Oracle® Enterprise Manager

Cloud Control Oracle Compliance Standards Reference

13c Release 2

E73349-03

March 2017

ORACLE

Oracle Enterprise Manager Cloud Control Oracle Compliance Standards Reference, 13c Release 2

E73349-03

Copyright © 2012, 2017, Oracle and/or its affiliates. All rights reserved.

Primary Author: Pavithra Mendon

Contributing Authors: Nicole Haba, Hozefa Palitanawala, Rajendra Pandey, Mohan Perugu, Peter Sharman, David Wolf

Contributors: Enterprise Manager Cloud Control Development Teams, Quality Assurance Teams, Customer Support Teams, and Product Management Teams

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 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 installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. 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 and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon 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, Opteron, the AMD logo, and the AMD Opteron 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

16 Oracle WebLogic Cluster Compliance Standards

17 Oracle WebLogic Domain Compliance Standards

Preface

Enterprise Manager 13*c* provides a rich and powerful compliance management framework that automatically tracks and reports conformance of managed targets to industry, Oracle, or internal standards. Enterprise Manager 13*c* ships with compliance standards for Oracle hardware and software including Database, Exadata Database Machine, Fusion Middleware, VM Manager, and more. These compliance standards validate conformance to Oracle configuration recommendations, best practices, and security recommendations.

Audience

This document is intended for administrators.

This document provides you with an understanding of the provided Oracle related compliance standards and how to go about using them. Although the Oracle compliance standards can be customized to match a user's specific requirements, the scope of this document is to explain how to use the compliance standards as provided.

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

For more information, see the following document in the Oracle Enterprise Manager Release 13*c* documentation set:

- Oracle® Enterprise Manager Lifecycle Management Administrator's Guide

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.
italic	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.

What's New in This Manual?

This section lists the highlights for Enterprise Manager 13*c* Release 2.

The list of compliance standards and compliance standard rules has been expanded to include:

- Cluster – See Cluster Compliance Standards
- Cluster ASM – See Cluster ASM Compliance Standards
- Fusion Instance – See Fusion Instance Compliance Standards
- Host – See Host Compliance Standards
- Oracle Access Management Cluster – See Oracle Access Management Cluster Compliance Standards
- Oracle Access Management Server – See Oracle Access Management Server Compliance Standards
- Oracle Database Machine – See Oracle Database Machine Compliance Standards
- Oracle Identity Manager – See Oracle Identity Manager Compliance Standards
- Oracle Identity Manager Cluster – See Oracle Identity Manager Cluster Compliance Standards
- Oracle Internet Directory – See Oracle Internet Directory Compliance Standards
- Oracle WebLogic Cluster – See Oracle WebLogic Cluster Compliance Standards
- Oracle WebLogic Domain – See Oracle WebLogic Domain Compliance Standards
- Oracle WebLogic Server – See Oracle WebLogic Server Compliance Standards
- Siebel Enterprise – See Siebel Enterprise Compliance Standards
- Systems Infrastructure Switch – See Systems Infrastructure Switch Compliance Standards
- Security Technical Implementation Guide (STIG Version 1.1) for Oracle WebLogic Server 12*c* – See Security Technical Implementation Guides
- Security Technical Implementation Guide (STIG Version 1.2) for Oracle WebLogic Server 12*c* – See Security Technical Implementation Guides

- Security Technical Implementation Guidelines (STIG) Rules Enhanced by Oracle for Oracle Databases – See Security Technical Implementation Guidelines (STIG) Rules Enhanced by Oracle
- Security Technical Implementation Guide (STIG Version 1) for Oracle HTTP Server 12.1.3– See Oracle HTTP Server

1

Introduction

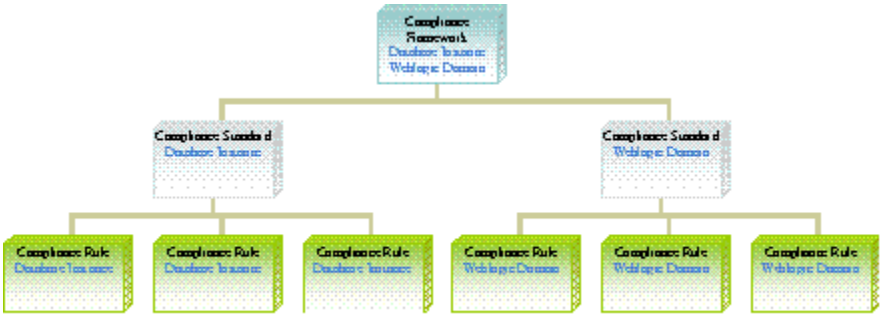
This section provides an overview of compliance, how to use compliance standards, and how to view and understand compliance results.

Enterprise Manager 13*c* provides a rich and powerful compliance management framework that automatically tracks and reports conformance of managed targets to industry, Oracle, or internal standards. Enterprise Manager 13*c* ships with compliance standards for Oracle hardware and software including Database, Exadata Database Machine, Fusion Middleware, and more. These compliance standards validate conformance to Oracle configuration recommendations, best practices, and security recommendations.

1.1 Compliance Overview

The compliance framework in Enterprise Manager 13*c* is hierarchical in nature allowing for ease of management and reuse. Starting from the top level, the hierarchy contains Compliance Frameworks, Compliance Standards, and Compliance Rules. Compliance Frameworks aggregate the compliance scores of Compliance Standards which may be for different target types. Compliance Standards contain one or more Compliance Rules but are specific to a single target type. Compliance Rules are responsible for executing a single and specific validation of a target and reporting conformance.

Figure 1-1 Compliance Framework Hierarchy



Compliance Standards are the only item associated to a target. Once associated, all rules contained in the compliance standard are executed against the data in the Enterprise Manager repository (there could be some exceptions). The compliance score for each target and the standard as a whole is a computed result based on numerous factors including number of violations, the severity of the compliance rule with the violation, the importance given to the rule in the specific compliance standard, and more. For complete information on how Compliance scores are calculated please see the Managing Compliance chapter in the *Oracle Enterprise Manager Lifecycle Management Administrator's Guide*.

1.2 Using Compliance Standards Provided by Oracle

Enterprise Manager 13*c* ships with ready-to-use compliance standards. You can choose to implement some or all of these compliance standards which consist of thousands of compliance rules.

For most of the compliance standards, you can use them out-of-the-box. However, to leverage a security standard, you must apply security monitoring templates. In other words, you must enable additional configuration collections for targets you want to associate to these compliance standards.

Oracle provides monitoring templates specifically to enable these additional collections for Database Instance (Standalone and Cluster Member), Cluster Database, Pluggable Database, and Listener. Table 1-1 lists the Oracle Certified monitoring template that can be used to enable the required configuration collections necessary for use in the Security Standards. For complete information on how to use Monitoring templates see the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

Table 1-1 Security Monitoring Templates

Target Type	Oracle Monitoring Template	Security Compliance Standard
Cluster Database	Oracle Certified-Enable RAC Security Configuration Metrics	Basic Security Configuration for Oracle Cluster Database High Security Configuration for Oracle Cluster Database Basic Security Configuration for Oracle Cluster Database Instance High Security Configuration for Oracle Cluster Database Instance
Database Instance	Oracle Certified-Enable Database Security Configuration Metrics	Basic Security Configuration for Oracle Database High Security Configuration for Oracle Database
Pluggable Database	Apply either a Real Application Cluster or Database template to a container database.	Basic Security Configuration for Oracle Pluggable Database High Security Configuration for Oracle Pluggable Database
Listener	Oracle Certified-Enable Listener Security Configuration Metrics	Basic Security Configuration for Oracle Listener High Security Configuration for Oracle Listener

Associating a Target to a Compliance Standard

You associate a target to a compliance standard using the Compliance Library page.

