

Oracle® Fusion Middleware

Securing a Production Environment for Oracle WebLogic Server



12c (12.2.1.3.0)

F32679-07

December 2023

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Copyright © 2007, 2023, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface

| | |
|--|----|
| Audience | v |
| Documentation Accessibility | v |
| Conventions | v |
| Related Information | v |
| New and Changed Features in This Release | vi |

1 Getting Started

| | |
|---|-----|
| Introduction | 1-1 |
| Critical Tasks for Locking Down WebLogic Server | 1-1 |

2 Understand and Secure Your Environment

| | |
|--|-----|
| Understand Your Environment | 2-1 |
| Hire Security Consultants or Use Diagnostic Software | 2-2 |
| Read Security Publications | 2-2 |
| Secure the Host Environment | 2-2 |
| Secure Your Database | 2-4 |

3 Lock Down WebLogic Server

| | |
|--|------|
| Install WebLogic Server in a Secure Manner | 3-1 |
| Apply the Latest Patches and Updates | 3-1 |
| Configure a Secure Domain | 3-3 |
| Configure Secured Production Mode | 3-3 |
| Understand How Domain Mode Affects the Default Security Configuration | 3-4 |
| Configure an Administration Port for the Domain | 3-9 |
| Disable Unused Internal Applications | 3-10 |
| Configure Additional Security Settings After Domain Creation | 3-12 |
| Set Permissions to Restrict Access to WebLogic Resources to One User Account | 3-17 |
| Do Not Include Unencrypted Passwords in Commands and Scripts | 3-18 |
| Secure WebLogic Resources | 3-19 |

| | |
|---|------|
| Review Potential Security Issues | 3-20 |
| Secure the Network | 3-24 |
| Configure Firewalls | 3-24 |
| Configure Network Channels and Firewalls to Prevent Access from Non-HTTPS Traffic | 3-25 |
| Configure Firewall to Prevent Access to Internal Applications | 3-27 |
| Configure Firewall for Cluster Communication | 3-32 |
| Configure Connection Filters | 3-32 |
| Configure Timeouts | 3-33 |
| Configure Sockets and File Descriptors | 3-34 |
| Configure SSL/TLS | 3-35 |
| An Important Note Regarding Null Cipher Use in SSL | 3-36 |
| Use JEP 290 to Restrict Incoming Serialized Java Objects | 3-37 |
| Setting the Deserialization Timeout Interval | 3-38 |
| Disable Remote Anonymous RMI T3 and IIOP Requests | 3-38 |
| Avoid Using These Configurations and Settings in a Locked Down Environment | 3-40 |
| Secure Applications | 3-46 |

Preface

This preface describes the document accessibility features and conventions used in this guide—*Securing a Production Environment for Oracle WebLogic Server*.

Audience

This document is intended for application architects, security architects, application developers and server administrators who design, implement, and test the security of their WebLogic Server configuration.

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>.

Accessible Access to Oracle Support

Oracle customers who 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.

Conventions

The following text conventions are used in this document:

| Convention | Meaning |
|-----------------|--|
| boldface | Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary. |
| <i>italic</i> | Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values. |
| monospace | Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter. |

Related Information

The following Oracle WebLogic Server documents contain information that is relevant to the WebLogic Security Service:

- *Administering Security for Oracle WebLogic Server* — explains how to configure security for WebLogic Server and how to use Compatibility security.

- *Developing Security Providers for Oracle WebLogic Server* — explains how vendors and application developers can develop custom security providers that can be used with WebLogic Server.
- *Understanding Security for Oracle WebLogic Server* — provides an overview of the features, architecture, and functionality of the WebLogic Security Service. It is the starting point for understanding the WebLogic Security Service.
- *Securing Resources Using Roles and Policies for Oracle WebLogic Server* — describes how to secure WebLogic resources. It primarily focuses on securing URL (Web) and Enterprise JavaBean (EJB) resources.
- [Java API Reference for Oracle WebLogic Server](#) — is reference documentation for the WebLogic security packages that are provided with and supported by this release of WebLogic Server.

New and Changed Features in This Release

For a comprehensive listing of the new WebLogic Server features introduced in this release, see *What's New in Oracle WebLogic Server 12.2.1.3.0*.

1

Getting Started

Learn about locking down your WebLogic Server production environment and see a list of the critical tasks that you need to perform to ensure that your system is secure.

Topics include:

- [Introduction](#)
- [Critical Tasks for Locking Down WebLogic Server](#)

Introduction

To ensure the security of your production environment, it is critical that you lockdown your system to prevent unauthorized access to your WebLogic Server resources and applications.

Lockdown refers to configuring your system to prevent unwanted intrusions. A comprehensive lockdown of a WebLogic Server production environment includes securing the host machine and database, ensuring that you install only the necessary WebLogic Server components, and limiting access only to authorized users. Lockdown also includes other configuration such as securing your domain using a domain-wide secure port for Administration Server communications, securing network resources using network channels and firewalls to limit access, and configuring the system to use SSL.

Oracle strongly recommends that you follow *all* of the guidelines provided in this document to protect your WebLogic Server environment.

Critical Tasks for Locking Down WebLogic Server

To ensure the security of your system, Oracle strongly recommends that you complete these critical tasks to lockdown your WebLogic Server system.

 **Note:**

Keep in mind that these are not the *only* tasks that you need to complete to lockdown your system. However, Oracle strongly recommends that these are the tasks that you must complete, but you should do them in combination with more general security guidelines described in [Understand and Secure Your Environment](#) and the other tasks described in [Lock Down WebLogic Server](#).

Table 1-1 Critical Tasks for Locking Down WebLogic Server

| Task | Description | More Information |
|---|---|--|
| Install WebLogic Server in a secure manner. | Performing a secure installation includes steps to secure the host machine on which WebLogic Server is installed, to limit access to that host to only authorized users, and to install only the components necessary to run WebLogic Server. | <ul style="list-style-type: none"> • Install WebLogic Server in a Secure Manner |
| Apply the latest WebLogic Server, Java, and database Critical Patch Updates on a quarterly basis. | To ensure that your system is protected against vulnerabilities, it is critical that you apply the latest Java, database, and WebLogic Server Critical Patch Updates (CPUs) as soon as they are released. | <ul style="list-style-type: none"> • Apply the Latest Patches and Updates |
| Configure your domains to use secured production mode. | Secured production mode enforces more restrictive and stringent security settings to ensure less vulnerability to threats. | <ul style="list-style-type: none"> • Configure Secured Production Mode • Understand How Domain Mode Affects the Default Security Configuration |
| Use a domain-wide administration port for administrative traffic. | <p>An administration port limits all administrative traffic between server instances in a WebLogic Server domain to a single port. The administration port accepts only secure, SSL traffic, and all connections via the port require authentication.</p> <p>The administration port is enabled by default in secured production mode.</p> | <ul style="list-style-type: none"> • Configure an Administration Port for the Domain |
| Set permissions to restrict the access of the user account used to run WebLogic Server to just the WebLogic resources and domain data stored on disk. Ensure that this account is not an administrator account. | <p>WebLogic domain and server configuration files should be accessible only by the operating system users who configure or execute WebLogic Server. No other operating system user (apart from the system administrators) should have read, write, or execute access to WebLogic Server product files nor to your domain files.</p> <p>Knowledgeable operating system users may be able to bypass WebLogic Server security if they are given write access, and in some cases read access to domain data stored on disk and in the persistent store.</p> | <ul style="list-style-type: none"> • Set Permissions to Restrict Access to WebLogic Resources to One User Account |
| <p>Use network channels to isolate incoming application traffic.</p> <p>Use a firewall to limit access to only HTTPS application traffic and block access to non-HTTPS traffic (T3/T3s/LDAP/IIOP/IIOPs).</p> | Oracle strongly recommends that you do not expose non-HTTPS traffic (T3/T3s/LDAP/IIOP/IIOPs) outside of the external firewall. You can control this access using a combination of network channels and firewalls. | <ul style="list-style-type: none"> • Configure Network Channels and Firewalls to Prevent Access from Non-HTTPS Traffic |

Table 1-1 (Cont.) Critical Tasks for Locking Down WebLogic Server

| Task | Description | More Information |
|--|--|---|
| Block access to internal applications by disabling unneeded applications and using a firewall to block access to internal application context paths. | Depending on your application usage and the domain configuration, some internal applications may not be used in a particular domain. To reduce the attack surface, Oracle strongly recommends that you configure a firewall to block external access to internal applications and disable access to these applications. | <ul style="list-style-type: none"> • Disable Unused Internal Applications • Configure Firewall to Prevent Access to Internal Applications |
| Use SSL/TLS, but do not use the demonstration digital certificates in a production environment. | <p>Configure SSL/TLS for the administration port, network channels, database connections, LDAP server connections, and other resources handling communication that must be secured. In particular, make sure that connections to remote server instances in the domain are secured with SSL.</p> <p>WebLogic Server includes a set of demonstration private keys, digital certificates, and trusted certificate authorities that are for development only. Oracle highly recommends that you use third-party Certificate Authority (CA) signed certificates in a production environment.</p> | <ul style="list-style-type: none"> • Configure SSL/TLS |
| Restrict incoming serialized objects. | Serialization in Java can be used to inject malicious code using serialized Java objects that can cause Denial of Service (DoS) or Remote Code Execution (RCE) attacks during deserialization. WebLogic Server uses the JDK JEP 290 mechanism to filter incoming serialized Java objects to protect against these malicious attacks. | <ul style="list-style-type: none"> • Use JEP 290 to Restrict Incoming Serialized Java Objects |
| Disable remote anonymous RMI T3 and IIOP requests. | Disabling remote anonymous T3 and IIOP RMI requests will require that clients authenticate before invoking on WebLogic Server. Unauthenticated clients will be rejected. | <ul style="list-style-type: none"> • Disable Remote Anonymous RMI T3 and IIOP Requests |
| Review the Security Warnings Report. | Check the Security Warnings Report to identify if any potential security issues are currently affecting your domain and how to resolve those issues. | <ul style="list-style-type: none"> • Review Potential Security Issues |

2

Understand and Secure Your Environment

The security requirements you establish for your WebLogic Server environment are based upon multiple considerations, such as the types of resources hosted on WebLogic Server that need to be protected, the users and other entities that access those resources, recommendations from Oracle as well as in-house or independent security consultants, and more.

This chapter includes the following sections:

- [Understand Your Environment](#)
- [Hire Security Consultants or Use Diagnostic Software](#)
- [Read Security Publications](#)
- [Secure the Host Environment](#)
- [Secure Your Database](#)

Understand Your Environment

The WebLogic Server environment includes not only the resources that are hosted on WebLogic Server, but also the software systems and other entities with which those WebLogic Server resources interoperate, such as databases, and load balancers, and the users who have access to that environment.

To better understand your security needs, ask yourself the following questions:

- Which resources am I protecting?
Many resources in the production environment can be protected, including information in databases accessed by WebLogic Server and the availability, performance, applications, and the integrity of the Web site. Consider the resources you want to protect when deciding the level of security you must provide.
- From whom am I protecting the resources?
For most Web sites, resources must be protected from everyone on the Internet. But should the Web site be protected from the employees on the intranet in your enterprise? Should your employees have access to all resources within the WebLogic Server environment? Should the system administrators have access to all WebLogic resources? Should the system administrators be able to access all data? You might consider giving access to highly confidential data or strategic resources to only a few well trusted system administrators. Perhaps it would be best to allow no system administrators access to the data or resources.
- What will happen if the protections on strategic resources fail?
In some cases, a fault in your security scheme is easily detected and considered nothing more than an inconvenience. In other cases, a fault might cause great damage to companies or individual clients that use the Web site. Understanding the security ramifications of each resource will help you protect it properly.

Hire Security Consultants or Use Diagnostic Software

Whether you deploy WebLogic Server on the Internet or on an intranet, it is a good idea to hire an independent security expert to go over your security plan and procedures, audit your installed systems, and recommend improvements. Oracle Consulting offers services and products that can help you to secure a WebLogic Server production environment. See the Oracle Consulting page at <https://www.oracle.com/consulting/index.html>.

Read Security Publications

Staying current with security publications, such as those made available on My Oracle Support, is critical to maintaining a secure operational environment for WebLogic Server.

Read about security issues:

- Register your WebLogic Server installation with My Oracle Support. By registering, Oracle Support will notify you immediately of any security updates that are specific to your installation. You can create a My Oracle Support account by visiting <http://www.oracle.com/support/index.html>.
- For security advisories, refer to the Critical Patch Updates, Security Alerts and Bulletins page at the following location:
<https://www.oracle.com/security-alerts/>
- When developing your web applications, ensure that they minimize the risks identified in the OWASP Top Ten Web Application Security Risks at <https://owasp.org/www-project-top-ten/>.

Secure the Host Environment

A WebLogic Server production environment is only as secure as the security of the machine on which it is running. It is important to secure the host on which WebLogic Server is running such as the physical machine, the operating system, and all other software that is installed on the host machine.

The following table lists the recommendations for securing a WebLogic Server host environment. Also check with the manufacturer of the machine and operating system for recommended security measures. For details about securing WebLogic Server, see [Lock Down WebLogic Server](#).

