Guidance Supplement for Oracle® Weblogic Server 12.1.3

December 2016
Version 1.3

Security Evaluations
Oracle Corporation
500 Oracle Parkway
Redwood Shores, CA 94065

Guidance Supplement for Oracle Weblogic Server 12.1.3

Version 1.3

Author: Oracle Corporation

Table of Contents

CHAPTER

1 Introduction

The Target of Evaluation (TOE) is the Oracle Weblogic Server 12.1.3. The TOE is a complete implementation of the Java EE 6 specification which provides a standard set of APIs for creating distributed Java applications that can access a wide variety of services, such as databases, messaging services, and connections to external enterprise systems.

1.1 Purpose

This document provides guidance on the secure installation and secure use of the TOE for the Common Criteria (CC) Evaluation Assurance Level EAL2+ evaluated configuration. This document provides clarifications and changes to the Oracle documentation and should be used as the guiding document for the installation and administration of the TOE in the CC evaluated configuration. The official Oracle documentation should be referred to and followed only as directed within this guiding document. Oracle documentation is available for download at https://docs.oracle.com.

Table 1 below lists the guidance documents relevant to the use of the TOE. Table 2 lists other documents relevant to the installation of the TOE.

Table 1 TOE Guidance Documents

Document Name	Description
Understanding Oracle WebLogic Server 12.1.3 E41937-04, August 2015	This document provides an overview of Oracle WebLogic Server 12.1.3 features and describes how you can use them to create enterprise-ready solutions.
Understanding Oracle Fusion Middleware Concepts E48202-01, May 2014	An overview of Oracle Fusion Middleware architecture and its key concepts. It also includes an introduction to Oracle Fusion Middleware components and tools.
Understanding Security for Oracle WebLogic Server, E42028-02, August 2015	This document introduces and explains the underlying concepts of the Oracle WebLogic Security Service.
WebLogic Server Administration Console Online Help E41845-03	Part of the TOE WebLogic Server Administration Console.
Developing and Securing RESTful Web Services for Oracle WebLogic Server, E47709-02, August 2015	Documentation for software developers that describes how to develop Java EE web services that conform to the Representational State Transfer (REST) architectural style using Java API for RESTful Web Services (JAX-RS).

Document Name	Description
Developing Applications with the WebLogic Security Service, E42029-04, August 2015	This document explains how to use the Oracle WebLogic Server security programming features.
Securing Resources Using Roles and Policies for Oracle WebLogic Server, E41904-02, August 2015	Documentation for security architects and administrators that describes how to use security roles and policies to determine who can access resources in a domain.
Securing WebLogic Web Services for Oracle WebLogic Server, E42030-02, August 2015	Documentation for security software developers that describes how to secure WebLogic web services for Oracle WebLogic Server, including configuring transport- and message-level security.
Developing Resource Adapters for Oracle WebLogic Server, E41877-02, August 2015	Documentation for resource adapter users, deployers, and software developers that describes how to develop applications that include Java EE resource adapters to be deployed to WebLogic Server.
Command Reference for Oracle WebLogic Server, E42026-03, August 2015	This document describes Oracle WebLogic Server command-line reference features and Java utilities and how to use them to administer Oracle WebLogic Server.
Administering Server Environments for Oracle WebLogic Server E41942-07, August 2015	This document describes how to design, configure, and manage WebLogic Server environments. It is a resource for system administrators and operators responsible for implementing a WebLogic Server installation.
Deploying Applications to Oracle WebLogic Server, E41940-03, August 2015	This document describes deploying Java EE applications or application modules to WebLogic Server instances or clusters.
Understanding Domain Configuration for Oracle WebLogic Server E41943-04, August 2015	This document describes Oracle WebLogic Server domains and how they are configured
Developing Enterprise JavaBeans for Oracle WebLogic Server E47839-05, August 2015	This document is a resource for software developers who develop applications that include WebLogic Server Enterprise JavaBeans (EJBs) using the Java Platform, Enterprise Edition 6.
Developing Enterprise JavaBeans, Version 2.1, for Oracle WebLogic Server E47840-04, August 2015	This document is a resource for software developers who develop applications that include WebLogic Server Enterprise JavaBeans (EJBs), Version 2.1 or earlier, using the Java Platform, Enterprise Edition 6 or earlier.
Administering Server Startup and Shutdown for Oracle WebLogic Server E41938-05, May 2016	This book describes how you manage Oracle WebLogic Server startup, shutdown, and server life cycle. It also describes WebLogic features that you help prevent and recover from server failure.
Developing Web Applications, Servlets, and JSPs for Oracle WebLogic Server E41936-07, August 2015	This document is a resource for software developers who develop Web applications and components such as HTTP servlets and JavaServer Pages (JSPs) for deployment on WebLogic Server.