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Select the Compliance Standard and click the **Associate** button.
3. Choose the target to add and click **OK**.

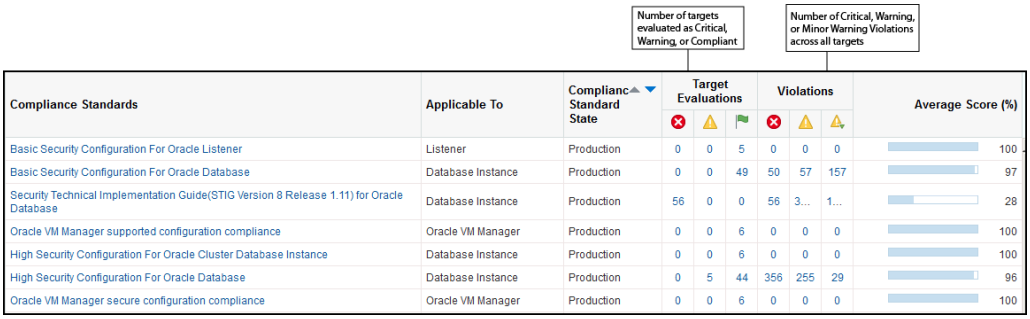
1.3 Viewing and Understanding Compliance Results

Once a Compliance Standard is associated to a specific target, the results can be seen almost immediately in the Compliance Results page. (From the **Enterprise** menu, select **Compliance**, then select **Results**.)

Results can be viewed by Compliance Framework, Compliance Standard, and Target. The Target Compliance tab shows the compliance score of a target across all compliance standards. This allows you to focus on your least compliant targets by sorting by the average score column.

Likewise the Compliance Standards tab shows the results of each Compliance Standard currently being evaluated. Compliance Standards that do not have any targets associated with them do not show in the list. It is important to understand how to interpret the different columns of the Evaluation Results page.

Figure 1-2 Compliance Standard Results



Compliance Standards	Applicable To	Compliance Standard State	Target Evaluations			Violations			Average Score (%)
Basic Security Configuration For Oracle Listener	Listener	Production	0	0	5	0	0	0	100
Basic Security Configuration For Oracle Database	Database Instance	Production	0	0	49	50	57	157	97
Security Technical Implementation Guide(STIG Version 8 Release 1.11) for Oracle Database	Database Instance	Production	56	0	0	56	3...	1...	28
Oracle VM Manager supported configuration compliance	Oracle VM Manager	Production	0	0	6	0	0	0	100
High Security Configuration For Oracle Cluster Database Instance	Database Instance	Production	0	0	6	0	0	0	100
High Security Configuration For Oracle Database	Database Instance	Production	0	5	44	356	255	29	96
Oracle VM Manager secure configuration compliance	Oracle VM Manager	Production	0	0	6	0	0	0	100

Column descriptions follow.

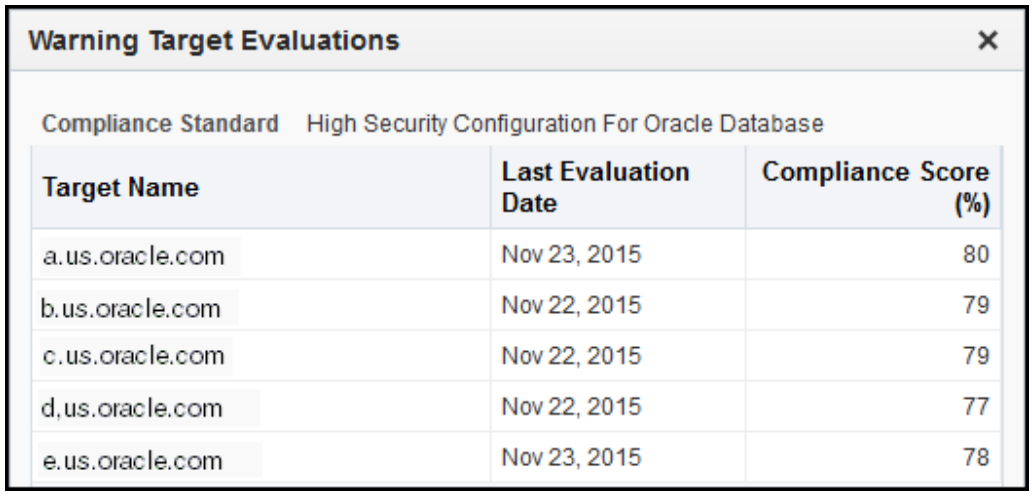
Target Evaluations

Target Evaluations

The Target Evaluation column shows how many targets evaluated with a score being Critical (less than 60), Warning (between and including 60 and 80) or Compliant (greater than 80). These levels are default and can be changed at a per target basis during the association process.

Clicking on the number in a column will show the list of targets and their specific compliance score. See Figure 1-3.

Figure 1-3 Warning Target Evaluations Details



Warning Target Evaluations

Compliance Standard High Security Configuration For Oracle Database

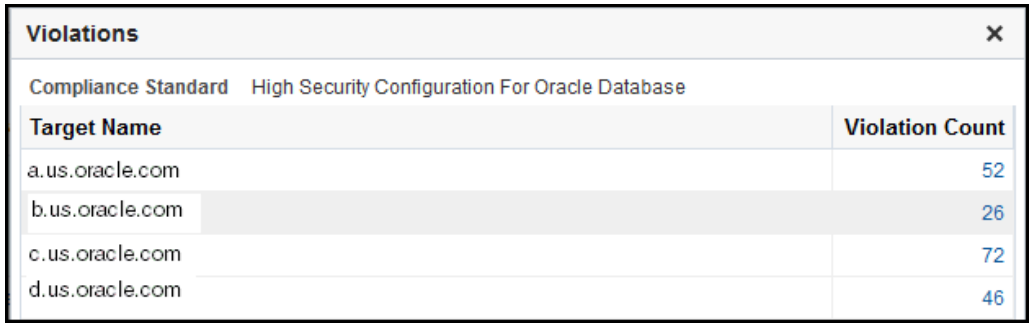
Target Name	Last Evaluation Date	Compliance Score (%)
a.us.oracle.com	Nov 23, 2015	80
b.us.oracle.com	Nov 22, 2015	79
c.us.oracle.com	Nov 22, 2015	79
d.us.oracle.com	Nov 22, 2015	77
e.us.oracle.com	Nov 23, 2015	78

Violations

The Violations columns show the number of unique violations by compliance rule severity (Critical, Warning, or Minor Warning) across all evaluated targets. It is important to remember that the number of violations is not related to the number of compliance rules in the compliance standard. Each compliance rule may generate multiple violations for a target. For example, the Secure Ports rule checks for open well known ports on hosts like SMTP(25) and FTP(21).