Table 2-1 Secure the WebLogic Server Host Environment

| Security Action | Description |
|---------------------------------|--|
| Physically secure the hardware. | Keep your hardware in a secured area to prevent unauthorized operating system users from tampering with the deployment machine or its network connections. |

Table 2-1 (Cont.) Secure the WebLogic Server Host Environment

| Security Action | Description |
|---|--|
| Secure networking services that the operating system provides. | <p>Have an expert review network services such as e-mail programs or directory services to ensure that a malicious attacker cannot access the operating system or system-level commands. The way you do this depends on the operating system you use.</p> <p>Sharing a file system with other machines in the enterprise network imposes risks of a remote attack on the file system. Be certain that the remote machines and the network are secure before sharing the file systems from the machine that hosts WebLogic Server.</p> <p>Make sure that the file system on each WebLogic Server host can prevent unauthorized access to protected resources. For example, on a Windows computer, use only NTFS.</p> |
| Limit the number of user accounts on the host machine. | <p>Avoid creating more user accounts than you need on WebLogic Server host machines, and limit the file access privileges granted to each account. On operating systems that allow more than one system administrator user, the host machine should have two user accounts with system administrator privileges and one user with sufficient privileges to run WebLogic Server. Having two system administrator users provides a back up at all times. The WebLogic Server user must be a restricted user, not a system administrator user. One of the system administrator users can always create a new WebLogic Server user if needed.</p> <p>Review active user accounts regularly and when personnel leave.</p> <p><i>Background Information:</i> Some WebLogic Server configuration data and some URL (Web) resources, including Java Server Pages (JSPs) and HTML pages, are stored in clear text on the file system. A sophisticated user or intruder with read access to files and directories might be able to defeat any security mechanisms you establish with WebLogic Server authentication and authorization schemes.</p> |
| On each host computer, give only one operating system (OS) user account access to WebLogic resources (in addition to the two system administrator users who also have access privileges). | <p>Important: WebLogic domain and server configuration files must be accessible only by the operating system user who configures or executes WebLogic Server. No other operating system user (apart from the system administrators) should have read, write, or execute access to WebLogic Server product files, nor to your domain files.</p> <p>See Set Permissions to Restrict Access to WebLogic Resources to One User Account</p> |
| Do not develop on a production machine. | <p>Develop first on a development machine and then move code to the production machine when it is completed and tested. This process prevents bugs in the development environment from affecting the security of the production environment.</p> |

Table 2-1 (Cont.) Secure the WebLogic Server Host Environment

| Security Action | Description |
|--|---|
| Do not install development or sample software on a production machine. | Do not install development tools on production machines. Keeping development tools off the production machine reduces the leverage intruders have should they get partial access to a WebLogic Server production machine. |
| Do not run Web servers as <code>root</code> . | <p>When you run a Web server on Unix systems — such as Apache HTTP Server, Microsoft IIS, or Oracle iPlanet Web Server — make sure of the following:</p> <ul style="list-style-type: none"> • The Web server must run only as an unprivileged user, never as <code>root</code>. • The directory structure in which the Web server is located, including all files, must be protected from access by unprivileged users. <p>Taking these steps helps ensure that unprivileged users cannot insert code that can potentially be executed by the Web server.</p> |
| Enable security auditing. | If the operating system on which WebLogic Server runs supports security auditing of file and directory access, Oracle recommends using audit logging to track any denied directory or file access violations. Administrators must ensure that sufficient disk space is available for the audit log. |
| Consider using additional software to secure your operating system. | <p>Most operating systems can run additional software to secure a production environment. For example, an Intrusion Detection System (IDS) can detect attempts to modify the production environment.</p> <p>Refer to the vendor of your operating system for information about available software.</p> |
| Apply operating-system patch sets and security patches. | Refer to the vendor of your operating system for a list of recommended patch sets and security-related patches. |

Secure Your Database

Most Web applications use a database to store their data. Common databases used with WebLogic Server are Oracle, Microsoft SQL Server, IBM DB2, and MySQL. The databases frequently hold the Web application's sensitive data including customer lists, customer contact information, credit card information, and other proprietary data. When creating your Web application you must consider what data is going to be in the database and how secure you need to make that data. You also need to understand the security mechanisms provided by the manufacturer of the database and decide whether they are sufficient for your needs. If the mechanisms are not sufficient, you can use other security techniques to improve the security of the database, such as encrypting sensitive data before writing it to the database. For example, leave all customer data in the database in plain text except for the encrypted credit card information.

3

Lock Down WebLogic Server

Lock down WebLogic Server by performing a secure installation, configuring your domains to use secured production mode, securing network resources using firewalls, and securing WebLogic resources and applications.

If you are installing WebLogic Server in a production environment, Oracle strongly recommends that you follow the guidelines described in these sections:

- [Install WebLogic Server in a Secure Manner](#)
- [Configure a Secure Domain](#)
- [Secure the Network](#)
- [Avoid Using These Configurations and Settings in a Locked Down Environment](#)
- [Secure Applications](#)

Install WebLogic Server in a Secure Manner

Creating a secure environment for WebLogic Server begins with planning a secure installation, which includes restricting access to the WebLogic Server host machine only to authorized users, and installing only the components of WebLogic Server that are needed in the target environment.

- Before you install WebLogic Server, be sure to secure the host machine, operating system, and file system to ensure that access is restricted only to authorized users. For specific recommendations, see [Secure the Host Environment](#).
- When running the installation program, do not install WebLogic Server sample applications and be sure to choose the option to receive security updates. For a detailed procedure, see Performing a Secure Installation of WebLogic Server in *Administering Security for Oracle WebLogic Server*.

Apply the Latest Patches and Updates

To ensure the security of your installed environment, Oracle strongly recommends that you apply the latest WebLogic Server, Java, and database Critical Patch Updates as soon as they are released.

The following table describes the patches and updates you need to apply to ensure that your WebLogic Server installation is protected by the latest software updates.

Table 3-1 Apply Latest Patch Sets and Updates

| Security Action | Description |
|---|---|
| Install the latest Patch Set Updates (PSUs). | <p>Fixes for WebLogic Server security vulnerabilities are included in WebLogic Server PSUs, released with the Critical Patch Update (CPU) program. PSUs are issued for WebLogic Server versions and patch sets that are actively supported and under error correction, on a planned schedule, per the Critical Patch Updates, Security Alerts and Bulletins.</p> <p>Oracle strongly recommends that you schedule the installation of these PSUs, and apply them in as timely a manner as possible after they are released.</p> <p>If you are responsible for security-related issues at your site, register your WebLogic Server installation with Oracle Support and create a My Oracle Support account at https://support.oracle.com. When PSUs are released, their content is documented in the My Oracle Support document <i>Patch Set Update (PSU) Release Listing for Oracle WebLogic Server (WLS) (Doc ID 1470197.1)</i>.</p> <p>For additional information about WebLogic Server security vulnerabilities, see the My Oracle Support document <i>Security Vulnerability FAQ for Oracle Database and Fusion Middleware Products (Doc ID 1074055.1)</i>.</p> |
| Ensure that the WebLogic Server version and patch set you are using is actively supported and under error correction. | <p>New bug fixes, including fixes for security vulnerabilities, are only provided for product versions and patch sets that are under Premier or Extended Support, and are also under error correction.</p> <p>To verify that your WebLogic Server version is under Premier or Extended Support, refer to the Oracle Lifetime Support Policy for Oracle Fusion Middleware.</p> <p>To verify that your WebLogic Server version and patch set is under error correction, refer to the Oracle Error Correction Policy as documented in the My Oracle Support document <i>Error Correction Support Dates for Oracle WebLogic Server (Doc ID 950131.1)</i>.</p> <p>You must proactively plan to upgrade the WebLogic Server version and patch set you are using as required to ensure that it will remain under Premier or Extended Support and under error correction.</p> |

Table 3-1 (Cont.) Apply Latest Patch Sets and Updates

| Security Action | Description |
|--|--|
| Maintain the security of the JDK and JVM versions used on the production system. | <p>Ensure that the JDK and JVM versions are certified with WebLogic Server as listed in Oracle Fusion Middleware Supported System Configurations, are currently supported by their vendors, and have the latest security updates applied.</p> <p>For users of Oracle JDKs and JVMs, we strongly recommend:</p> <ul style="list-style-type: none"> • Using JDK and JVM versions that are currently supported per the Oracle Java SE Support Roadmap. • Applying the latest Java Critical Patch Updates (CPUs) as soon as they are released. The Critical Patch Updates, Security Alerts and Bulletins page references the latest <i>Patch Availability Document for Oracle Java SE</i> documents that are available on My Oracle Support. |

Configure a Secure Domain

Configuring a secure domain involves using secured production mode, configuring a password validation provider, configuring auditing and user lockouts, limiting the accounts with access to WebLogic resources, and so on.

Topics include:

- [Configure Secured Production Mode](#)
- [Configure an Administration Port for the Domain](#)
- [Disable Unused Internal Applications](#)
- [Configure Additional Security Settings After Domain Creation](#)
- [Set Permissions to Restrict Access to WebLogic Resources to One User Account](#)
- [Do Not Include Unencrypted Passwords in Commands and Scripts](#)
- [Secure WebLogic Resources](#)
- [Review Potential Security Issues](#)

Configure Secured Production Mode

To ensure less vulnerability to threats, Oracle strongly recommends that you configure your domain to run in secured production mode.

The domain mode determines default settings regarding security and logging. In development mode, the security configuration is more relaxed. You can start the Administration Server using a boot identity file or deploy an application using the `autodeploy` directory. In production mode, the security configuration is more stringent, such as requiring a user name and password to deploy applications and start the Administration Server. In secured production mode, your production domain is highly secure because the security configuration defaults are more secure, insecure configuration items are logged as warnings, and default

authorization and role mapping policies are more restrictive. See [Understand How Domain Mode Affects the Default Security Configuration](#).

To configure secured production mode, you must first ensure that your domain is in production mode. The secured production mode option is not available for domains that are running in development mode. For information about how to change the WebLogic Server instances in a domain to run in production mode, see [Change to production mode](#) in the *Oracle WebLogic Server Administration Console Online Help*. You can also enable production mode on the `DomainMBean` using the WebLogic Scripting Tool by navigating to the Domain configuration and setting `ProductionModeEnabled` MBean attribute to `true`. See [DomainMBean](#) in *MBean Reference for Oracle WebLogic Server*.

For details about how to configure secured production mode, see [Creating a WebLogic Domain for Production Use](#) in *Administering Security for Oracle WebLogic Server*.

Also, Oracle strongly recommends that you enable the most secure values for WebLogic Server MBeans. WebLogic Server contains a number of MBeans that have attributes that affect the security of the WebLogic domain. When you enable secured production mode, most of these attributes are set to the most secure value automatically. However, there are some MBean attributes that cannot be set automatically and must be set to most secure value manually if required for your environment. For example, although SSL is enabled by default (`Enabled = true` on the SSL MBean), the `TwoWaySSLEnabled` and `ClientCertificateEnforced` attributes on the `SSLMBean` and the `NetworkAccessPointMBean` are not set to `true` because it requires certificates from all clients. If two-way SSL is required, you can set these attributes manually. For a complete list of these attributes and their most secure values, see [Secure Values for MBean Attributes](#) in *MBean Reference for Oracle WebLogic Server*.

Understand How Domain Mode Affects the Default Security Configuration

The domain mode you select determines the default security configuration for your domain. When configuring a domain, be sure to select the domain mode that best meets the security requirements of the environment in which WebLogic Server runs.

[Table 3-2](#) describes how the security and performance-related configuration parameters differ depending on whether your domain is configured in development mode, production mode, or secured production mode. Note that you can customize the behavior of the different domain modes by setting attribute values that override the defaults. For example, you could enable the Administration port in a production mode domain.

Note:

WebLogic Server automatically checks if your domain meets certain security standards. For each potential security issue in a domain, a warning is logged and displayed in the Security Warnings Report in the Administration Console. As a domain progresses from development to production to secured production mode, the security validation checks become more strict.