Document Name	Description
WLST Command Reference for WebLogic Server E35669-03, February 2016	This document describes all of the commands that are available to use with the WebLogic Scripting Tool (WLST). This document includes only WLST commands for WebLogic Server.
Developing JAX-WS Web Services for Oracle WebLogic Server E47706-04, August 2015	Documentation for software developers that describes how to develop Java EE web services using the Java API for XML-based Web services (JAX-WS).
Developing JAX-RPC Web Services for Oracle WebLogic Server E47707-03, August 2015	Documentation for software developers that describes how to develop WebLogic web services using Java API for XML-based RPC (JAX-RPC).
The WebLogic Server® MBean Reference E41843-02	Online WebLogic Server MBean Reference
Administering Clusters for Oracle WebLogic Server 12.1.3 E41944-06, August 2015	This document describes clusters and provides information for planning, implementing, and supporting a production environment that includes clusters in WebLogic Server 12.1.3.
Creating WebLogic 12.1.3 Domains Using the Configuration Wizard E41890-02, August 2015	This document describes how to use the Configuration Wizard to create, update, and extend WebLogic Server 12.1.3 domains.
Administering JDBC Data Sources for Oracle WebLogic Server 12.1.3 E41864-09, May 2016	This book contains JDBC data source configuration and administration information for WebLogic Server 12.1.3.
Administering JMS Resources for Oracle WebLogic Server 12.1.3 E41859-04, August 2015	This document is a resource for WebLogic Server 12.1.3 system administrators who configure, manage, and monitor WebLogic JMS resources, including JMS servers, stand-alone destinations (queues and topics), distributed destinations, and connection factories.
Administering the JMS Resource Adapter for Oracle WebLogic Server 12.1.3 E41853-02, August 2015	This document describes how to configure and manage a JMS Resource Adapter hosted by a third-party application server to interoperate with WebLogic Server 12.1.3 using WebLogic JMS.
Monitoring Oracle WebLogic Server 12.1.3 with SNMP 12c (12.1.3) E41906-02, August 2015	Documentation for administrators that describes the SNMP capabilities of Oracle WebLogic Server 12.1.3.

Table 2 Installation Documents

Document Name	Description
Administering Security for Oracle WebLogic Server, E41905-08, April 2016	Documentation for application architects, developers, and security administrators that explains how to configure WebLogic Server security, including settings for security realms, providers, identity and trust, single sign-on, and SSL.
Installing and Configuring Oracle WebLogic Server and Coherence, E48355-02. July 2014	Documentation for installers and system administrators that describes how to install and configure Oracle WebLogic Server and Coherence
Securing a Production Environment for Oracle WebLogic Server, E41900-06, March 2016	This document describes how to secure an Oracle WebLogic Server production environment
Planning an Installation of Oracle Fusion Middleware E48353-01, May 2014	Documentation for installers and system administrators that describes how to plan and prepare your system for installing and configuring an Oracle Fusion Middleware product.
Installing Software with the Oracle Universal Installer E48351-01, May 2014	Documentation for installers and system administrators that describes how to use the Oracle Universal Installer for Oracle Fusion Middleware products.
Release Notes for Oracle WebLogic Server E41931-13, April 2016	This document describes all known issues for this release of Oracle WebLogic Server.
Administering Node Manager for Oracle WebLogic Server 12.1.3 E41941-05, May 2016	This document describes how to configure and use Node Manager to control and manage servers within a WebLogic Server 12.1.3 environment.