If a single host has both of these ports open for example, it would generate 2 different violations. Clicking on a number in a column will show the number of violations per target. See Figure 1-4.

Figure 1-4 Critical Compliance Violations



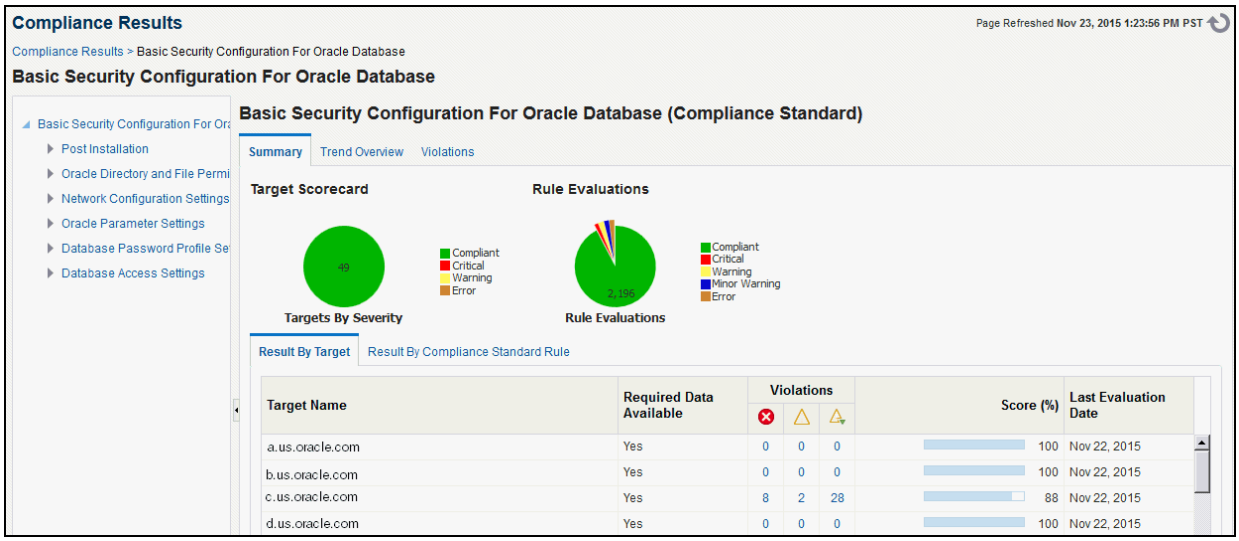
Violations

Compliance Standard High Security Configuration For Oracle Database

Target Name	Violation Count
a.us.oracle.com	52
b.us.oracle.com	26
c.us.oracle.com	72
d.us.oracle.com	46

To see details of the violations as well as historical trend information, click the **Show Details** button with a Compliance Standard highlighted.

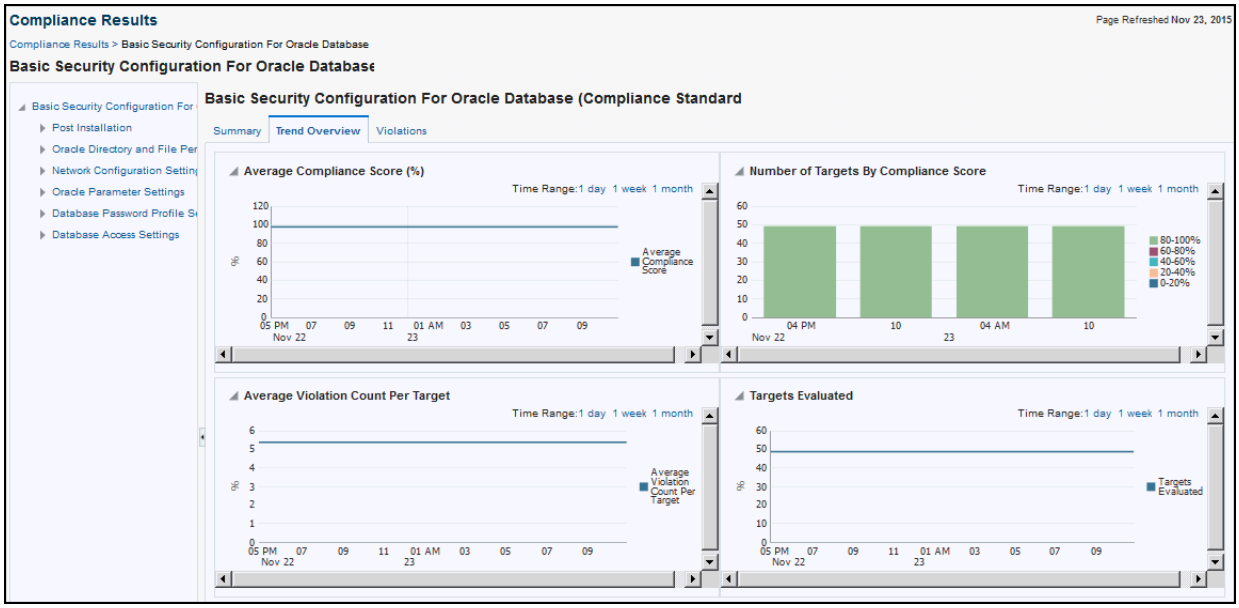
Figure 1-5 Compliance Standard Result Details - Summary



The navigator on the left allows you to select different levels of the hierarchy of the Compliance Standard to see the score at that level in the tree. The detail section at the bottom of the page shows the Results By Target or by Compliance Standard rule. The summary tab at the top shows Targets by Severity and Rule Evaluations results by severity.

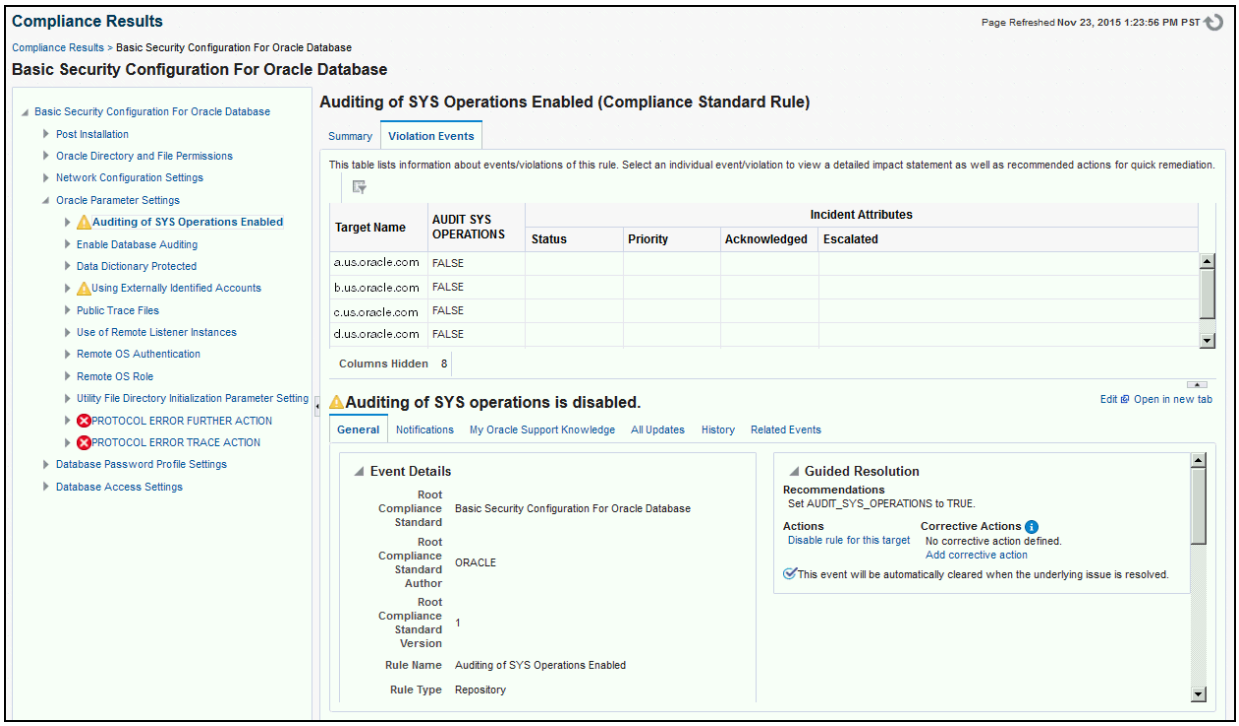
Clicking the **Trend Overview** tab shows the historical compliance metrics which can each be changed to show date ranges of 1 day, 1 week, or 1 month.