Table 3-2 Differences in Domain Modes

| Feature | Development Mode | Production Mode | Secured Production Mode |
|---------------------|---|---|---|
| SSL/TLS | You can use the demonstration digital certificates and the demonstration keystores provided by the WebLogic Server security services. With these certificates, you can design your application to work within environments secured by SSL/TLS. See Overview of Configuring SSL in WebLogic Server in <i>Administering Security for Oracle WebLogic Server</i> . | Demonstration digital certificates and the keystores are not recommended in production mode. If you do so, a warning message appears. | In this mode, WebLogic Server logs a warning if the SSL/TLS configuration is insecure. Also, the Administration Server will not start if the SSL Identity certificate is expired. WebLogic Server validates the minimum SSL/TLS version, constraints, and ciphers. |
| Administration port | The administration port is disabled by default. | The administration port is disabled by default. To enable an administration port for your domain, see Configure the domain-wide administration port in the <i>Oracle WebLogic Server Administration Console Online Help</i> . | The administration port is enabled by default. The administrative traffic is no longer allowed on the non-administration ports. In this mode, you must specify T3s protocol and the administration port when using WLST to connect to the Administration Server. The Administration Console is available only via https on the administration port (default is 9002). |
| Listen Port | The server listen port is enabled by default. The default port value is 7001. | The server listen port is enabled by default. The default port value is 7001. | The listen port is disabled by default. To enable and manage the listen port, see Configure listen ports in the <i>Oracle WebLogic Server Administration Console Online Help</i> . |

Table 3-2 (Cont.) Differences in Domain Modes

| Feature | Development Mode | Production Mode | Secured Production Mode |
|------------------------|--|---|---|
| SSL/TLS listen Port | The SSL/TLS listen port is disabled by default. | The SSL/TLS listen port is disabled by default. You can enable the SSL/TLS listen port for servers in your domain. See Configure listen ports in the <i>Oracle WebLogic Server Administration Console Online Help</i> . | The SSL/TLS listen port is enabled by default. The default port value is 7002. |
| Auditing | Security or configuration auditing is disabled by default. | Security or configuration auditing is disabled by default. | When the domain is created, the WebLogic Auditing provider is configured by default. Configuration changes are audited. WebLogic Server logs a warning if an Auditing provider is not configured. |
| Deploying applications | WebLogic Server instances can deploy and update applications that reside in the <i>domain_name/autodeploy</i> directory automatically. Oracle recommends that you use this method only in a single-server development environment. See <i>Deploying Applications and Modules with weblogic.deployer</i> in <i>Deploying Applications to Oracle WebLogic Server</i> . | The auto-deployment feature is disabled. Use the WebLogic Server Administration Console, the <i>weblogic.deployer</i> tool, or the WebLogic Scripting Tool. | The auto-deployment feature behavior in secured production mode is the same as in production mode. |

Table 3-2 (Cont.) Differences in Domain Modes

| Feature | Development Mode | Production Mode | Secured Production Mode |
|-------------------------------------|---|---|--|
| Log file rotation | <p>By default, when you start the WebLogic Server instance, the server automatically renames (rotates) its local server log file as <code>SERVER-NAME.log.n</code>. For the remainder of the server session, messages accumulate in the log file until the file grows to a size of 500 kilobytes.</p> <p>See Rotate Log Files in the <i>Oracle WebLogic Server Administration Console Online Help</i>.</p> <p>The default value of the Limit number of retained files setting in Logging Configuration is <code>true</code>. This value limits the number of log files that the server instance creates to store old messages.</p> | <p>The server rotates the local log file after the size of the file reaches 5000 kilobytes.</p> <p>When the server is configured for production mode, by default, all versions of the log files are kept. Administrators may want to customize the number of log files that are retained. Use the LogFile MBean attributes to configure the location, file-rotation criteria, and number of files that a WebLogic Server instance uses to store log messages.</p> <p>The default value of the Limit number of retained files setting in Logging Configuration is <code>true</code>. The server creates 100 log files of 5 megabytes each. You must clean up the files as needed.</p> | <p>The log file rotation behavior in secured production mode is the same as in production mode.</p> |
| <code>boot.properties</code> | <p>A <code>boot.properties</code> file is created, which allows you to boot the server without specifying a user name and password.</p> | <p>A <code>boot.properties</code> file is <i>not</i> created.</p> | <p>A <code>boot.properties</code> file is <i>not</i> created.</p> |
| Deployment of internal applications | <p>For a development domain, the default is for WebLogic Server to deploy internal applications on the first access (on-demand).</p> | <p>For a production domain, the default is for WebLogic Server to deploy internal applications as part of server startup. If you want to change this behavior, see <i>On-Demand Deployment of Internal Applications in Deploying Applications to Oracle WebLogic Server</i>.</p> | <p>The deployment of internal applications in secured production mode is the same as in production mode.</p> |

Table 3-2 (Cont.) Differences in Domain Modes

| Feature | Development Mode | Production Mode | Secured Production Mode |
|-------------------------------------|--|---|---|
| Node Manager user name and password | In development mode, Node Manager uses the default user name and password credentials. | When a domain is created in production mode, then the user name and password for Node Manager are randomly generated. See <i>Specifying Node Manager User Name and Password</i> in <i>Administering Node Manager for Oracle WebLogic Server</i> . | In secured production mode, the Node Manager user name and password are generated the same way as in production mode. |
| Web Services Test Client | In a development environment, the Web Services Test Client is enabled, by default. | In a production environment, the Web Services Test Client is disabled (and not deployed), by default. It is recommended that you not enable the Web Services Test Client in production mode. You can enable or disable the Web Services Test Client using the Administration Console, Fusion Middleware Control, or WLST. See <i>Enabling and Disabling the Web Services Test Client</i> in <i>Administering Web Services</i> . | The default behavior of the Web Services Test Client in secured production mode is the same as in production mode. |
| Classloader Analysis Tool | Classloader Analysis Tool (CAT) is deployed as an internal on-demand application only in development mode. Deployment happens upon first access. | If the server is running in production mode, it is not deployed automatically. You can deploy it in production mode; there are no limitations on its use, but you must deploy it manually, just like any other Web application. See <i>Using the Classloader Analysis Tool (CAT)</i> in <i>Developing Applications for Oracle WebLogic Server</i> . | The CAT tool behavior in secured production mode is the same as in production mode. |

Table 3-2 (Cont.) Differences in Domain Modes

| Feature | Development Mode | Production Mode | Secured Production Mode |
|--------------------------------------|--|--|---|
| FastSwap deployment | You can use FastSwap deployment to minimize redeployment. FastSwap is only supported when WebLogic Server is running in development mode. See <i>Using FastSwap Deployment to Minimize Redeployment in Deploying Applications to Oracle WebLogic Server</i> . | FastSwap is automatically disabled in production mode. | FastSwap is automatically disabled in secured production mode. |
| Administration Console Change Center | The Change Center in the Administration Console provides a way to lock a domain configuration so you can make changes to the configuration while preventing other accounts from making changes during your edit session. This feature is disabled by default if your domain is running in development mode. It can be enabled or disabled in development domains. See Enable and disable the domain configuration lock in the <i>Oracle WebLogic Server Administration Console Online Help</i> . | In production mode, you need to procure a lock and edit session before making configuration changes to the domain. Therefore, this domain configuration locking feature is always enabled in production domains. | The domain configuration locking feature is the same as in production mode. |
| JMS File Store | A file store is automatically created in the file system. | The file store directory is not created automatically in the file system and users must manually create the directory with the necessary permissions. | The default behavior of the JMS file store is the same as in production mode. |

Configure an Administration Port for the Domain

Oracle strongly recommends that you use a domain-wide administration port for administrative traffic.

 **Note:**

If your domain is configured to run in secured production mode, then the administration port is enabled by default and the administrative traffic is no longer allowed on the non-administration ports. In this mode, WebLogic Server logs a warning if the administration port is not enabled.

An administration port limits all administrative traffic between server instances in a WebLogic Server domain to a single port. If an administration port is enabled, WebLogic Server automatically generates an administrative channel for your domain, based on the port settings upon server instance startup. The administrative channel provides a listen address and listen port to handle administration traffic.

When the server is run without an administration port, a management client can inadvertently transmit confidential server configuration on the wire in clear-text. Running the server with an administration port significantly reduces the chances of this happening. Furthermore, having an administrative port configured is helpful should a Denial of Service (DoS) attack occur because the resources for handling requests for, and the limitations on administration port requests are separate from those of the rest of the server.

When used in conjunction with a connection filter, you can specify that a WebLogic Server instance accepts administrative requests only from a known set of machines or subnets and only on a single port.

Enabling the administration port requires clients to interact with the WebLogic Server Administration Console using SSL which protects sensitive data from being sniffed on the wire by an attacker and protects against some cross site scripting attacks.

See the following topics for more information:

- [Configure the domain-wide administration port](#) in the *Oracle WebLogic Server Administration Console Online Help*
- Administration Port and Administrative Channel in *Administering Server Environments for Oracle WebLogic Server*

Disable Unused Internal Applications

Depending on your application usage and the domain configuration, some internal applications may not be used in a particular domain. Oracle strongly recommends that you disable access to these applications to reduce the attack surface.

You can disable unused internal applications using the configuration settings. Some internal applications are disabled by default; they must be enabled only if needed. The following table provides a list of internal applications that can be disabled and the process to disable them.

Table 3-3 Disabling Internal Applications

| Internal Application | Process to Disable |
|---|--|
| WebLogic Server Administration Console | Set the <code>ConsoleEnabled</code> attribute in the <code>DomainMBean</code> to <code>false</code> , or deselect the Console Enabled check box under advanced configuration settings for your domain in the Administration Console. |
| Restful Services | Set the <code>Enabled</code> attribute in the <code>RestfulManagementServicesMBean</code> to <code>false</code> , or deselect the Enable RESTful Management Services check box under advanced configuration settings for your domain in the Administration Console. |
| Management EJB (Java EE Management APIs) | Set the <code>ManagementEJBEnabled</code> attribute in the <code>JMXMBean</code> to <code>false</code> , or deselect the Management EJB Enabled check box under advanced configuration settings for your domain in the Administration Console. |
| Default Internal Servlets | Set the <code>DefaultInternalServletsDisabled</code> attribute in the <code>ServerMBean</code> to <code>true</code> . In secured production mode, this attribute is set to <code>true</code> by default and internal servlets are disabled. |
| Web Service Asynchronous Request-Response | Use the <code>OptionalFeatureMBean</code> to add an asynchronous request-response internal application with the name <code>JAXRPC_ASYNC_RESPONSE</code> , and set the feature to <code>false</code> . You can do this using WLST as shown in the following snippet: <pre> optf = cmo.getOptionalFeatureDeployment() async = optf.createOptionalFeature("JAXRPC_ASYNC_RESPONSE") async.setEnabled(false) </pre> |
| Web Service Atomic Transactions (WSAT) | Use the <code>OptionalFeatureMBean</code> to add a WSAT internal application with the name <code>WSAT</code> , and set the feature to <code>false</code> . You can do this using WLST as shown in the following snippet: <pre> optf = cmo.getOptionalFeatureDeployment() wsat = optf.createOptionalFeature("WSAT") wsat.setEnabled(false) </pre> |

Table 3-3 (Cont.) Disabling Internal Applications

| Internal Application | Process to Disable |
|----------------------|--|
| Ready App | <p>Use the <code>OptionalFeatureMBean</code> to add a feature with the name <code>READYAPP</code>, and set the feature to <code>false</code>. You can do this using WLST as shown in the following snippet:</p> <pre> optf = cmo.getOptionalFeatureDeployment() ra = optf.createOptionalFeature("READYAPP") ra.setEnabled(false) </pre> |

Configure Additional Security Settings After Domain Creation

After you create your domain and configure secured production mode, there are a number of additional steps and configuration that you must complete to secure the domain.

The following table describes additional configuration and settings that you must configure to ensure the security of your domain.

Table 3-4 Additional Configuration and Settings to Secure the Domain

| Security Action | Description |
|--|---|
| Create no fewer than two user accounts with system administrator privileges. | <p>Having at least two system administrator user accounts helps to ensure that one user maintains account access in case another user becomes locked out by a dictionary/brute force attack.</p> <p>One of the system administrator users is created when you create the domain. Create other user(s) and assign them the <code>Admin</code> security role. When creating system administrator users give them unique names that cannot be easily guessed. Avoid using obvious names such as <code>system</code>, <code>admin</code>, or <code>administrator</code>.</p> <p>Note: If you have enabled secured production mode, then WebLogic Server logs warnings if users in the administrator group have obvious user names such as <code>system</code>, <code>admin</code>, <code>administrator</code>, or <code>weblogic</code>.</p> |

Table 3-4 (Cont.) Additional Configuration and Settings to Secure the Domain

| Security Action | Description |
|---|---|
| Configure the Password Validation provider immediately after configuring a new WebLogic domain | <p>The Password Validation provider, which is included with WebLogic Server, can be configured with several out-of-the-box authentication providers to manage and enforce password composition rules. Consequently, whenever a password is created or updated in the security realm, the corresponding authentication provider automatically invokes the Password Validation provider to ensure that the password meets the composition requirements that are established.</p> <p>For information about how to configure and use the Password Validation provider, see <i>Configuring the Password Validation Provider</i> in <i>Administering Security for Oracle WebLogic Server</i>.</p> |
| To bind to protected ports on UNIX, configure WebLogic Server to switch user IDs or use Network Address Translation (NAT) software. | <p>On UNIX systems, only processes that run under a privileged user account (in most cases, root) can bind to ports lower than 1024. UNIX systems allow only one system administrator (root) user.</p> <p>However, long-running processes like WebLogic Server must not run under these privileged accounts. Instead, you can do either of the following:</p> <ul style="list-style-type: none"> • For each WebLogic Server instance that needs access to privileged ports, configure the server to start under the privileged user account, bind to privileged ports, and change its user ID to a non-privileged account. <ul style="list-style-type: none"> If you use Node Manager to start the server instance, configure Node Manager to accept requests only on a secure port and only from a single, known host. Note that Node Manager needs to be started under a privileged user account. See Create and configure machines to run on UNIX in the <i>Oracle WebLogic Server Administration Console Online Help</i>. • Start WebLogic Server instances from a non-privileged account and configure your firewall to use Network Address Translation (NAT) software to map protected ports to unprotected ones. <p>Note: If you are using a domain that is running in secured production mode, then WebLogic Server logs a warning if the following are true:</p> <ul style="list-style-type: none"> • Ports less than 1024 are used. • The <code>PostBindGIDEnabled</code> and <code>PostBindUIDEnabled</code> attributes of the <code>UnixMachineMBean</code> are <i>not</i> set to true. |