Along with the above-referenced documentation, additional supporting documentation for the TOE is available in the Oracle Weblogic Server 12.1.3 Books: https://docs.oracle.com/middleware/1213/wls/docs.htm.

1.2 Target Audience

The audience for this document consists of the end-user, the Oracle development staff, the CC Evaluation Laboratory staff, and the Government Certifier.

1.3 Evaluated TOE Configurations

The TOE comprises the following components:

- Oracle WebLogic Server version 12.1.3
- JDK Java Cryptographic Extension (JCE) provider (bundled with the corresponding JDK).
- JDK Java Secure Socket Extension (JSSE) provider (bundled with the corresponding JDK).
- RSA Java Cryptographic Extension (JCE) provider, included in RSA Crypto-J version 6.1.1
- RSA Java Secure Socket Extension (JSSE) provider, included in RSA SSL-J version 6.1.2

The TOE does not include the hardware, firmware, operating system or Java virtual machine used to run the software components.

The TOE can run in as a single WebLogic Server instance in a domain, or as a WebLogic Server instance in a set of distributed nodes that are part of the same domain. In this case, one TOE instance assumes the role of an Administration Server, and one or more instances assume the roles of a Managed Server or a cluster Managed Server.

The Operational Environment for the TOE allows the use of one of the following operating systems:

- Oracle Linux 6.7
- Oracle Solaris 11.3

The Operational Environment for the TOE allows the use of one of the following Java Runtime Environments:

- Oracle Java Development Kit (JDK) version 7 Update 101 or higher
- Oracle Java Development Kit (JDK) version 8 Update 91 or higher

The following LDAP servers are allowed for storing TSF data. These external servers are part of the operational environment and therefore not covered with security claims in this Security Target:

- Oracle Internet Directory
- Oracle Virtual Directory
- iPlanet
- Active Directory
- Open LDAP
- Novell LDAP

The following relational databases are allowed to be used with the TOE for both application data access and database-dependent features. These databases are part of the operational environment and therefore not covered with security claims in this Security Target:

- Oracle Database version 12.1.0.1+
- Oracle Database versions 11.1.0.7+ and 11.2.0.3+
- IBM DB2 10.1
- IBM DB2 9.7
- Microsoft SQL Server 2008 R2
- MySQL Database Server 5.5.14+ and 5.6.*
- Sybase Adaptive Server Enterprise 15.7

The TOE is intended to operate in a networked environment, either alone, or with other instances of the TOE, within the context of a single management "domain". Configuration and security policy for all TOE instances in a domain are managed by a single "administration server". Configuration and policy artifacts are automatically distributed by the administration server to each "managed server" in the domain.

Communication links between individual instances of the TOE can be protected against loss of confidentiality and integrity using separate physical networks or by cryptographic protection mechanisms supported by the TOE.

Data under the control of the TOE is stored in named objects, and the TOE can associate with each named object a description of the access rights to that object.

Instances of the TOE execute as Java processes running on one of the supported Java Virtual Machines and operating system. The TOE does not control or manage the JVM, the operating system or their security policies; instead it does depend for its security on the secure configuration and management of the underlying JVM and operating system.