Figure 1-6 Compliance Standard Result Details - Trend Overview



When a rule having violations is selected in the navigator, a Violations Events tab displays. The table at the top shows summary information about each violation including target name and violation condition. By selecting a specific row in the table, a detailed section appears showing complete event details and guided resolution areas.

Figure 1-7 Compliance Violation Events Detail



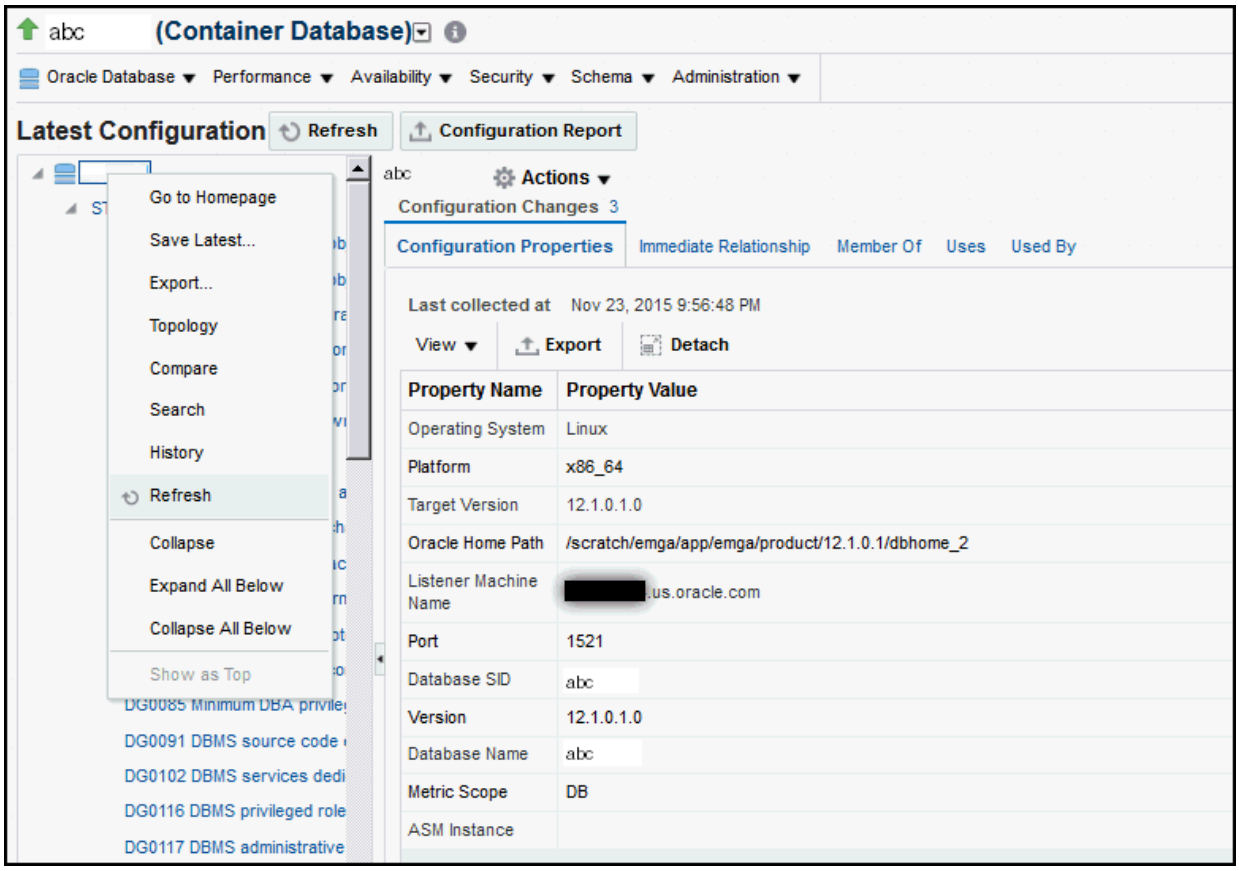
For every Oracle provided compliance rule contains information to assist you in understanding the rationale behind the validation as well as recommendations on how to correct the violation. In Figure 1-7, we can see the "Auditing of SYS Operations Enabled" rule has a violation event. We can see the category of this event is security related and exactly when it was reported. In addition we can see the recommendation to "Set AUDIT_SYS_OPERATIONS to TRUE" in the Guided resolution area.

From this point you have many options to investigate the violation further or resolve the issue including:

- View My Oracle Support Knowledge base pertaining to this validations (assuming My Oracle Support (MOS) is in Online mode.)
- View the Topology of the target and related targets to perform dependency analysis.
- View recently detected configuration changes to see when the change may have been made causing the violation.
- Disable the rule for the target causing the violation in case it is determined this rule is not relevant to this target.
- Create an incident from this event to prevent escalation notifications and create a workflow to resolution.
- View any updates to the event by other users.

Once the underlying cause of the violation has been resolved, the next scheduled configuration collection will cause the automatic recalculation of the targets compliance score. If you want to force a collection sooner, you can select refresh from the targets Last Collected configuration page as shown in Figure 1-8.

Figure 1-8 Manual Configuration Refresh



1.4 Summary

Enterprise Manager 13*c* makes it easy for you to validate your targets against Oracle recommendations, best practices and security standards by providing ready to use Compliance Standards. As DBAs and IT managers can easily track, manage, and report on the adherence of your managed targets to your standards in an automated and consistent manner.

2

Automatic Storage Management Compliance Standards

This section lists the compliance rules for the Automatic Storage Management(ASM) compliance standards.

2.1 Patchable Configuration For Asm

The compliance rules for the Patchable Configuration For Asm standard follow.