Table 3-4 (Cont.) Additional Configuration and Settings to Secure the Domain

| Security Action | Description |
|---|--|
| Secure your JNDI root context. | <p>Group <code>Everyone</code> must not have access to the JNDI Root Content resource if the WebLogic Server Administration Console is externally visible. By default, JNDI resources have a default group security policy of <code>Everyone</code>.</p> <p>Note: If secured production mode is enabled for your domain, then WebLogic Server does not allow remote anonymous JNDI access for list or modify operations. You can control anonymous JNDI access by setting the <code>RemoteAnonymousJNDIEnabled</code> attribute that is contained in the <code>SecurityConfigurationMBean</code>.</p> |
| Configure WebLogic Server to avoid overload conditions. | <p>Configure WebLogic Server to avoid overload conditions in order to allow WebLogic Server sufficient processing power so that an administrator can connect to it and attempt to correct the problem in case the server comes under heavy load.</p> <p>Because communication over administration channels is not prevented when the system is overloaded, administrators can always connect regardless of any current overload condition.</p> <p>In case of heavy load, the administrator must bring the server into the admin state, locate the offending user, and then prevent that user from overloading the server with requests.</p> <p>To configure WebLogic Server to avoid overload conditions, set the shared capacity attribute in the overload protection MBean. The setting you choose for this attribute is the threshold after which no more non-administrator requests are accepted by WebLogic Server.</p> <p>See <i>Avoiding and Managing Overload</i> in <i>Administering Security for Oracle WebLogic Server</i>.</p> |

Table 3-4 (Cont.) Additional Configuration and Settings to Secure the Domain

| Security Action | Description |
|--|--|
| Configure user lockouts and login time limits to prevent attacks on user accounts. | <p>By default, the WebLogic Security Service provides security against dictionary and brute force attacks of user accounts. If during development you changed the settings for the number of invalid login attempts required before locking the account, the time period in which invalid login attempts have to take place before locking the account, or the amount of time the user account is locked, review the settings and verify that they are adequate for your production environment.</p> <p>Note: User lockout is effected by the WebLogic Security Service on a per-server basis. For example, a user who has been locked out of an application hosted on a given Managed Server (or cluster) is not necessarily locked out of the WebLogic Server Administration Console. Likewise, a user who has been locked out of the WebLogic Server Administration Console is not necessarily prevented from attempting to log in to an application hosted on a Managed Server.</p> <p>See Set user lockout attributes in the <i>Oracle WebLogic Server Administration Console Online Help</i>.</p> <p><i>Background Information:</i> In a dictionary/brute force attack, a hacker sets up a script to attempt logins using passwords out of a dictionary. The WebLogic Server user lockout and login settings can protect user accounts from dictionary/brute force attacks.</p> <p>Note: If you have configured your domain to run in secured production mode, then WebLogic Server logs a warning if the user lockout is configured to a value less than the default value.</p> |

Table 3-4 (Cont.) Additional Configuration and Settings to Secure the Domain

| Security Action | Description |
|---|--|
| Enable security auditing. | <p>Auditing is the process of recording key security events in your WebLogic Server environment. When the Auditing provider that the WebLogic Security Service provides is enabled, it logs events in <code>DomainName\DefaultAuditRecorder.log</code>.</p> <p>You enable an Auditing provider in the WebLogic Server Administration Console on the Security Realms > RealmName > Providers > Auditing page.</p> <p>See Configure Auditing providers in the <i>Oracle WebLogic Server Administration Console Online Help</i>.</p> <p>Note: Using an Auditing provider might adversely affect the performance of WebLogic Server even if only a few events are logged.</p> <p>Review the auditing records periodically to detect security breaches and attempted breaches. Noting repeated failed logon attempts or a surprising pattern of security events can prevent serious problems.</p> <p>If you develop your own custom Auditing provider and would like more information on posting audit events from a provider's Mbean, refer to Best Practice: Posting Audit Events from a Provider's MBean in <i>Developing Security Providers for Oracle WebLogic Server</i>.</p> <p>Note: If secured production mode is enabled for your domain, then WebLogic Server logs a warning if an audit provider is not configured. In this mode, the <code>ConfigurationAuditType</code> domain configuration element has a secure default value of <code>CONFIG_CHANGE_AUDIT</code>. Use the <code>WarnOnAuditing</code> attribute contained in the <code>SecureModeMBean</code> to specify whether warnings should be logged if auditing is not enabled.</p> |
| Ensure that you have correctly assigned users and groups to the default WebLogic Server security roles. | <p>By default, all WebLogic resources are protected by security policies that are based on a default set of security roles.</p> <p>Make sure you have assigned the desired set of users and groups to these default security roles.</p> <p>See <i>Users, Groups, And Security Roles in Securing Resources Using Roles and Policies for Oracle WebLogic Server</i>.</p> |
| If you have a requirement to comply with Federal Information Processing Standards (FIPS) 140-2, ensure that FIPS mode is enabled. | <p>FIPS mode is supported for JSSE via the RSA provider. FIPS 140-2 is a standard that describes U.S. Federal government requirements for sensitive, but unclassified use.</p> <p>To enable FIPS from the installed JDK file, see <i>Enabling FIPS 140-2 Mode From java.security in Administering Security for Oracle WebLogic Server</i>.</p> <p>Note: The April 2021 Patch Set Update (PSU) adds support for: RSA Crypto-J V6.2.5, RSA SSL-J V6.2.6, and RSA Cert-J V6.2.4.0.1.</p> |

Set Permissions to Restrict Access to WebLogic Resources to One User Account

On each host computer, give only one operating system (OS) user account access to WebLogic resources (in addition to the two system administrator users who also have access privileges) and set operating system file access permissions to restrict access to data stored on disk and in the persistent store..

Important: WebLogic domain and server configuration files must be accessible only by the operating system user who configures or executes WebLogic Server. No other operating system user (apart from the system administrators) should have read, write, or execute access to WebLogic Server product files, nor to your domain files.

On each WebLogic Server host computer, use the operating system to establish a special user account (for example, `wls_owner`) specifically to run WebLogic Server. Grant to this operating-system (OS) user account access privileges only to the following directories:

- **Oracle home**

The top-level directory that is created for all the Oracle Fusion Middleware products that are installed on your machine; this directory is created when WebLogic Server is installed.

- **WebLogic Server product installation directory**

This directory contains all the WebLogic Server software components that you choose to install on your system, including program files. By default, this directory is a subdirectory of the Oracle home and is named `wlserver`.

- **WebLogic domain directories**

These directories contain the configuration files, security files such as `SerializedSystemIni.Dat`, log files, Java EE applications, and other Java EE resources for a single WebLogic domain. By default, a domain is a subdirectory of Oracle home (for example, `Oracle/WebLogicServer/user_projects/domains/domain1`); however, domain directories can be located outside the WebLogic Server installation directory and Oracle home as well. If you create multiple domains on a WebLogic Server host computer, each domain directory must be protected.

- **Keystore directories**

These directories include the private keystore and the Root Certificate Authority (CA) keystore that contain private keys, their associated digital certificates, and trusted CA certificates. See *Storing Private Keys, Digital Certificates, and Trusted Certificate Authorities* in *Administering Security for Oracle WebLogic Server*.

- **Application archive directories**

These optional directories contain the application archives that are provisioned to WebLogic Server during deployment in the provisioning stage for the domain. These directories are separate from the WebLogic Server installation and domain directories.

This protection limits the ability of other applications that are executing on the same machine as WebLogic Server to gain access to WebLogic Server files and your domain files. Without this protection, some other application could gain write access and insert malicious, executable code in JSPs and other files that provide dynamic content. The code would be executed the next time the file was served to a client.

Knowledgeable operating system users may be able to bypass WebLogic Server security if they are given write access, and in some cases read access, to the following files:

- WebLogic Server Installation
- JDK files (typically in the WebLogic Server installation, but can be configured to be separate)
- Domain directory
- JMS SAF files
- File backed HTTP sessions

Everything that uses the persistent store, such as JMS SAF files, has sensitive data that must be protected from read access as well as from write access. The persistent store supports persistence to a file-based store or to a JDBC-enabled database.

If you use the file store to store files on WebLogic Server, the files can be stored anywhere. You must remember the locations of all of the files in order to protect them from read and write access.

If you use the JDBC store to store data, make sure to properly secure the database by protecting it from read and write access.

**Note:**

If your domain is running in secured production mode and your file system supports POSIX, then WebLogic Server logs warnings if directories and files (such as domain directories, JMS SAF files, etc) have incorrect permissions. Use `umask 027` as the minimum value when setting permissions.

Do Not Include Unencrypted Passwords in Commands and Scripts

Several WebLogic Server commands, including `WLST` and `weblogic.Deployer` commands, permit you to specify unencrypted passwords in the command line. Oracle strongly recommends that you do not include unencrypted passwords in command lines or scripts.

Specifying unencrypted passwords in the command line is a security risk: they can be easily viewed from the monitor screen by others, and they are displayed in process listings that log the execution of those commands.

When entering commands that require an unencrypted password, whether in a command window or script, take the following precautions to ensure that the passwords are entered securely:

- Enter passwords only when prompted. If you omit the password from the command line, you are subsequently prompted for it when the command is executed. The characters you type are not echoed.
- In script-based Node Manager commands that start remote Administration Server instances, ensure that the remote start username and password are obtained from the Administration Server's boot identity file.

- For WLST scripts that contain commands requiring a user name and password, create a user configuration file. This file, which you can create via the WLST `storeUserConfig` command, contains:
 - Your credentials in an encrypted form
 - A key file that WebLogic Server uses to unencrypt the credentials

During WLST sessions, or in WLST scripts, the user configuration file can be passed in commands such as the following:

 - `connect` — for connecting to a running WebLogic Server instance
 - `startServer` — for starting the Administration Server
 - `nmConnect` — for connecting WLST to Node Manager to establish a session
- For `weblogic.Deployer` scripts containing commands requiring a user name and password, you can specify the user configuration file created via the WLST `storeUserConfig` command instead of entering your unencrypted credentials.

For more information about passing user credentials securely in scripts, see the following topics:

- Starting and Stopping Servers and Boot Identity Files in *Administering Server Startup and Shutdown for Oracle WebLogic Server*.
- Security for WLST in *Understanding the WebLogic Scripting Tool*.
- Configuring Remote Server Start Security for Script-based Node Manager in *Administering Node Manager for Oracle WebLogic Server*.
- Syntax for Invoking `weblogic.Deployer` in *Deploying Applications to Oracle WebLogic Server*

Secure WebLogic Resources

The WebLogic Security Service combines several layers of security features to prevent unauthorized access to your WebLogic Server resources such as JDBC, JMS or EJB resources.

To secure resources in your WebLogic Server domain, review the items in the following table.

Table 3-5 Securing WebLogic Resources

| Security Action | Description |
|--|--|
| Restrict application use of JDBC over RMI. | <p>JDBC application calls made over RMI are not secure and may allow unrestricted access to the database. Oracle recommends configuring RMI JDBC security to disable JDBC application calls over RMI. To do so:</p> <ul style="list-style-type: none"> • Set the <code>RmiJDBCSecurity</code> attribute on the <code>DataSourceMBean</code> to <code>Secure</code>, which will reject all incoming application JDBC calls over RMI by remote clients and servers. <p>Note that RMI JDBC security does not disable Logging Last Resource, One Phase Commit, and Emulate Two Phase Commit data source transaction participants that span servers.</p> <ul style="list-style-type: none"> • Ensure that the SSL Listen Port setting is enabled for the server in the Configuration > General page of the WebLogic Server Administration Console. |

Table 3-5 (Cont.) Securing WebLogic Resources

| Security Action | Description |
|--|---|
| Configure Cross-Domain Security for JTA communication. | <p>Communication channels must be secure to prevent a malicious third-party from using man-in-the-middle attacks to affect transaction outcomes and potentially gaining administrative control over one or more domains. To ensure secure communication channels between domains, WebLogic Server supports a type of domain trust that is referred to as Cross-Domain Security. Cross-Domain Security establishes trust between two domains — a domain pair — such that principals in a subject from one WebLogic domain can make calls in another domain. WebLogic Server establishes a security role for cross-domain users, and uses the WebLogic Credential Mapping security provider in each domain to store the credentials to be used by the cross-domain users.</p> <p>For more information and configuration details, see:</p> <ul style="list-style-type: none"> • Cross Domain Security in <i>Developing JTA Applications for Oracle WebLogic Server</i> • Configuring Cross-Domain Security in <i>Administering Security for Oracle WebLogic Server</i> |
| Verify all WebLogic security policies. | <p>In WebLogic Server, security policies answer the question "who has access" to a WebLogic resource.</p> <p>Make sure that you have not removed security policies from WebLogic resources, and make sure that your security role assignments provide users the kind of access that you intend.</p> <p>For information about various resource types, and how you can secure resource types using policies, see the following topics in <i>Securing Resources Using Roles and Policies for Oracle WebLogic Server</i>:</p> <ul style="list-style-type: none"> • Understanding WebLogic Resource Security • Resource Types You Can Secure with Policies |

Review Potential Security Issues

The WebLogic Server July 2021 Patch Set Update (PSU) includes new WebLogic Administration Console security validation screens and new security validation MBeans that validate security configuration settings in your domain. With the July 2021 PSU applied, WebLogic Server regularly validates your domain configuration settings against a set of security configuration guidelines to determine whether the domain meets key security guidelines recommended by Oracle.

If your domain does not meet a recommendation for a security configuration setting, a warning is logged in the Security Warnings Report in the WebLogic Administration Console. When there are active warnings in the Security Warnings Report, a banner with red text appears across the top of the Administration Console. Click the text to see the report. In the Security Warnings Report, you will see any issues that need to be addressed and on which servers. You can also click View Security Warnings Report on the Administration Console home page to see current warnings.

Figure 3-1 Security Validation Screens

Security warnings detected. Click here to view the report and recommended remedies.

Home Log Out Preferences Record Help

Home

Home Page

Security Validation

Warnings Report

- View Security Warnings Report

Warnings Configuration

- Configure Security Warnings

Information and Resources

Helpful Tools

- Configure applications
- Configure GridLink for RAC Data Source
- Configure a Dynamic Cluster

General Information

- Common Administration Task Descriptions
- Read the documentation
- Ask a question on My Oracle Support

Security Warnings Report

This page displays a list of security warnings that should be addressed by the WebLogic administrators for this domain. For more information, see the guide *Securing a Production Environment for Oracle WebLogic Server*.