1.4 Assumptions

The writers of this document assume the following:

- Those responsible for the administration of the TOE are competent and trustworthy individuals, capable of managing the TOE, the operational environment, and the security of the information it contains..
- Those responsible for the TOE must ensure that the operating system and the Java virtual machine are installed and configured in accordance with the guidance of the TOE and that these mechanisms operate as specified. This also covers that only the Java virtual machines enumerated in the Security Target are used as the underling platform to ensure that proper date and time information is available to the audit facility.
- Those responsible for the TOE must establish and implement procedures to ensure the software components that comprise the TOE are distributed, installed, configured and administered in a secure manner.
- Those responsible for the TOE must ensure that the TOE as well as the underlying hardware and software are protected from physical attack, which might compromise IT security objectives.
- Those responsible for the TOE shall ensure that the developers of the applications executed by the TOE are trustworthy and implement the applications in accordance with the guidance provided with the TOE.
- The real time clock of the underlying operating system shall provide reliable time stamps.
- Digital certificates, CRLs user for certificate validation and private and public keys must be generated externally and imported into the TOE. This material must meet the corresponding standards and provide sufficient strength, through the use of appropriate key lengths and message digest algorithms.
- External entities used to provide identity assertions to authenticate users must operate according to the specification and must be configured in the TOE to be trusted.
- External entities providing storage for TSF data in the operational environment like LDAP servers or database servers must be trusted, and must be protected against unauthorized physical access and modification. Communication between the TOE and those systems must be also protected from eavesdropping and modification.
- Communication between the TOE instances that constitute an application domain and between the TOE and external entities providing services to the TOE must be protected from eavesdropping and modification through physical or logical means. This objective complements the protection provided by O.SEC_CHANNEL.

CHAPTER

2 Installation Procedure

This section describes the installation procedure notes and changes.

2.1 Introduction

This section provides guidance for how to properly step through the installation instructions referenced in Table 2, along with additions to the instructions contained therein, in order to allow the installer to properly install the evaluated configuration of the TOE.

2.2 Secure Installation

Note: Throughout this section the reader will be instructed to read certain passages from referenced documents. Unless otherwise stated, such instructions refer to the documents listed in Table 1 and Table 2.

2.2.1 Phase 1 – Initial Preparation

Before the administrator begins the installation, he should make certain that he has all the necessary components as listed below.

Components Required for the TOE Installation Configuration

The following components are required for the TOE installation:

- Hardware platform with one of the operating systems installed listed in section 1.3.
- The TOE downloaded from the Oracle Software Delivery Cloud at https://edelivery.oracle.com. The right ISO image depending on the platform should be downloaded for installation.
    - Go to https://edelivery.oracle.com/ and register/sign in
    - In the product dropdown menu type and select "Oracle Weblogic Server 12.1.3.0.0"
    - In "Select Platform", select the appropriate platform for your environment, for example "Linux x86-64", and press the 'Select' button. Press the continue button on the main page.
    - Download "Oracle Fusion Middleware 12c (12.1.3.0.0) WebLogic Server and Coherence" (Part Number V44413-01, V44413-01.zip)

- The following Patch Set Update (PSU) must also be downloaded:
  - Go to the Master Note on Weblogic Server Patch Set Updates (PSUs) (Doc ID 1470197.1) (https://support.oracle.com/epmos/faces/DocContentDisplay?id=1470197.1)
  - Download 12.1.3.0.160719 Patch Set Update (PSU) for WebLogic Server 12.1.3.0 (Patch name p23094292_121300_Generic.zip).

Documents Required for the TOE Installation Configuration

The documents are listed in table 2 should be referred to.

The process to obtain the documentation is as follows:

1. Download the required guidance from the Oracle website, using the https links embedded within this document (which will provide a TLS v1.2 connection). Download the support note titled *Common Criteria Oracle WebLogic Server 12.1.3 Support Note* from support.oracle.com that contains SHA-256 hash sums for the TOE guidance documents not available via TLSv1.2 connections. *This document is provided via an SSL connection with the op*tion to verify Oracle's server certificates.

After downloading the Support Note, for those documents not downloaded via a TLS v.12 connection, verify this documents' checksums using a SHA-256 file hash tool. SHA-256 tools are available for any platform. This will generate a hexadecimal number that can be compared to the relevant SHA-256 checksum value in the Support note. If differences exist, the customer should contact Oracle Customer Support.