2.1.1 Patchability

Description: Ensure the ASM target has a patchable configuration

Severity: Warning

Rationale: Unpatchable ASM target could not be patched by using the provided EM Patching feature

2.2 Storage Best Practices For Asm

The compliance rules for the Storage Best Practices For Asm standard follow.

2.2.1 Disk Group Contains Disks Of Significantly Different Sizes

Description: Checks the disk group for disks with disk sizes which vary by more than 5%.

Severity: Warning

Rationale: Disks in a disk group should have sizes within 5% of each other, unless data migration is in progress. Automatic Storage Management distributes data uniformly proportional to the size of the disks. For balanced I/O and optimal performance, disks in a given disk group should have similar size and performance characteristics.

2.2.2 Disk Group Contains Disks With Different Redundancy Attributes

Description: Checks the disk group for disks that have different redundancy attributes.

Severity: Warning

Rationale: Disks in the same disk group with different redundancy attributes may offer inconsistent levels of data protection.

2.2.3 Disk Group Depends On External Redundancy And Has Unprotected Disks

Description: Checks the disk group, which depends on external redundancy, for disks that are not mirrored or parity protected.

Severity: Warning

Rationale: Data loss can occur if the disk group depends on external redundancy and disks are not mirrored or parity protected.

2.2.4 Disk Group With Normal Or High Redundancy Has Mirrored Or Parity Protected Disks

Description: Checks the disk group, with NORMAL or HIGH redundancy, for disks that are mirrored or parity protected.

Severity: Minor Warning

Rationale: Disk resources are wasted, and performance may be unnecessarily affected when both a disk and its owning disk group are providing data redundancy.

3

Cluster Compliance Standards

These are the compliance rules for the Cluster compliance standards

3.1 Patchable Configuration For Cluster

The compliance rules for the Patchable Configuration For Cluster standard follow.

3.1.1 Patchability

Description: Ensure the Cluster target has a patchable configuration

Severity: Warning

Rationale: Unpatchable Cluster target could not be patched by using the provided EM Patching feature

4

Cluster ASM Compliance Standards

These are the compliance rules for the Cluster ASM compliance standards

4.1 Storage Best Practices For Cluster Asm

The compliance rules for the Storage Best Practices For Cluster Asm standard follow.

4.1.1 Disk Group Contains Disks Of Significantly Different Sizes

Description: Checks the disk group for disks with disk sizes which vary by more than 5%.

Severity: Warning

Rationale: Disks in a disk group should have sizes within 5% of each other, unless data migration is in progress. Automatic Storage Management distributes data uniformly proportional to thesize of the disks. For balanced I/O and optimal performance, disks in a given disk group should have similar size and performance characteristics.

4.1.2 Disk Group Contains Disks With Different Redundancy Attributes

Description: Checks the disk group for disks that have different redundancy attributes.

Severity: Warning

Rationale: Disks in the same disk group with different redundancy attributes may offer inconsistent levels of data protection.

4.1.3 Disk Group Depends On External Redundancy And Has Unprotected Disks

Description: Checks the disk group, which depends on external redundancy, for disks that are not mirrored or parity protected.

Severity: Warning

Rationale: Data loss can occur if the disk group depends on external redundancy and disks are not mirrored or parity protected.

4.1.4 Disk Group With Normal Or High Redundancy Has Mirrored Or Parity Protected Disks

Description: Checks the disk group, with NORMAL or HIGH redundancy, for disks that are mirrored or parity protected.

Severity: Minor Warning

Rationale: Disk resources are wasted, and performance may be unnecessarily affected when both a disk and its owning disk group are providing data redundancy.

5

Fusion Instance Compliance Standards

These are the compliance rules for the Fusion Instance compliance standards

5.1 Automated Release Update Patch Recommendations For Fusion Applications

The compliance rules for the Automated Release Update Patch Recommendations For Fusion Applications standard follow.

5.1.1 Automated Release Update Patch Recommendation Rule For Oracle Fusion Applications

Description: This rule ensures that Oracle Fusion Applications and its underlying stack components (e.g. Oracle Database, Oracle WebLogic Server etc.) have all patches recommended in ARU and raises a violation for every missing patch.

Severity: Critical

Rationale: Patch Recommended

5.2 Java Platform Security Configuration Standard For Oracle Fusion Applications

The compliance rules for the Java Platform Security Configuration Standard For Oracle Fusion Applications standard follow.

5.2.1 Jps_Jps.Authz

Description: Fusion Applications Configuration rule for Java Platform Security jps.authz

Severity: Minor Warning

Rationale: Java Platform Security jps.authz

5.2.2 Jps_Jps.Combiner.Lazyeval

Description: Fusion Applications Configuration rule for Java Platform Security jps.combiner.lazyeval

Severity: Minor Warning

Rationale: Java Platform Security jps.combiner.lazyeval

5.2.3 Jps_Jps.Combiner.Optimize

Description: Fusion Applications Configuration rule for Java Platform Security jps.combiner.optimize

Severity: Minor Warning

Rationale: Java Platform Security jps.combiner.optimize

5.2.4 Jps_Jps.Policystore.Hybrid.Mode

Description: Fusion Applications Configuration rule for Java Platform Security jps.policystore.hybrid.mode

Severity: Minor Warning

Rationale: Java Platform Security jps.policystore.hybrid.mode

5.2.5 Java Platform Security Enable Policy Lazy Load Property

Description: Fusion Applications Configuration rule for Java Platform Security Enable Policy Lazy Load Property

Severity: Minor Warning

Rationale: Java Platform Security Enable Policy Lazy Load Property

5.2.6 Java Platform Security Refresh Purge Time Out

Description: Fusion Applications Configuration rule for Java Platform Security Refresh Purge Time Out

Severity: Warning

Rationale: Java Platform Security Refresh Purge Time Out

5.2.7 Java Platform Security Permission Cache Size

Description: Fusion Applications Configuration rule for Java Platform Security permission cache size

Severity: Minor Warning

Rationale: Java Platform Security permission cache size

5.2.8 Java Platform Security Permission Cache Strategy

Description: Fusion Applications Configuration rule for Java Platform Security permission cache strategy

Severity: Minor Warning

Rationale: Java Platform Security permission cache strategy

5.2.9 Java Platform Security Rolemember Cache Size

Description: Fusion Applications Configuration rule for Java Platform Security rolemember cache size

Severity: Minor Warning

Rationale: Java Platform Security rolemember cache size

5.2.10 Java Platform Security Rolemember Cache Strategy

Description: Fusion Applications Configuration rule for Java Platform Security rolemember cache strategy

Severity: Minor Warning

Rationale: Java Platform Security rolemember cache strategy

5.2.11 Java Platform Security Rolemember Cache Type

Description: Fusion Applications Configuration rule for Java Platform Security rolemember cache type

Severity: Minor Warning

Rationale: Java Platform Security rolemember cache type

5.3 Java Virtual Machine Configuration Standard For Oracle Fusion Applications

The compliance rules for the Java Virtual Machine Configuration Standard For Oracle Fusion Applications standard follow.