Click the Refresh Warnings button to refresh the list. This action may take a few seconds to complete.

[Customize this table](#)

Security Warnings Table

View Details Refresh Warnings Showing 1 to 1 of 1 Previous | Next

| | Message ID | # of Servers | Server Name(s) | Description |
|-----------------------|------------|--------------|----------------|--|
| <input type="radio"/> | 091003 | 1 | AdminServer | Secure Mode requires that users in the Administrators group do not have obvious user names. SOLUTION: Change the user name "weblogic" so it is not a commonly used administrator name. |

View Details Refresh Warnings Showing 1 to 1 of 1 Previous | Next

Settings

Configuration Monitoring Control **Security** Web Service Security ZDT Control Notes

General **Warnings** Filter Unlock User Embedded LDAP Roles Policies SSL Certificate Revocation

Click the **Lock & Edit** button in the Change Center to modify the settings on this page.

Save

This page allows you to define the security warnings settings for this WebLogic Server domain. For more info see *Production Environment for Oracle WebLogic Server*.

Warn on Patches Returns whether a war required WebLogic Server are not applied. [More](#)

Warn on Anonymous Requests Returns whether a war anonymous RMI request

Check Identity Certificates Returns true if identity periodically for expiration

Check Trust Certificates Returns true if trust certificate periodically for expiration

Warnings may appear for common issues that may indicate an insecure domain such as inadequate SSL/TLS configuration, outdated patch updates, or imminent certificate expiration. To protect your domain, resolve these warnings as consistent with your security and business requirements. You can resolve the warnings by updating your domain configuration settings to align with Oracle recommendations, or by disabling the security validation checks for that domain configuration setting.

Each warning in the Security Warnings Report includes a recommended solution for how to update the domain configuration setting. If you follow the recommended solution, the warning should be resolved. The same issue may affect multiple servers within your domain simultaneously. As you review the Security Warnings Report, make sure that you fix the issue on every affected server. Depending on the problem and its resolution, you may need to restart servers to update the Security Warnings Report.

For detailed advice on implementing the solutions identified, refer to the My Oracle Support article Doc ID 2788605.1. If you have the October 2021 PSU installed, detailed resolution information is also available from within the console. Select a warning message in the Security Warnings Table and then click View Details. Click the link beside More Information to see guidance on how to resolve the warning.

Although Oracle recommends resolving the warnings by changing the domain configuration setting, you may determine that based on your security and business requirements, certain warnings do not apply to your domain. For those warnings, you can disable the relevant security configuration settings. In the WebLogic Administration Console, go to Domain > Security > Warnings. Deselect any settings for which you do not want to see warnings.

You can also configure security configuration settings on the `SecureMode` MBean using WLST by navigating to the domain configuration and setting the relevant attributes to true or false. For example, using WLST:

```
edit()
startEdit()
cd("SecurityConfiguration/mydomain/SecureMode/mydomain")
cmo.setWarnOnAnonymousRequests(false)
activate()
```

The Certificate Expiry for identity and trust attributes can be configured through the `SecurityConfiguration` MBean.

WebLogic Server always verifies if your domain has the minimum required JDK version; you cannot disable the JDK version check.

Some level of security validation occurs in all domain modes. Validation is most strict in secured production mode and least strict in development mode. In secured production mode, almost all security configuration settings are enabled by default. [Table 3-6](#) lists the security configuration settings.

Domains are scanned every 24 hours. You can also run the scan manually as needed.

 **Note:**

Do not rely on the Security Warnings Report alone to determine the security of your domain. While these security configuration settings cover a broad set of potential security issues, other security issues that do not generate warnings may still exist in your domain.

Table 3-6 Security Validation Checks

| Security Configuration Setting | Description | Applicable Domain Mode |
|---|---|------------------------|
| Warn on Patches | Issues a warning if the domain does not have the latest WebLogic Server or Coherence critical patch update. | Production mode |
| Warn on Anonymous Requests | Issues a warning if anonymous request configuration attributes (<code>RemoteAnonymousRMIT3Enabled</code> , <code>RemoteAnonymousRMIIIOPEEnabled</code>) are not disabled. | Production mode |
| Check Identity Certificates | Issues a warning if Identity certificates are set to expire within the period specified by the Number of days before expiration for warnings configuration setting. | Production mode |
| Check Trust Certificates | Issues a warning if Trust certificates are set to expire within the period specified by the Number of days before expiration for warnings configuration setting. | Production mode |
| Number of days before expiration for warnings | Enter (in days) how early WebLogic Server should warn of impending Identity or Trust certification expiration. | Production mode |
| Number of days between certificates checking | Enter (in days) how often WebLogic Server should check if the Identity or Trust certificates are set to expire. | Production mode |
| Warn on Insecure SSL | Issues a warning if SSL/TLS configuration is insecure. This includes checking for host verification, SSL versions, constraints, and so on. | Production mode |
| Warn on Insecure File System | Issues a warning if the file permissions in the domain directory are insecure. | Production mode |
| Warn on Insecure Ports | Issues a warning if the network port configuration is insecure. | Production mode |
| Warn on User Lockout | Issues a warning if user lockout settings are not secure. | Production mode |

Table 3-6 (Cont.) Security Validation Checks

| Security Configuration Setting | Description | Applicable Domain Mode |
|--------------------------------|--|-------------------------|
| Warn on Username Passwords | Issues a warning if usernames or passwords do not meet recommended complexity standards. | Production mode |
| Warn on Insecure Applications | Issues a warning if applications are not secure. | Production mode |
| Warn on Auditing | Issues a warning if auditing is not enabled. | Secured production mode |

Secure the Network

Secure the network in the production environment by using software and hardware to create firewalls, components such as network channels to isolate incoming and outgoing application traffic, and connection filters to deny access at the network level.

As part of securing the network, be sure to enable the administration port to limit all administrative traffic between server instances in a WebLogic Server domain to a single port. See [Configure an Administration Port for the Domain](#).

Topics include:

- [Configure Firewalls](#)
- [Configure Connection Filters](#)
- [Configure Timeouts](#)
- [Configure Sockets and File Descriptors](#)
- [Configure SSL/TLS](#)
- [Use JEP 290 to Restrict Incoming Serialized Java Objects](#)
- [Disable Remote Anonymous RMI T3 and IIOP Requests](#)

Configure Firewalls

A firewall controls network traffic by acting as a barrier between a trusted and an untrusted network. Along with firewalls, you can use network channels, an administration port, WebLogic Server connection filters, and perimeter authentication to restrict access to resources based on user and network information.

Oracle strongly recommends that you:

- Configure a HTTPS protocol network channel to segregate HTTPS application traffic. Doing so ensures that HTTPS application traffic will run on a dedicated port by itself. Configure the firewall to allow external access to the HTTPS port, but block external access to any of the non-HTTPS ports.
- Configure internal channels for non-HTTPS protocols and use firewalls so that the internal channels are accessible only to trusted client IP addresses.
- Do not enable tunneling on channels.

Topics

- [Configure Network Channels and Firewalls to Prevent Access from Non-HTTPS Traffic](#)
- [Configure Firewall to Prevent Access to Internal Applications](#)
- [Configure Firewall for Cluster Communication](#)

Configure Network Channels and Firewalls to Prevent Access from Non-HTTPS Traffic

Oracle strongly recommends that you use a combination of network channels and firewalls to restrict external access to only HTTPS application traffic and that you block external access of non-HTTPS traffic (T3/T3s/IOP/IOPs).

Network channels define the attributes of a network connection to WebLogic Server, such as the protocol the network supports, the listen address, listen ports for secure and non-secure communication, and so on. Using network channels allow administrators to have more control over exposing network access to WebLogic Server. See *Understanding Network Channels in Administering Server Environments for Oracle WebLogic Server*.

Once you have defined a network channel, you can further isolate the network connections for that channel using a load balancer or firewall.

- To restrict the use of T3/T3s/IOP/IOPs protocols to *only* WebLogic servers and clients that are behind the firewall:
 1. Create a network channel to support only HTTPS traffic coming from the external applications. For the steps required to create a network channel, see [Configure custom network channels](#) in *Oracle WebLogic Server Administration Console Online Help*
 2. Configure the firewall so that the network channel that you created in the previous step is available externally, and that the default network channel and other customer internal channels are only accessible internally. Refer to your firewall documentation for the required steps.
 3. Do not enable tunneling on the externally available network channel. Tunneling is *not* enabled by default.
- If you already have existing network channels for HTTPS traffic from external applications, Oracle strongly recommends that you disable tunneling to avoid a T3 or IOP call being wrapped inside the HTTPS protocol. If your existing network channel enables tunneling, disable it using the WebLogic Server Administration Console:
 1. Select the Server.
 2. Go to Protocols->Channels.
 3. Select the desired external channel.
 4. Clear the Tunneling Enabled checkbox.
 5. Save and activate the changes.

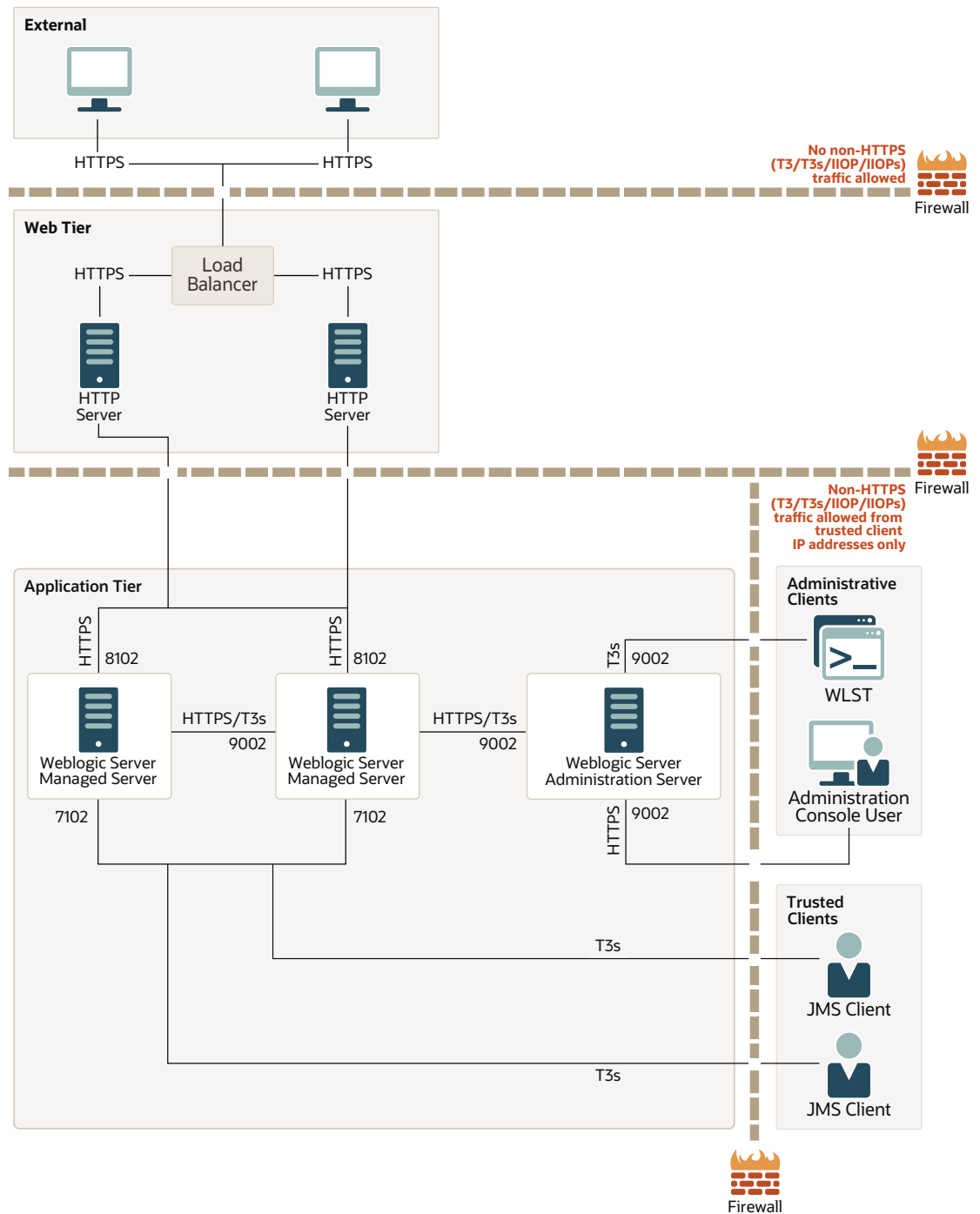
The following diagram represents a secure WebLogic Server domain configuration using firewalls, network channels, and the administration port. This configuration includes:

- An external tier where users access the web tier through a firewall which is open only to HTTPS traffic. The firewall is configured to block access from non-HTTPS protocols such as T3/T3s/IOP, and IOPs.

- A web tier that consists of a load balancer and two HTTP servers. A firewall between the web tier and the application tier is configured to allow HTTPS traffic on port 8102 only.
- An application tier that includes a WebLogic Server domain configured with an Administration Server and two Managed Servers. The domain is configured using:
 - An administration port enabled and configured to use port 9002 (the default in secured production mode). The administration port separates administration traffic from application traffic in the domain and is used by each Managed Server in the domain exclusively for communication with the Administration Server. For more information about using an administration port, see [Configure an Administration Port for the Domain](#).
 - Two network channels:
 - * One network channel is configured on port 7102 to support only T3s traffic coming from trusted clients.
 - * A second network channel is configured on port 8102 to support only HTTPS traffic coming from the external applications through the firewall.

