain's applications are to be stored.<br>This location will be APPLICATION_HOME |
| Administrator Account | Specify the username and password for the domain's administrator account. |
| Domain Mode and JDK | Select **Production** as the Domain Mode.<br>Select the JDK to use in the domain or click **Browse** to navigate to the preferred JDK. |
| Database Configuration Type | Select **RCU Data**.<br>Complete the database Vendor, Driver, DBMS/Service, Host Name, Port, Schema Owner, Schema Password field and click **Get RCU Configuration**.<br>Note that this database refers to the RCU configuration set up in the previous section.<br>The **Connection Result Log** should complete successfully. |
| Component Datasources | If required, modify password of each indivdual schema. Click **Next**. |
| JDBC Test | Each schema will be tested individually. Ensure test are successful and click **Next**. |
| Advanced Configuration | Click **Next**. |
| Configuration Summary | Verify the information on this screen, then click **Create** to begin domain creation. |
| Configuration Progress | This screen allows you to see the progress of the installation. |
| Configuration Success | This screen appears when the domain creation is complete.<br>Make note of the Domain Location and the Admin Server URL.<br>Do not select **Start Admin Server** on this screen. Click **Finish**. |

### 2.2.4 Enable FIPS 140-2 Mode

The system must be enabled for FIPS 140-2 compliance. Perform the following steps:

1. Download and install the **Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files** that correspond to the version of JDK installed in section **3.1.3**, from here:

   ```
   http://www.oracle.com/technetwork/java/javase/downloads/index.html
   ```

   Open the .ZIP distribution and update **local_policy.jar** and **US_export_policy.jar** in the *JAVA_HOME/jre/lib/security* directory. See the **README.txt** file in the .ZIP distribution for more information and installation instructions.

2. Create a new *java.security* file. The one that comes with the installed JDK can be used as a guide. Add both the **RSA JCE** provider and the **RSA JSSE** provider as the first two Java security providers listed in your *java.security* properties file, as shown:

   ```
   #
   security.provider.1=com.rsa.jsafe.provider.JsafeJCE
   security.provider.2=com.rsa.jsse.JsseProvider

   security.provider.3=sun.security.provider.Sun
   :
   ```

3. Navigate to the *DOMAIN_HOME* directory and make the following modifications to the appropriate WebLogic Server start script. Be sure to change **mylocation** to the actual path of the *java.security* file created in step 2 above.

   On UNIX operating systems:

```
startWebLogic.sh
```

Add the following lines beneath the **DOMAIN_HOME=** line, as shown:

```
DOMAIN_HOME=” ... “

JAVA_OPTIONS=” -Djava.security.properties==/mylocation/java.security ${JAVA_OPTIONS}”

PRE_CLASSPATH=”%MW_HOME%\wlserver\server\lib\jcmFIPS.jar;%MW_HOME%\wlserver\server\lib\ss
lj.jar ${PRE_CLASSPATH}”
```

On Microsoft Windows operating systems:

```
startWebLogic.cmd
```

Add the following lines beneath the **set DOMAIN_HOME=** line, as shown:

```
set DOMAIN_HOME= ...

set JAVA_OPTIONS= -Djava.security.properties==C:\mylocation\java.security %JAVA_OPTIONS%

set PRE_CLASSPATH=
%MW_HOME%\wlserver\server\lib\jcmFIPS.jar;%MW_HOME%\wlserver\server\lib\sslj.jar;%PRE_CLA
SSPATH%
```

## 2.3 Oracle WebLogic Server 12c Startup

### 2.3.1 Starting up Admin Server

To start up Oracle WebLogic Server 12c for the newly created domain, first the Admin Server must be started. Perform the following steps:

1. Log in to the target system.
2. Navigate to the *DOMAIN_HOME* directory.
3. Start Admin Server using the provided scripts:

   On UNIX operating systems:

   ```
   ./startWebLogic.sh
   ```

   On Microsoft Windows operating systems:

   ```
   startWebLogic.cmd
   ```

4. Enter username and password for the Administrator account, which was specified in the previous section.
5. A terminal window will be started up. Wait for the following message to print in the terminal window:

```
<The server started in RUNNING mode.>
```

### 2.3.2 Accessing Administrative Interfaces

Oracle WebLogic Server 12c provides two management and administrative interfaces. While some functionality overlaps, each interface will be referenced within the STIG remediation steps, and can be described as follows:

- WebLogic Admin Console (**AC**) – Used to configure the domain constructs and elements within it, such as server ports and channels, clustering topology, PKI resources, data sources, diagnostic monitors and system auditing. AC may be accessed via browser using the following URL:

```
http://<hostname>:<admin-server-port>/console
```

- Enterprise Manager FMW Control (**EM**) – Used to administer security aspects of the domain, such as users/roles, security auditing, metadata services and integration with Oracle Fusion Middleware components installed within the domain. EM may be accessed via browser using the following URL:

```
http://<hostname>:<admin-server-port>/em
```

**Note**: After installation of WebLogic, the interfaces are accessed via http, but during the STIG process, the interfaces are configured to use https and cannot be accessed via http.

The username and password for each of these interfaces will match the Administrator Account set during the **WebLogic Domain Creation** section above.

### 2.3.3 Using Change Center during configuration

Oracle WebLogic Server 12c allows administrative users to make configuration changes within the administrative interface using the Change Center. The Change Center provides a way to lock a domain configuration so changes may be made to the configuration while preventing other accounts from making changes during the edit session. The Change Center will be referenced within the STIG remediation steps. To change a production domain's configuration, perform the following steps:

1. Locate the Change Center in the upper left of the Administration Console (AC) or Enterprise Manager (EM) screens.
2. Click the **Lock & Edit** button to lock the configuration edit hierarchy for the domain.
3. Make the changes desired on the relevant page of the administrative interface. Click **Save** (or in some cases **Finish**) on each page where changes are made.
4. When finished making all the desired changes, click **Activate Changes** in the Change Center.

As changes are made using the administrative interfaces, clicking **Save** (or in some cases **Finish**) does not cause the changes to take effect immediately. The changes take effect when the **Activate Changes** button in the Change Center is clicked. At that point, the configuration changes are distributed to each of the servers in the domain. If the changes are acceptable to each of the servers, then they take effect. If any server cannot accept a change, then all of the changes are rolled back from all of the servers in the domain. The changes are left in a pending state; at that point pending changes can either be edited to resolve the problem or reverted.

Any pending (saved, but not yet activated) changes may be reverted by clicking **Undo All Changes** in the Change Center. Any individual changes may be reverted by going to the appropriate page in the administrative interface and restoring the attribute to its previous value.