5.3.1 Jvm_Httpclient.Socket.Connectiontimeout

Description: Fusion Applications Configuration rule for HTTPClient.socket.connectionTimeout

Severity: Minor Warning

Rationale: HTTPClient.socket.connectionTimeout

5.3.2 Jvm_Httpclient.Socket.Readtimeout

Description: Fusion Applications Configuration rule for HTTPClient.socket.readTimeout

Severity: Minor Warning

Rationale: HTTPClient.socket.readTimeout

5.3.3 Jvm_Heapdumponoutofmemoryerror

Description: Fusion Applications Configuration rule for HeapDumpOnOutOfMemoryError

Severity: Minor Warning

Rationale: HeapDumpOnOutOfMemoryError

5.3.4 Jvm_Vomaxfetchsize

Description: Fusion Applications Configuration rule for VOMaxFetchSize

Severity: Minor Warning

Rationale: VOMaxFetchSize

5.3.5 Jvm_Xgc

Description: Fusion Applications Configuration rule for Xgc

Severity: Warning

Rationale: Xgc

5.3.6 Jvm_Xmanagement

Description: Fusion Applications Configuration rule for Xmanagement

Severity: Minor Warning

Rationale: Xmanagement

5.3.7 Jvm_Xverbose

Description: Fusion Applications Configuration rule for Xverbose

Severity: Minor Warning

Rationale: Xverbose

5.3.8 Jvm_Jbo.Ampool.Minavailablesize

Description: Fusion Applications Configuration rule for jbo.ampool.minavailablesize

Severity: Minor Warning

Rationale: jbo.ampool.minavailablesize

5.3.9 Jvm_Jbo.Ampool.Timetolive

Description: Fusion Applications Configuration rule for jbo.ampool.timetolive

Severity: Minor Warning

Rationale: jbo.ampool.timetolive

5.3.10 Jvm_Jbo.Doconnectionpooling

Description: Fusion Applications Configuration rule for jbo.doconnectionpooling

Severity: Minor Warning

Rationale: jbo.doconnectionpooling

5.3.11 Jvm_Jbo.Load.Components.Lazily

Description: Fusion Applications Configuration rule for jbo.load.components.lazily

Severity: Minor Warning

Rationale: jbo.load.components.lazily

5.3.12 Jvm_Jbo.Max.Cursors

Description: Fusion Applications Configuration rule for jbo.max.cursors

Severity: Minor Warning

Rationale: jbo.max.cursors

5.3.13 Jvm_Jbo.Recyclethreshold

Description: Fusion Applications Configuration rule for jbo.recyclethreshold

Severity: Minor Warning

Rationale: jbo.recyclethreshold

5.3.14 Jvm_Jbo.Txn.Disconnect_Level

Description: Fusion Applications Configuration rule for jbo.txn.disconnect_level

Severity: Minor Warning

Rationale: jbo.txn.disconnect_level

5.3.15 Jvm_Jps.Auth.Debug

Description: Fusion Applications Configuration rule for jps.auth.debug

Severity: Minor Warning

Rationale: jps.auth.debug

5.3.16 Jvm_Jrockit

Description: Fusion Applications Configuration rule for jrockit

Severity: Warning

Rationale: jrockit

5.3.17 Jvm_Weblogic.Productionmodeenabled

Description: Fusion Applications Configuration rule for weblogic.ProductionModeEnabled

Severity: Minor Warning

Rationale: weblogic.ProductionModeEnabled

5.3.18 Jvm_Weblogic.Socketreaders

Description: Fusion Applications Configuration rule for weblogic.SocketReaders

Severity: Minor Warning

Rationale: weblogic.SocketReaders

5.3.19 Jvm_Weblogic.Http.Client.Defaultreadtimeout

Description: Fusion Applications Configuration rule for weblogic.http.client.defaultReadTimeout

Severity: Minor Warning

Rationale: weblogic.http.client.defaultReadTimeout

5.3.20 Jvm_Weblogic.Http.Client.Weblogic.Http.Client.Defaultconnecttimeout

Description: Fusion Applications Configuration rule for weblogic.http.client.defaultConnectTimeout

Severity: Minor Warning

Rationale: weblogic.http.client.defaultConnectTimeout

5.3.21 Jvm_Weblogic.Security.Providers.Authentication.Ldapdelegatepoolsize

Description: Fusion Applications Configuration rule for weblogic.security.providers.authentication.LDAPDelegatePoolSize

Severity: Minor Warning

Rationale: weblogic.security.providers.authentication.LDAPDelegatePoolSize

5.4 Oracle Business Intelligence Configuration Standard For Oracle Fusion Applications

The compliance rules for the Oracle Business Intelligence Configuration Standard For Oracle Fusion Applications standard follow.

5.4.1 Bi Presentation Service Client Session Expire Minutes

Description: Fusion Applications Configuration rule for BI Presentation Service Client Session Expire Minutes

Severity: Warning

Rationale: BI Presentation Service Client Session Expire Minutes

5.4.2 Bi Presentation Service Max Queue

Description: Fusion Applications Configuration rule for BI Presentation Service Max Queue

Severity: Warning

Rationale: BI Presentation Service Max Queue

5.4.3 Bi Presentation Service Max Threads

Description: Fusion Applications Configuration rule for BI Presentation Service Max Threads

Severity: Warning

Rationale: BI Presentation Service Max Threads

5.4.4 Bi Presentation Service New Sync Logon Wait Seconds

Description: Fusion Applications Configuration rule for BI Presentation Service New Sync Logon Wait Seconds

Severity: Warning

Rationale: BI Presentation Service New Sync Logon Wait Seconds

5.4.5 Bi Presentation Service Path Job Log

Description: Fusion Applications Configuration rule for BI Presentation Service Path Job Log

Severity: Warning

Rationale: BI Presentation Service Path Job Log

5.4.6 Bi Presentation Service Path Saw

Description: Fusion Applications Configuration rule for BI Presentation Service Path Saw

Severity: Warning

Rationale: BI Presentation Service Path Saw

5.4.7 Bi Server Db Gateway Thread Range

Description: Fusion Applications Configuration rule for BI Server DB GateWay Thread Range

Severity: Warning

Rationale: BI Server DB GateWay Thread Range

5.4.8 Bi Server Db Gateway Thread Stack Size

Description: Fusion Applications Configuration rule for BI Server DB GateWay Thread Stack Size

Severity: Warning

Rationale: BI Server DB GateWay Thread Stack Size

5.4.9 Bi Server Enable

Description: Fusion Applications Configuration rule for BI Server Enable

Severity: Warning

Rationale: BI Server Enable

5.4.10 Bi Server Fmw Sec. Max No. Of Conns

Description: Fusion Applications Configuration rule for BI Server FMW Sec. Max No. Of Conns

Severity: Warning

Rationale: BI Server FMW Sec. Max No. Of Conns

5.4.11 Bi Server Init Block Cache Entries

Description: Fusion Applications Configuration rule for BI Server Init Block Cache Entries

Severity: Warning

Rationale: BI Server Init Block Cache Entries

5.4.12 Bi Server Max Cache Entries

Description: Fusion Applications Configuration rule for BI Server Max Cache Entries

Severity: Warning

Rationale: BI Server Max Cache Entries

5.4.13 Bi Server Max Cache Entry Size

Description: Fusion Applications Configuration rule for BI Server Max Cache Entry Size