You can specify any available port number for the network channels.
- A firewall between the application tier and trusted application clients that is configured to allow administration traffic on port 9002 and T3s traffic on port 7102. Within the internal firewall:
 - Administrators in a trusted administrator group use WLST and the Administration Console with a set of trusted IP addresses to communicate with the Administration Server using the administration port 9002.
 - Trusted JMS and EJB clients running on a set of trusted IP addresses use the T3s protocol on port 7102 to communicate with the Managed Servers.

Figure 3-2 WebLogic Server Secure Configuration



Configure Firewall to Prevent Access to Internal Applications

Enable the Administration port for your domain, and configure a firewall to prevent external access to internal applications accessible on the Administration port. Using both the administration port and the firewall ensures that internal applications such as the WebLogic Server Administration Console and RESTful services cannot be accessed externally.

To block access to internal applications:

1. Ensure that you have disabled any unused internal applications as described in [Disable Unused Internal Applications](#).
2. Configure a firewall to limit access to internal applications that are accessible on the non-Administration ports, such as SAML and web services. To do so, disable access to the appropriate context paths.

The following table lists the WebLogic Server internal applications and their context paths.

Table 3-7 WebLogic Server Internal Applications Context Paths

| Internal Application | Administration Port Only (if enabled) | Context Path | Description |
|--|---------------------------------------|------------------------------|--|
| File Distribution | Yes | bea_wls_management_internal2 | Used for distributing the initial LDAP data to a Managed Server. Only Managed Servers access this internal application. |
| WebLogic Server Administration Console | Yes | console, console-help | Used for management and monitoring. WebLogic Administrators, Deployers, Monitors, and Operators access the console from browsers on their client machines. Note that the console context path can be changed by the ConsoleContextPath attribute on the DomainMBean. Your firewall configuration must match the default or, if specified, the value in <code>config.xml</code> . |
| WebLogic Server Test Client | Yes | wls_utc | Used to test web services without the need to write client code. The test client is disabled in production mode. WebLogic developers access this application from browsers on their client machines. |
| RESTful Services | Yes | wls-management-services | Provides the REST API functionality used for management and monitoring. WebLogic Administrators, Deployers, Monitors, and Operators access the RESTful services from their client machines. |

Table 3-7 (Cont.) WebLogic Server Internal Applications Context Paths

| Internal Application | Administration Port Only (if enabled) | Context Path | Description |
|----------------------------|---------------------------------------|---|--|
| Deployment Service | Yes | bea_wls_deployment_internal/DeploymentService | Used to coordinate deployment and activate changes between the Administration Server and Managed Servers. This web application may be called by WLST or <code>weblogic.Deployer</code> clients to upload the application archive or plan. WebLogic Administration Servers and Managed Servers access this application. WebLogic Administrators, Deployers and Operator access this application using WLST and <code>weblogic.Deployer</code> on their client machines. |
| Cluster servlet | Yes | bea_wls_cluster_internal | Used for cluster communication including replication, saving state, and session recovery. Only cluster members use this API. |
| Internal servlets | No | bea_wls_internal | Used for tunneling RMI/IOP over HTTP. This application is disabled by default. Managed Servers and WebLogic Server clients running on client machines access this application. |
| Web service async response | No | _async | Contains the web service Async Response Service. This application is disabled by default. A WebLogic Server JAX-RPC asynchronous application client (for example WS-RM) accesses this application when the client runs within a WebLogic Server server application. |

Table 3-7 (Cont.) WebLogic Server Internal Applications Context Paths

| Internal Application | Administration Port Only (if enabled) | Context Path | Description |
|---------------------------|---------------------------------------|--------------|--|
| Web Service AT app | No | wls-wsat | Contains the WebLogic Server Web Services Atomic Transactions Service. This application serves as the transaction coordinator. Web service clients running on client machines access this application. |
| Classloader Analysis Tool | Yes | wls-cat | A web-based class analysis tool which simplifies filtering classloader configuration and aids you in analyzing classloading issues, such as detecting conflicts, debugging application classpaths and class conflicts, and proposes solutions to help you resolve them. This application is disabled in production domains. WebLogic application developers access this application from browsers on their client machines. |
| SAML ITS Apps Basic | No | samlits_ba | Supports the Intersite Transfer Service for basic authentication. This application is only enabled if the appropriate FederationServiceMBean IntersiteTransferURIs are configured. Application Single Sign-On (SSO) integration functions, SAML partners, and application users using web browsers can access these endpoints for SAML Single Sign-On (SSO) support with deployed applications. |

Table 3-7 (Cont.) WebLogic Server Internal Applications Context Paths

| Internal Application | Administration Port Only (if enabled) | Context Path | Description |
|----------------------|---------------------------------------|--------------|---|
| SAML ITS Apps Cert | No | samlits_cc | <p>Supports the Intersite Transfer Service for client cert authentication. This application is only enabled if the appropriate <code>FederationServiceMBean</code> <code>IntersiteTransferURIs</code> are configured.</p> <p>Application Single Sign-On (SSO) integration functions, SAML partners, and application users using web browsers can access these endpoints for SAML Single Sign-On (SSO) support with deployed applications.</p> |
| SAML ACS Apps | No | samlacs | <p>Supports the SAML Assertion Consumer Service. This application is only enabled if appropriate <code>FederationServiceMBean</code> <code>AssertionConsumerURIs</code> are configured.</p> <p>Application Single Sign-On (SSO) integration functions, SAML partners, and application users using web browsers can access these endpoints for SAML Single Sign-On (SSO) support with deployed applications.</p> |
| SAML ARS App | No | samlars | <p>Listens for incoming assertion retrieval requests. This application is only enabled if <code>FederationServicesMBean</code> <code>AssertionRetrievalURIs</code> are configured for the <code>samlars</code> application.</p> <p>Application Single Sign-On (SSO) integration functions, SAML partners, and application users using web browsers can access these endpoints for SAML Single Sign-On (SSO) support with deployed applications.</p> |

Table 3-7 (Cont.) WebLogic Server Internal Applications Context Paths

| Internal Application | Administration Port Only (if enabled) | Context Path | Description |
|----------------------|---------------------------------------|--------------|--|
| SAML2 Application | No | saml2 | Contains the services used for SAML 2 support. This includes the SP Initiator, IdP SSO service, SP Assertion Consumer Service, and Artifact Resolution Service. This application is only enabled if <code>SingleSignOnServicesMBean</code> <code>ServiceProviderEnabled</code> or <code>IdentityProviderEnabled</code> attributes are set to true. Application Single Sign-On (SSO) integration functions, SAML partners, and application users using web browsers can access these endpoints for SAML Single Sign-On (SSO) support with deployed applications. |

Configure Firewall for Cluster Communication

It is important to understand the communication between servers in a cluster so that you can configure firewalls appropriately.

WebLogic Server allows you to configure either multicast or unicast communication between cluster members. A firewall should allow the cluster network traffic from subnets with cluster members, but prevent it from other subnets. For more information about communications within a cluster, see *Communications In a Cluster in Administering Clusters for Oracle WebLogic Server*. In some cases, more complex port splitting may be required, especially if you use JMS or EJBs. In such cases, more than two ports may be necessary. Port splitting gives you the flexibility to define different firewall rules for different protocols. For example, if the IP of the remote client using the non-HTTPS protocol is known, a firewall rule based on that IP can be configured, assuming that the relevant non-HTTPS protocol is appropriately split out to its own port.

See *Security Options for Cluster Architectures in Administering Clusters for Oracle WebLogic Server*.

Configure Connection Filters

In addition to creating firewalls, use WebLogic Server connection filters to limit incoming connections.

When you use a connection filter, the connections to ports exposed externally come only from expected front-end hosts, and connections for administration traffic come only from the expected subnets where other WebLogic Servers or Administration Consoles are running.

Connection filters are most appropriate when the machines in a WebLogic Server domain can access each other without going through a firewall. For example, you might use a firewall to limit traffic from outside the network, and then use WebLogic Server connection filters to limit traffic behind the firewall.

In a single server configuration, Oracle strongly recommends that you close off the embedded LDAP listen port using a connection filter to protect the embedded LDAP port against brute force attacks. While this does not protect the embedded LDAP port in a multiple server configuration, the default connection filter implementation supports filtering based on the source IP address which should be used to allow access only from servers that are part of the domain. As a result, only the machines in the domain can access the LDAP port.

For details about configuring connection filters, see Using Connection Filters in *Administering Security for Oracle WebLogic Server*.

Configure Timeouts

To reduce the potential for Denial of Service (DoS) attacks, make sure that you restrict message size, configure complete message timeouts appropriately for your system, and limit the number of sockets allowed for a server.

Table 3-8 Configure Secure Timeouts

| Security Action | Description | More Information |
|---|---|--|
| Configure the Complete Message Timeout parameter appropriately for your system. | <p>The Complete Message Timeout parameter sets the maximum number of seconds that a server waits for a complete message to be received.</p> <p>This timeout helps guard against a Denial of Service (DoS) attack in which a caller indicates that it will be sending a message of a certain size that it never finishes sending.</p> <p>The default value for this parameter is 60 seconds, which applies to all connection protocols for the default network channel. This setting might be appropriate if the server has a number of high-latency clients. However, you should tune this to the smallest possible value without compromising system availability.</p> <p>If you need a complete message timeout setting for a specific protocol, you can alternatively configure a new network channel for that protocol.</p> | <p>For information about displaying the WebLogic Server Administration Console page from which the Complete Message Timeout parameter can be set, see Configure protocols in the <i>Oracle WebLogic Server Administration Console Online Help</i>.</p> |

Table 3-8 (Cont.) Configure Secure Timeouts

| Security Action | Description | More Information |
|---|--|--|
| Restrict the size and the time limit of requests on external channels to prevent Denial of Service attacks. | <p>To prevent some Denial of Service (DoS) attacks, WebLogic Server can restrict the size of a message as well as the maximum time it takes a message to arrive. The default setting for message size is 10 megabytes and 480 seconds for the complete message timeout. Oracle recommends that you:</p> <ul style="list-style-type: none"> • Set the size limit of requests on internal channels so that a Managed Server can accept messages from the Administration Server. • Restrict the size and time limits of requests on external channels. <p><i>Background Information:</i> A DoS attack leaves a Web site running but unusable. Hackers deplete or delete one or more critical resources of the Web site.</p> <p>To perpetrate a DoS attack on a WebLogic Server instance, an intruder bombards the server with many requests that are very large, are slow to complete, or never complete so that the client stops sending data before completing the request.</p> | <p>To configure these settings for the HTTP, T3, and IIOOP protocols refer to the following tasks in the <i>Oracle WebLogic Server Administration Console Online Help</i>:</p> <ul style="list-style-type: none"> • Configure HTTP protocol • Configure T3 Protocol • Enable and configure IIOOP <p>See also Reducing the Potential for Denial of Service Attacks in <i>Tuning Performance of Oracle WebLogic Server</i>.</p> |

Configure Sockets and File Descriptors

To prevent DoS attacks, Oracle strongly recommends that you limit the number of sockets allowed for a server. To optimize availability on UNIX systems, be sure to set the number of file descriptors consumed by sockets to a number that is appropriate for your system.

[Table 3-9](#) describes the actions that you need to take to set the number of sockets and file descriptors.

Table 3-9 Sockets and File Descriptors

| Security Action | Description | More Information |
|--|---|--|
| Set the number of sockets allowed for a server to prevent DoS attacks. | <p>To prevent some DoS attacks, limit the number of sockets allowed for a server so that there are fewer than the number of sockets allowed to the entire process. This ensures that the number of file descriptors allowed by the operating system limits is not exceeded.</p> <p>Even after the server's limit is exceeded, administrators can access the server through the Administration Port.</p> <p>You can configure this setting using the <code>MaxOpenSockCount</code> flag.</p> | See Servers: Configuration: Tuning in the <i>Oracle WebLogic Server Administration Console Online Help</i> . |
| On UNIX systems, set number of file descriptors appropriately for your system. | <p>On UNIX systems, each socket connection to WebLogic Server consumes a file descriptor. To optimize availability, the number of file descriptors for WebLogic Server must be appropriate for the host machine. By default, WebLogic Server configures 1024 file descriptors. However, this setting may be low, particularly for production systems.</p> <p>Note that when you tune the number of file descriptors for WebLogic Server, your changes must be in balance with any changes made to the complete message timeout parameter. A higher complete message timeout setting results in a socket not closing until the message timeout occurs, which therefore results in a longer hold on the file descriptor. So if the complete message timeout setting is high, the file descriptor limit must also be set high. This balance provides optimal system availability with reduced potential for DoS attacks.</p> | <ul style="list-style-type: none"> For more information about the complete message timeout parameter, see Configure Timeouts. For information about tuning the number of available file descriptors, consult your UNIX vendor's documentation. |

Configure SSL/TLS

To prevent sensitive data from being compromised, secure data transfers using SSL/TLS. SSL/TLS provides secure connections by allowing two applications connecting over a network to authenticate each other's identity and by encrypting the data exchanged between the applications.

Oracle strongly recommends that you configure SSL/TLS for the administration port, network channels, database connections, LDAP server connections, and other resources handling communication that must be secured. In particular, make sure that connections to remote

server instances in the domain are secured with SSL/TLS. The specific components for which either one- or two-way SSL/TLS needs to be configured depends on the overall topology of the production environment. For details about configuring SSL/TLS, see *Configuring SSL* in *Administering Security for Oracle WebLogic Server*.