2.2.2 Phase 2 – Verification of the TOE

When the TOE is downloaded via Oracle's website, the Support Note described above additional includes SHA-256 hashes to verify the integrity of the data. The customer should download an appropriate SHA-256 Hash calculation tool and obtain values on the downloaded files. If the SHA-256 data in the Support Note matches the customer calculated SHA-256 result, this indicates that the data has not been altered. Should the TOE fail the SHA-256 hash procedure, the customer should download the TOE again and re-check the hash. If the failure persists, the customer should contact Oracle Customer Support.

2.2.3 Phase 3 – Installation

The evaluated configuration consists of the following Weblogic Server components:

- Weblogic Server 12.1.3.0.0
- Weblogic Server PSU 12.1.3.0.160719

The guidance and installation documents referenced in table 2 provide detailed instructions for installing the above functionality. In particular, Chapter 1.1.1 "Using the Standard Installation Topology as a Starting Point" in Installing and Configuring Oracle WebLogic Server and Coherence, should be referred to. The other scenarios provided in chapters 1.1.2 to 1.1.4 of the same document are not supported as methods of installing the evaluated configuration.

2.2.4 Phase 4 – Evaluated Configuration of the TOE

Once the TOE is properly installed as instructed above, the documents referenced in table 2 describes the actions required to bring it into the evaluated configuration. In addition, the guidance in Section 3 (Administrative Guidance) should also be applied.

2.2.5 Flaw Remediation

Oracle Weblogic Server customers or partners can receive information on flaw remediation through the secure My Oracle Support portal to report security vulnerabilities or other flaws in the TOE. Other individuals, i.e. independent researchers, should refer to How to Report Security Vulnerabilities to Oracle.

Refer to the below references for additional information on Oracle security practices and flaw handling procedures.

Importance of Software Security Assurance
Security Fixing Policies
Oracle Lifetime Support Policies

The Critical Patch Updates, Security Alerts and Third Party Bulletin provides the latest patch update information on all Oracle products, and is available as an RSS subscription.

Specifically for WebLogic Server, there is a Master Note on WebLogic Server Patch Set Updates(PSUs), which provides detailed information and download links for the latest patches.

CHAPTER

3 Administrative Guidance

This section provides additional guidance not found in the guides listed in Table 1 or Table 2. Any clarifications, exclusions, or additions are detailed here to allow the TOE Administrator to properly configure and maintain the evaluated configuration of the TOE. The TOE Administrator should have successfully completed the installation procedures listed in section 2 before applying the guidance found here.

You must apply the following deserialization blacklist setting, as a system property, when starting the server:

-Dweblogic.rmi.blacklist="+org.apache.commons.fileupload.disk.DiskFileItem"

This may be done in one of the following two ways:

i) Using a custom start script. Follow the instructions in section 4.8.2.3 of Administering Node Manager for Oracle WebLogic Server 12.1.3 to create a custom start script containing the following three lines:

```
#!/bin/sh
export JAVA_OPTIONS="${JAVA_OPTIONS} -Dweblogic.rmi.blacklist=+org.apache.commons.fileupload.disk.DiskFileItem"
startWebLogic.sh
```

ii) If using Node Manager to start/stop WebLogic Servers, the command line argument provided above can be set via console or WLST; see WebLogic Server Administration Console Online Help "Set Java options for servers started by Node Manager" for details.

CHAPTER

4 Acronyms

This section defines the acronyms.

Acronym	Definition
API	Application Programming Interface
CC	Common Criteria
CRL	Certificate Revocation List
EAL	Evaluation Assurance Level
IT	Information Technology
JCE	Java Cryptographic Extension
JDK	Java Development Kit
JRE	Java Runtime Engine
JSSE	Java Secure Socket Extension
JVM	Java Virtual Machine
LDAP	Lightweight Directory Access Protocol
PSU	Patch Set Update
RSA	Rivest, Shamir and Adleman
SHA	Secure Hash Algorithm
TOE	Target of Evaluation
TSF	TOE Security Functionality
WLS	WebLogic Server