Severity: Warning

Rationale: BI Server Max Cache Entry Size

5.4.14 Bi Server Max Drilldown Info Cache Entries

Description: Fusion Applications Configuration rule for BI Server Max Drilldown Info Cache Entries

Severity: Warning

Rationale: BI Server Max Drilldown Info Cache Entries

5.4.15 Bi Server Max Drilldown Query Cache Entries

Description: Fusion Applications Configuration rule for BI Server Max Drilldown Query Cache Entries

Severity: Warning

Rationale: BI Server Max Drilldown Query Cache Entries

5.4.16 Bi Server Max Expanded Subquery Predicates

Description: Fusion Applications Configuration rule for BI Server Max Expanded Subquery Predicates

Severity: Warning

Rationale: BI Server Max Expanded Subquery Predicates

5.4.17 Bi Server Max Query Plan Cache Entries

Description: Fusion Applications Configuration rule for BI Server Max Query Plan Cache Entries

Severity: Warning

Rationale: BI Server Max Query Plan Cache Entries

5.4.18 Bi Server Max Request Per Session Limit

Description: Fusion Applications Configuration rule for BI Server Max Request Per Session Limit

Severity: Warning

Rationale: BI Server Max Request Per Session Limit

5.4.19 Bi Server Max Session Limit

Description: Fusion Applications Configuration rule for BI Server Max Session Limit

Severity: Warning

Rationale: BI Server Max Session Limit

5.4.20 Bi Server Read Only Mode

Description: Fusion Applications Configuration rule for BI Server Read Only Mode

Severity: Warning

Rationale: BI Server Read Only Mode

5.4.21 Bi Server Thread Range

Description: Fusion Applications Configuration rule for BI Server Thread Range

Severity: Warning

Rationale: BI Server Thread Range

5.4.22 Bi Server Thread Stack Size

Description: Fusion Applications Configuration rule for BI Server Thread Stack Size

Severity: Warning

Rationale: BI Server Thread Stack Size

5.5 Oracle Database Configuration Standard For Oracle Fusion Applications

The compliance rules for the Oracle Database Configuration Standard For Oracle Fusion Applications standard follow.

5.5.1 Database Audit Trail

Description: Fusion Applications Configuration rule for Database Audit Trail

Severity: Warning

Rationale: Database Audit Trail

5.5.2 Database B-Tree Bitmap Plans

Description: Fusion Applications Configuration rule for Database B-tree Bitmap Plans

Severity: Warning

Rationale: Database B-tree Bitmap Plans

5.5.3 Database Compatible

Description: Fusion Applications Configuration rule for Database Compatible

Severity: Warning

Rationale: Database Compatible

5.5.4 Database Db Files

Description: Fusion Applications Configuration rule for Database DB Files

Severity: Warning

Rationale: Database DB Files

5.5.5 Database Db Writer Processes

Description: Fusion Applications Configuration rule for Database DB Writer Processes

Severity: Warning

Rationale: Database DB Writer Processes

5.5.6 Database Disk Asynchronous Io

Description: Fusion Applications Configuration rule for Database Disk Asynchronous IO

Severity: Warning

Rationale: Database Disk Asynchronous IO

5.5.7 Database Fast Start Monitor Target

Description: Fusion Applications Configuration rule for Database Fast Start Monitor target

Severity: Warning

Rationale: Database Fast Start Monitor target

5.5.8 Database File System Io Options

Description: Fusion Applications Configuration rule for Database File System IO Options

Severity: Warning

Rationale: Database File System IO Options

5.5.9 Database Job Queue Processes

Description: Fusion Applications Configuration rule for Database Job Queue Processes

Severity: Warning

Rationale: Database Job Queue Processes

5.5.10 Database Log Buffer

Description: Fusion Applications Configuration rule for Database Log Buffer

Severity: Warning

Rationale: Database Log Buffer

5.5.11 Database Log Checkpoints To Alert

Description: Fusion Applications Configuration rule for Database Log Checkpoints to Alert

Severity: Warning

Rationale: Database Log Checkpoints to Alert

5.5.12 Database Maximum Dump File Size

Description: Fusion Applications Configuration rule for Database Maximum Dump File Size

Severity: Warning

Rationale: Database Maximum Dump File Size

5.5.13 Database Memory Target

Description: Fusion Applications Configuration rule for Database Memory Target

Severity: Warning

Rationale: Database Memory Target

5.5.14 Database Nls Sort

Description: Fusion Applications Configuration rule for Database NLS Sort

Severity: Warning

Rationale: Database NLS Sort

5.5.15 Database Open Cursors

Description: Fusion Applications Configuration rule for Database Open Cursors

Severity: Warning

Rationale: Database Open Cursors

5.5.16 Database Pga Aggregate Target

Description: Fusion Applications Configuration rule for Database PGA Aggregate Target

Severity: Warning

Rationale: Database PGA Aggregate Target

5.5.17 Database Plsql Code Type

Description: Fusion Applications Configuration rule for Database PLSQL Code Type

Severity: Warning

Rationale: Database PLSQL Code Type

5.5.18 Database Processes

Description: Fusion Applications Configuration rule for Database Processes

Severity: Warning

Rationale: Database Processes

5.5.19 Database Recovery File Dest Size

Description: Fusion Applications Configuration rule for Database Recovery File Dest Size

Severity: Warning

Rationale: Database Recovery File Dest Size

5.5.20 Database Sga Target

Description: Fusion Applications Configuration rule for Database SGA Target

Severity: Warning

Rationale: Database SGA Target

5.5.21 Database Session Cached Cursors

Description: Fusion Applications Configuration rule for Database Session Cached Cursors

Severity: Warning

Rationale: Database Session Cached Cursors

5.5.22 Database Trace Enabled

Description: Fusion Applications Configuration rule for Database Trace Enabled

Severity: Warning

Rationale: Database Trace Enabled

5.5.23 Database Undo Management

Description: Fusion Applications Configuration rule for Database Undo management

Severity: Warning

Rationale: Database Undo management

5.6 Oracle Http Server Configuration Standard For Oracle Fusion Applications

The compliance rules for the Oracle Http Server Configuration Standard For Oracle Fusion Applications standard follow.

5.6.1 Oracle Http Server Browser Caching

Description: Fusion Applications Configuration rule for Oracle HTTP Server Browser Caching

Severity: Warning

Rationale: Oracle HTTP Server Browser Caching

5.6.2 Oracle Http Server Conn Retry Secs

Description: Fusion Applications Configuration rule for Oracle HTTP Server Conn retry secs

Severity: Warning

Rationale: Oracle HTTP Server Conn retry secs

5.6.3 Oracle Http Server Custom Log

Description: Fusion Applications Configuration rule for Oracle HTTP Server Custom Log

Severity: Warning

Rationale: Oracle HTTP Server Custom Log

5.6.4 Oracle Http Server File Caching

Description: Fusion Applications Configuration rule for Oracle HTTP Server File Caching

Severity: Warning

Rationale: Oracle HTTP Server File Caching

5.6.5 Oracle Http Server Max Spare Threads

Description: Fusion Applications Configuration rule for Oracle HTTP Server Max Spare Threads

Severity: Warning

Rationale: Oracle HTTP Server Max Spare Threads

5.6.6 Oracle Http Server Min Spare Threads

Description: Fusion Applications Configuration rule for Oracle HTTP Server Min Spare Threads