In the October 2019 PSU, WebLogic Server added the ability to enable HTTP Strict Transport Security (HSTS), which is a web security policy mechanism that allows a web server to be configured so that web browsers, or other user agents, can access the server using only secure connections, such as HTTPS. For details about enabling HSTS in this release of WebLogic Server, see the My Oracle Support document *HTTP Strict Transport Security (HSTS) in Oracle WebLogic Server (Doc ID 2146367.1)*.

An Important Note Regarding Null Cipher Use in SSL

A cipher suite is an SSL/TLS encryption method that includes the key exchange algorithm, the symmetric encryption algorithm, and the secure hash algorithm. A cipher suite is used to protect the integrity of a communication. For example, the cipher suite called `RSA_WITH_RC4_128_MD5` uses RSA for key exchange, RC4 with a 128-bit key for bulk encryption, and MD5 for message digest.

Oracle strongly recommends that you do not allow the use of unencrypted null ciphers in a production environment. SSL/TLS clients start the SSL/TLS handshake by connecting to the server. As part of the connection, the client sends the server a list of the cipher suites it supports. The server then selects a mutually-supported cipher suite from the list supplied by the client for the client and server to use for this session.

However, an incorrectly configured client might specify a set of cipher suites that contain only null ciphers. A null cipher passes data on the wire in clear-text. (An example of a cipher suite with a null cipher is `SSL_RSA_WITH_NULL_MD5`.) Using a null cipher makes it possible to see the SSL messages by using a network packet sniffer. In essence, SSL is used but does not provide any security.

The server selects the null cipher only when it is the only cipher suite they have in common. If the server selects a null cipher from the client's cipher suite list, the log contains the following message: SSL has established a session that uses a Null cipher.

This message is output only when the server has selected a null cipher from the client's list.

Note:

If there is any potential whatsoever that an SSL/TLS client might use a null cipher to inappropriately connect to the server, you should check the log file for this message. Oracle recommends that new client configurations be given extra attention with respect to the use of a null cipher to ensure that they are properly configured.

It is unlikely that an existing client configuration would suddenly start using null ciphers if it had not been doing so previously. However, an existing client configuration that is unknowingly configured incorrectly could be using null ciphers.

Other SSL/TLS errors unrelated to null ciphers are possible as well, and each will display an appropriate error message in the log.

For information on configuring SSL, see Configuring SSL in *Administering Security for Oracle WebLogic Server*. For information on viewing log files, see [View and configure logs](#) in the *Oracle WebLogic Server Administration Console Online Help*.

WebLogic Server Control to Prevent Null Cipher Use

As of release 10g Release 3 (10.3), WebLogic Server includes a WebLogic Server Administration Console control to prevent the server from using a null cipher.

The **Allow Unencrypted Null Cipher** control, which is available in the WebLogic Server Administration Console by selecting **Servers** > *ServerName* > **Configuration** > **SSL** > **Advanced**, determines whether null ciphers are allowed. By default, this control is not set and the use of a null cipher is not allowed on the server. In such a configuration, if the SSL/TLS clients want to use the null cipher suite (by indicating `SSL_RSA_WITH_NULL_MD5` as the only supported cipher suite), the SSL/TLS handshake will fail.

If you set this control, the null cipher suite (for example, `SSL_RSA_WITH_NULL_MD5`) is added to the list of supported cipher suites by the server. The SSL/TLS connection has a chance to use the null cipher suite if the client wants to do so. If the null cipher suite is used, the message will be unencrypted.

Caution:

Do not set this control in a production environment unless you are aware of the implications and consequences of doing so.

This control is also exposed as a system runtime parameter, `weblogic.security.SSL.allowUnencryptedNullCipher`, and as an [AllowUnencryptedNullCipher](#) attribute on the `SSLMBean`.

Use JEP 290 to Restrict Incoming Serialized Java Objects

To improve security, WebLogic Server uses the JDK JEP 290 mechanism to filter incoming serialized Java objects and limit the classes that can be deserialized. The filter helps to protect against attacks from specially crafted, malicious serialized objects that can cause denial of service (DOS) or remote code execution (RCE) attacks.

At startup, WebLogic Server configures a default JEP 290 filter that includes a set of prohibited classes and packages, and default values for some JEP 290 options.

WebLogic Server Patch Set Updates (PSUs) may include updates to the set of prohibited classes and packages used in the default filter. To ensure that your system is protected against deserialization vulnerabilities with the most current default filter, be sure to apply the latest WebLogic Server PSUs and Java Critical Patch Updates (CPUs) as soon as they are released. The [Critical Patch Updates, Security Alerts and Bulletins](#) page references the latest Java and WebLogic Server updates that are available on My Oracle Support.

For a list of the default filter settings, see support document *Restricting Incoming Serialized Java Objects to Oracle WebLogic Server (Doc ID 2421487.1)* on My Oracle Support. You can access My Oracle Support at <https://support.oracle.com/>.

The April 2021 WebLogic Server PSU adds support for dynamic blocklists, which provide the ability to update your blocklist filters by creating a configuration file that can be updated or replaced while the server is running.

 **Note:**

Oracle strongly recommends that you ensure WebLogic Server is running with a JDK version that supports JEP 290 global scope filtering, is certified with WebLogic Server, and that continues to be supported by Oracle. In this WebLogic Server release, Oracle strongly recommends that you use the following JDK update level at a minimum:

- JDK 8 Update 191 (JDK 8u191) or later

If you are using a JDK that does not support JEP 290 global scope filtering, then WebLogic Server continues to run and provide some protection against known deserialization attacks, but will not have the protection of the more advanced features of JEP 290.

You can use WebLogic Server system properties to customize, replace, or disable the filter. For details, see *Configuring a Custom JEP 290 Deserialization Filter in Administering Security for Oracle WebLogic Server*.

WebLogic Server also provides a system property, `weblogic.oif.serialFilterLogging`, that you can use to log the current blocklist classes and packages. To enable logging, start WebLogic Server with the `weblogic.oif.serialFilterLogging` system property set to `true`. The filter settings are displayed in the server log.

For more information about JEP 290, see <http://openjdk.java.net/jeps/290>.

Setting the Deserialization Timeout Interval

You can further strengthen your protection against potential denial of service attacks by setting a time limit on deserialization. When the time limit elapses, the deserialization process is automatically terminated.

The April 2022 Patch Set Update (PSU) adds support for the `weblogic.rmi.stream.deserialization.timelimitmillis` system property .

By default, the time limit is disabled and not enforced when deserializing Java objects. To add a limit, set your desired time interval, in milliseconds, using the `weblogic.rmi.stream.deserialization.timelimitmillis` system property.

Enter an interval of 100 ms or longer. Very short intervals may prevent deserialization from operating smoothly.

For example, to set a time limit of 10 seconds, use -
`Dweblogic.rmi.stream.deserialization.timelimitseconds=10000`.

Enter 0 to disable the time limit.

Disable Remote Anonymous RMI T3 and IIOP Requests

By default, WebLogic Server allows clients to perform anonymous RMI requests. The April 2021 PSU added the ability to disable anonymous requests from clients.

The ability to disable anonymous requests from clients provides two benefits:

- Unauthenticated clients are rejected and are not allowed to invoke on WebLogic Server.
- If anonymous requests are disabled, then additional JEP 290 filtering is performed and helps protect against deserialization exploits.

To disable anonymous RMI T3 and IIOp requests, do one of the following:

- Use the WebLogic Server Administration console to disable the remote anonymous RMI T3 and IIOp requests:

 **Note:**

Console support to disable the remote anonymous RMI T3 and IIOp requests was added in the July 2021 PSU.

1. In the Change Center of the Administration Console, click **Lock & Edit**.
 2. In the left pane of the console, under **Domain Structure**, select the domain name.
 3. Select **Security>General**, then expand the **Advanced** node.
 4. Clear the **Remote anonymous RMI access via IIOp** and **Remote anonymous RMI access via T3** check boxes.
 5. Click **Save**, then in the Change Center, click **Activate Changes**.
- Use WLST to set the `RemoteAnonymousRMIT3Enabled` and `RemoteAnonymousRMIIIOPEEnabled` attributes to `false` to disable anonymous requests. (The default is `true`.) For example, using WLST online:

```
edit()
startEdit()
cd("SecurityConfiguration/mydomain")
cmo.setRemoteAnonymousRMIIIOPEEnabled(false)
cmo.setRemoteAnonymousRMIT3Enabled(false)
activate()
```

- Set the `RemoteAnonymousRMIT3Enabled` and `RemoteAnonymousRMIIIOPEEnabled` system properties to `false` when starting WebLogic Server. For example:

```
-Dweblogic.security.remoteAnonymousRMIT3Enabled=false
-Dweblogic.security.remoteAnonymousRMIIIOPEEnabled=false
```

 **Note:**

Although use of these system properties will disable remote anonymous T3 and IIOp access, the security validation infrastructure delivered in the WebLogic Server July 2021 PSU may falsely warn that remote anonymous T3 and IIOp access is enabled. To resolve this warning, follow the instructions for disabling remote anonymous T3 and IIOp access using the WebLogic Server Administration Console or WLST as described above.

You cannot disable remote anonymous RMI T3 and IIOp requests if any of the following is used in your WebLogic Server environment:

- T3 or IIOP clients that do not pass credentials (username and password) when creating a JNDI initial context to WebLogic Server
- T3 clients that use the deprecated `weblogic.rmi` APIs
- Clients that utilize the `weblogic.j2eeclient.Main` API
- Environments that configure inter-domain transaction communication with Security Interoperability Mode set to `performance` or `default` (when an administrative channel is not configured). If you want to disable Anonymous RMI T3 and IIOP requests, Oracle recommends that you enable Cross Domain Security for inter-domain communication. See *Configuring Secure Inter-Domain and Intra-Domain Transaction Communication in Developing JTA Applications for Oracle WebLogic Server*.

Disabling remote anonymous requests when they are required in your environment will result in the anonymous requests being rejected and <BEA-000582> and <BEA-002045> errors will be logged in the server log.

Avoid Using These Configurations and Settings in a Locked Down Environment

Oracle strongly recommends that you avoid using configurations and settings that are not secure, such as development mode and demonstration certificates, and that you do not disable default secure settings designed to protect your environment.

Table 3-10 Configurations and Settings that You Must Not Use in a Locked Down Environment

| Configuration/Setting | Description | More Information |
|--|--|---|
| Do not enable tunneling on channels that are available external to the firewall. | If you allow tunneling, then the external client can send T3/IIOP traffic which can contribute to T3/RMI serialization security vulnerabilities. | <ul style="list-style-type: none"> • Configure Network Channels and Firewalls to Prevent Access from Non-HTTPS Traffic |

Table 3-10 (Cont.) Configurations and Settings that You Must Not Use in a Locked Down Environment

| Configuration/Setting | Description | More Information |
|---|--|---|
| Do not run WebLogic Server in development mode in a production environment. | <p>Production mode or secured production mode sets the server to run with settings that are more secure and appropriate for a production environment. Oracle strongly recommends that you enable secured production mode to ensure high security standards for your production environment.</p> <p>Caution:</p> <p>When WebLogic Server is configured in development mode, certain error conditions, such as a misbehaving application or an invalid configuration of WebLogic Server, may result in a trace stack being displayed. While error responses generally are not dangerous, they have the potential to give attackers information about the application or the WebLogic Server installation that can be used for malicious purposes. However, when you configure WebLogic Server in production mode or secured production mode, stack traces are not generated; therefore, you must never run WebLogic Server in development mode in a production environment.</p> | <ul style="list-style-type: none"> • Configure Secured Production Mode |

Table 3-10 (Cont.) Configurations and Settings that You Must Not Use in a Locked Down Environment

| Configuration/Setting | Description | More Information |
|-------------------------|--|---|
| Do not use MLet MBeans. | <p>MLet (Management applet) MBeans allow a client user to upload the MBean implementation and then execute that implementation in WebLogic Server. Since any authenticated user can instantiate and invoke on them, WebLogic Server disables the use of MLet MBeans by default with the <code>ManagementAppletCreateEnabled</code> attribute of the JMX MBean.</p> <p>Oracle strongly recommends that you do not enable the use of MLet MBeans. If you choose to enable MLet MBeans, then you must ensure that only authorized users can access the MLet MBeans by running with the Java security manager and using permissions to restrict access to the MLet MBeans. To grant MBean register permissions for the <code>javax.management.loading.MLet</code> MBean to authorized users with Administrator or Deployer roles, use the grant principal <code>weblogic.security.principal.WLSPolicyFileGroupPrincipalImpl</code> "Administrators" and "Deployers" element.</p> | <p>See WLSPolicyFileGroupPrincipalImpl in <i>Java API Reference for Oracle WebLogic Server</i>.</p> |

Table 3-10 (Cont.) Configurations and Settings that You Must Not Use in a Locked Down Environment

| Configuration/Setting | Description | More Information |
|--|--|--|
| Do not disable security constraints on digital certificates. | <p>When communicating by SSL, by default WebLogic Server rejects any digital certificates in a certificate chain that do not have the Basic Constraint extension defined by the Certificate Authority. This level of enforcement protects your Web site from the spoofing of digital certificates.</p> <p>Make sure that no server startup command includes the following option, which disables this enforcement:</p> <p>-</p> <pre>Dweblogic.security.SSL.enforceConstraints=false</pre> <p>Note: If secured production mode is enabled for your domain, then WebLogic Server logs a warning if the <code>weblogic.security.SSL.enforceConstraints</code> system property value is set to <code>false</code>.</p> | See <i>SSL Certificate Validation in Administering Security for Oracle WebLogic Server</i> . |
| Do not use the demonstration digital certificates in a production environment. | <p>WebLogic Server includes a set of demonstration private keys, digital certificates, and trusted certificate authorities that are for development only. Everyone who downloads WebLogic Server has the private keys for these digital certificates. Do not use the demonstration identity and trust.</p> | <ul style="list-style-type: none"> • Configure keystores in the <i>Oracle WebLogic Server Administration Console Online Help</i> • Configuring SSL in <i>Administering Security for Oracle WebLogic Server</i> |

Table 3-10 (Cont.) Configurations and Settings that You Must Not Use in a Locked Down Environment

| Configuration/Setting | Description | More Information |
|--|--|---|
| Do not use the SNMPv1 and SNMPv2 protocols. | <p>By default, Simple Network Management Protocol (SNMP) is disabled in WebLogic Server. However, once you enable SNMP, the SNMPv1 and SNMPv2 protocols are enabled. SNMPv1 and SNMPv2 are not secure and can cause certain potential security problems to occur on the SNMP service, including unauthorized access and Denial of Service attacks.</p> <p>Oracle strongly recommends disabling the SNMPv1 and SNMPv2 protocols and using the SNMPv3 protocol instead. When using the SNMPv3 protocol, additional security configuration is required because both the SNMP agent and manager must encode identical credentials in their protocol data units (PDUs) for the communication to succeed. If you cannot use SNMPv3, you must limit the weak security problems in SNMP v1 and SNMPv2 by ensuring that your network is secure and that the firewall is configured to restrict access to the ports in your WebLogic Server environment.</p> | <p>See the following topics for details and configuration information:</p> <ul style="list-style-type: none"> • Security for SNMP in <i>Monitoring Oracle WebLogic Server with SNMP</i>. • Secure SNMPv3 communication in the <i>Oracle WebLogic Server Administration Console Online Help</i>. |
| Do not use SSLv2, SSLv3, TLSv1.0, TLSv1.1 protocol versions. | <p>TLS v1.1 is the default minimum protocol version configured in this release of WebLogic Server. However, Oracle strongly recommends that you use TLS v1.2 or later in a production environment, and that you do not use TLS v1.0 and v1.1.</p> | <p>See Specifying the SSL Protocol Version in <i>Administering Security for Oracle WebLogic Server</i>.</p> |

Table 3-10 (Cont.) Configurations and Settings that You Must Not Use in a Locked Down Environment

| Configuration/Setting | Description | More Information |
|---|--|---|
| Do not enable remote access to the JVM platform MBean server. | <p>The JDK provides an MBean server (the platform MBean server) and a set of MBeans that contain monitoring information about the JVM. You can configure the WebLogic Server Runtime MBean Server to run as the platform MBean server, which enables JMX clients to access the JVM MBeans and WebLogic Server MBeans from a single MBean server connection.</p> <p>Remote access to the platform MBean server can be secured only by standard JDK security features (see http://docs.oracle.com/javase/8/docs/technotes/guides/management/agent.html). If you have configured the WebLogic Server Runtime MBean Server to be the platform MBean server, enabling remote access to the platform MBean server creates an access path to WebLogic Server MBeans that is not secured through the WebLogic Server security framework.</p> <p>If it is essential that remote JMX clients have access to the JVM MBeans, Oracle recommends that you access them through the WebLogic Server Runtime MBean Server.</p> | <p>Registering MBeans in the JVM Platform MBean Server in <i>Developing Manageable Applications Using JMX for Oracle WebLogic Server</i>.</p> |

Table 3-10 (Cont.) Configurations and Settings that You Must Not Use in a Locked Down Environment

| Configuration/Setting | Description | More Information |
|--|--|--|
| Do not disable host name verification. | <p>By default, the WebLogic SSL implementation validates that the host to which a connection is made is the intended or authorized party. However, during the implementation of WebLogic Server at your site, you might have disabled host name verification:</p> <p>-</p> <pre>Dweblogic.security.SSL.ignoreHostnameVerification=true</pre> <p>Background Information: A man-in-the-middle attack occurs when a machine inserted into the network captures, modifies, and retransmits messages to the unsuspecting parties. One way to avoid man-in-the-middle attacks is to validate that the host to which a connection is made is the intended or authorized party. An SSL client can compare the host name of the SSL server with the digital certificate of the SSL server to validate the connection. The WebLogic Server HostName Verifier protects SSL connections from man-in-the-middle attacks.</p> <p>Note: If secured production mode is enabled for your domain, then WebLogic Server logs a warning if host name verification is disabled.</p> | <p>Using Host Name Verification in <i>Administering Security for Oracle WebLogic Server</i>.</p> <p>To enable host name verification if it is disabled, see Configure a custom host name verifier in the <i>Oracle WebLogic Server Administration Console Online Help</i>.</p> |
| Do not enable network classloading. | <p>The <code>network-class-loading-enabled</code> element in the central domain configuration file controls whether a server can attempt to load classes from the network. By default, this is set to false, preventing the server from loading classes remotely. If you enable <code>network-class-loading-enabled</code>, it exposes WebLogic Server to remote code execution vulnerabilities.</p> | <p>Overview of Domain Configuration Files in <i>Understanding Domain Configuration for Oracle WebLogic Server</i>.</p> |

Secure Applications

Although much of the responsibility for securing resources in a WebLogic domain fall within the scope of the server, some security responsibilities lie within the scope of individual applications.

For some security options, the WebLogic Security Service enables you to determine whether the server or individual applications are responsible for those settings. For

each application that you deploy in a production environment, review the items in the following table to verify that you have secured its resources.



Note:

The HTTP Publish-Subscribe server included in WebLogic Server has specific lockdown steps, which are described in *Using the HTTP Publish-Subscribe Server* in *Developing Web Applications, Servlets, and JSPs for Oracle WebLogic Server*.

Table 3-11 Securing Applications

| Security Action | Description |
|--|---|
| Determine which deployment model secures your Web applications and EJBs. | <p>By default, each Web application and EJB uses deployment descriptors (XML files) to declare its secured resources and the security roles that can access the secured resources.</p> <p>Instead of declaring security in Web application and EJB deployment descriptors, you can use the WebLogic Server Administration Console to set security policies that secure access to Web applications and EJBs. This technique provides a single, centralized location from which to manage security for all Web applications and EJBs.</p> <p>You can combine these two techniques and configure WebLogic Server to copy security configurations from existing deployment descriptors upon the initial deployment of a URL (Web) or EJB resource. Once these security configurations are copied, the WebLogic Server Administration Console can be used for subsequent updates.</p> <p>See <i>Options for Securing Web Application and EJB Resources</i> in <i>Securing Resources Using Roles and Policies for Oracle WebLogic Server</i>.</p> |
| Set the <code>FrontendHost</code> attribute on the <code>WebServerMBean</code> or <code>ClusterMBean</code> to prevent redirection attacks | <p>When a request on a web application is redirected to another location, the <code>Host</code> header contained in the request is used by default in the <code>Location</code> header of the response. Because the <code>Host</code> header can be spoofed — that is, corrupted to contain a different host name and other parameters — this behavior can be exploited to launch a redirection attack on a third party.</p> <p>To prevent the likelihood of this occurrence, set the <code>FrontendHost</code> attribute on either the <code>WebserverMBean</code> or <code>ClusterMBean</code> to specify the host to which all redirected URLs are sent. The host specified in the <code>FrontendHost</code> attribute will be used in the <code>Location</code> header of the response instead of the one contained in the original request.</p> <p>See <code>FrontendHost</code> in <i>MBean Reference for Oracle WebLogic Server</i>.</p> |
| Use JSP comment tags instead of HTML comment tags. | <p>Comments in JSP files that might contain sensitive data and or other comments that are not intended for the end user should use the JSP syntax of <code><%/* xxx */%></code> instead of the HTML syntax <code><!-- xxx --></code>. The JSP comments, unlike the HTML comments, are deleted when the JSP is compiled and therefore cannot be viewed in the browser.</p> |
| Do not install uncompiled JSPs and other source code on the production machine. | <p>Always keep source code off of the production machine. Getting access to your source code allows an intruder to find security holes.</p> <p>Consider precompiling JSPs and installing only the compiled JSPs on the production machine. See <i>Precompiling JSPs</i> in <i>Developing Web Applications, Servlets, and JSPs for Oracle WebLogic Server</i>.</p> |

Table 3-11 (Cont.) Securing Applications


| Security Action | Description |
|---|---|
| Configure your applications to use SSL. | <p>Set the <code>transport-guarantee</code> to <code>CONFIDENTIAL</code> in the <code>user-data-constraint</code> element of the <code>web.xml</code> file whenever appropriate.</p> <p>See <code>security-constraint</code> in <i>Developing Web Applications, Servlets, and JSPs for Oracle WebLogic Server</i>.</p> |
| Do not use the <code>Servlet</code> servlet. | <p>Oracle does not recommend using the <code>Servlet</code> servlet in a production environment.</p> <p>Instead, map servlets to URIs explicitly. Remove all existing mappings between WebLogic servlets and the <code>Servlet</code> servlet from all Web applications before using the applications in a production environment.</p> <p>For information on mapping servlets, see <i>Configuring Servlets in Developing Web Applications, Servlets, and JSPs for Oracle WebLogic Server</i>.</p> |
| | <div style="border: 1px solid #0070C0; padding: 10px; background-color: #E6F2FF;"> <p> Note:</p> <p>When your domain is running in secured production mode, the Web application container logs a warning if the <code>Servlet</code> servlet is used by your application.</p> </div> |
| Do not leave <code>FileServlet</code> as the default servlet in a production environment. | <p>Oracle does not recommend using the <code>FileServlet</code> servlet as the default servlet in a production environment.</p> <p>See <i>Setting Up a Default Servlet in Developing Web Applications, Servlets, and JSPs for Oracle WebLogic Server</i>.</p> |
| Examine applications for security. | <p>There are instances where an application can lead to a security vulnerability. Many of these instances are defined by third-party organizations such as Open Web Application Security Project (OWASP) at http://www.owasp.org/.</p> <p>Of particular concern is code that uses Java native interface (JNI) because Java positions native code outside of the scope of Java security. If Java native code behaves errantly, it is only constrained by the operating system. That is, the Java native code can do anything WebLogic Server itself can do. This potential vulnerability is further complicated by the fact that buffer overflow errors are common in native code and can be used to run arbitrary code.</p> |

Table 3-11 (Cont.) Securing Applications

| Security Action | Description |
|--|---|
| If your applications contain untrusted code, enable the Java security manager. | <p>The Java security manager defines and enforces permissions for classes that run within a JVM. In many cases, where the threat model does not include malicious code being run in the JVM, the Java security manager is unnecessary. However, when third parties use WebLogic Server and untrusted classes are being run, the Java security manager may be useful. To enable the Java security manager for a server instance, use the following Java options when starting the server:</p> <pre data-bbox="574 569 1000 621">-Djava.security.manager -Djava.security.policy[=]filename</pre> <p>See Using the Java Security Manager to Protect WebLogic Resources in <i>Developing Applications with the WebLogic Security Service</i>.</p> |
| Replace HTML special characters when servlets or JSPs return user-supplied data. | <p>The ability to return user-supplied data can present a security vulnerability called <i>cross-site scripting</i>, which can be exploited to steal a user's security authorization. See the following topics on the Open Web Application Security Project (OWASP) website:</p> <ul data-bbox="574 1224 1279 1409" style="list-style-type: none"> • <i>Input Validation Cheat Sheet</i> at https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html • <i>Cross Site Scripting Prevention Cheat Sheet</i> at https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html <p>To remove the security vulnerability, before you return data that a user has supplied, scan the data for HTML special characters. If you find any such characters, replace them with their HTML entity or character reference. Replacing the characters prevents the browser from executing the user-supplied data as HTML.</p> <p>See Securing User-Supplied Data in JSPs and Securing Client Input in <i>Developing Web Applications, Servlets, and JSPs for Oracle WebLogic Server</i>.</p> |

 **Note:**

When your domain is running in secured production mode, WebLogic Server logs a warning if security manager is not enabled. However, you can specify whether this warning should be logged or not by using the `WarnOnJavaSecurityManager` attribute contained in the `SecureModeMBean`.

Table 3-11 (Cont.) Securing Applications

| Security Action | Description |
|--|--|
| Configure WebSocket applications to use authentication and authorization and verified-origin policies. | <p>Use standard Web container authentication and authorization functionality (BASIC, FORM, CLIENT-CERT) to prevent unauthorized clients from opening WebSocket connections.</p> <p>You can also configure WebSocket applications to only accept WebSocket connections from expected origins. Apply a verified-origin policy to WebSocket applications by specifying the <code>Origin</code> HTTP header in the <code>accept</code> method of the <code>WebSocketListener</code> implementation class.</p> <p>See Securing WebSocket Applications in <i>Developing Applications for Oracle WebLogic Server</i>.</p> |
| Establish secure WebSocket connections by using the <code>wss://</code> URI. | <p>WebSocket applications should use the <code>wss://</code> URI to establish a secure WebSocket connection and prevent data from being intercepted. The <code>wss://</code> URI ensures that clients send handshake requests as HTTPS requests, encrypting transferred data by TLS/SSL.</p> <p>See Securing WebSocket Applications in <i>Developing Applications for Oracle WebLogic Server</i>.</p> |