Severity: Warning

Rationale: Oracle HTTP Server Min Spare Threads

5.6.7 Oracle Http Server Startservers

Description: Oracle HTTP Server StartServers

Severity: Minor Warning

Rationale: Oracle HTTP Server StartServers

5.6.8 Oracle Http Server Wliotimeoutsecs

Description: Fusion Applications Configuration rule for Oracle HTTP Server WLIOTimeoutSecs

Severity: Minor Warning

Rationale: Oracle HTTP Server WLIOTimeoutSecs

5.6.9 Oracle Http Server Keep Alive Timeout

Description: Fusion Applications Configuration rule for Oracle HTTP Server keep alive timeout

Severity: Minor Warning

Rationale: Oracle HTTP Server keep alive timeout

5.6.10 Oracle Http Server Lock File

Description: Fusion Applications Configuration rule for Oracle HTTP Server lock file

Severity: Warning

Rationale: Oracle HTTP Server lock file

5.6.11 Oracle Http Server Maximum Clients

Description: Fusion Applications Configuration rule for Oracle HTTP Server maximum clients

Severity: Minor Warning

Rationale: Oracle HTTP Server maximum clients

5.6.12 Oracle Http Server Maximum Keep Alive Requests

Description: Fusion Applications Configuration rule for Oracle HTTP Server maximum keep alive requests

Severity: Minor Warning

Rationale: Oracle HTTP Server maximum keep alive requests

5.6.13 Oracle Http Server Server Limit

Description: Fusion Applications Configuration rule for Oracle HTTP Server server limit

Severity: Warning

Rationale: Oracle HTTP Server server limit

5.6.14 Oracle Http Server Set Env If No Case

Description: Fusion Applications Configuration rule for OHS SENC

Severity: Warning

Rationale: OHS set env if no case

5.6.15 Oracle Http Server Thread Limit

Description: Fusion Applications Configuration rule for Oracle HTTP Server thread limit

Severity: Warning

Rationale: Oracle HTTP Server thread limit

5.6.16 Oracle Http Server Threads Per Child

Description: Fusion Applications Configuration rule for Oracle HTTP Server threads per child

Severity: Warning

Rationale: Oracle HTTP Server threads per child

5.7 Weblogic Server Configuration Standard For Oracle Fusion Applications

The compliance rules for the Weblogic Server Configuration Standard For Oracle Fusion Applications standard follow.

5.7.1 Weblogic Domain Log File Format

Description: Fusion Applications Configuration rule for WebLogic Domain Log File Format

Severity: Warning

Rationale: WebLogic Domain Log File Format

5.7.2 Weblogic Domain Login Delay Seconds

Description: Fusion Applications Configuration rule for WebLogic Domain Login Delay Seconds

Severity: Warning

Rationale: WebLogic Domain Login Delay Seconds

5.7.3 Weblogic Keep Alive Enabled

Description: Fusion Applications Configuration rule for WebLogic Keep Alive Enabled

Severity: Warning

Rationale: Weblogic Domain Keep Alive Enabled

5.7.4 Weblogic Domain Conn. Creation Retry Frequency Secs

Description: Fusion Applications Configuration rule for WebLogic domain Conn. Creation Retry Frequency Secs

Severity: Warning

Rationale: WebLogic domain Conn. Creation Retry Frequency Secs

5.7.5 Weblogic Domain Conn. Reserve Timeout Secs

Description: Fusion Applications Configuration rule for WebLogic domain conn. reserve timeout secs

Severity: Warning

Rationale: WebLogic domain conn. reserve timeout secs

5.7.6 Weblogic Domain Highest Num Waiters

Description: Fusion Applications Configuration rule for WebLogic domain highest num waiters

Severity: Warning

Rationale: WebLogic domain highest num waiters

5.7.7 Weblogic Domain Ignore In Use Connections Enabled

Description: Fusion Applications Configuration rule for WebLogic domain ignore in use connections enabled

Severity: Warning

Rationale: WebLogic domain ignore in use connections enabled

5.7.8 Weblogic Domain Inactive Conn. Timeout Secs

Description: Fusion Applications Configuration rule for WebLogic domain inactive conn. timeout secs

Severity: Warning

Rationale: WebLogic domain inactive conn. timeout secs

5.7.9 Weblogic Domain Init Sql

Description: Fusion Applications Configuration rule for WebLogic domain init sql

Severity: Warning

Rationale: WebLogic domain init sql

5.7.10 Weblogic Domain Initial Capacity

Description: Fusion Applications Configuration rule for WebLogic domain initial capacity

Severity: Warning

Rationale: WebLogic domain initial capacity

5.7.11 Weblogic Domain Log Severity

Description: Fusion Applications Configuration rule for WebLogic domain log severity

Severity: Minor Warning

Rationale: WebLogic domain log severity

5.7.12 Weblogic Domain Min Capacity

Description: Fusion Applications Configuration rule for WebLogic domain min capacity

Severity: Warning

Rationale: WebLogic domain min capacity

5.7.13 Weblogic Domain Pinned To Thread

Description: Fusion Applications Configuration rule for WebLogic domain pinned to thread

Severity: Warning

Rationale: Weblogic Domain Pinned To Thread

5.7.14 Weblogic Domain Statement Timeout

Description: Fusion Applications Configuration rule for WebLogic domain statement timeout

Severity: Warning

Rationale: WebLogic domain statement timeout

5.7.15 Weblogic Domain Test Frequency Seconds

Description: Fusion Applications Configuration rule for WebLogic domain test frequency seconds

Severity: Warning

Rationale: WebLogic domain max capacity

5.7.16 Weblogic Domain Test Table Name

Description: Fusion Applications Configuration rule for WebLogic domain test table name

Severity: Warning

Rationale: WebLogic domain test table name

5.7.17 Weblogic Log File Severity

Description: Fusion Applications Configuration rule for WebLogic log file severity

Severity: Minor Warning

Rationale: WebLogic log file severity

5.7.18 Weblogic Memory Buffer Severity

Description: Fusion Applications Configuration rule for WebLogic memory buffer severity

Severity: Minor Warning

Rationale: WebLogic memory buffer severity

5.7.19 Weblogic Stdout Severity

Description: Fusion Applications Configuration rule for WebLogic stdout severity

Severity: Minor Warning

Rationale: WebLogic stdout severity

5.7.20 Weblogic Domain Cache Size

Description: Fusion Applications Configuration rule for Weblogic Domain Cache Size

Severity: Warning

Rationale: Weblogic Domain Cache Size

5.7.21 Weblogic Domain Cache Ttl

Description: Fusion Applications Configuration rule for Weblogic Domain Cache TTL

Severity: Warning

Rationale: Weblogic Domain Cache TTL

5.7.22 Weblogic Domain Capacity Increment

Description: Fusion Applications Configuration rule for Weblogic Domain Capacity Increment

Severity: Warning

Rationale: Weblogic Domain Capacity Increment

5.7.23 Weblogic Domain Elf Fields

Description: Fusion Applications Configuration rule for Weblogic Domain Elf Fields

Severity: Warning

Rationale: Weblogic Domain Elf Fields

5.7.24 Weblogic Domain Enable Group Membership Lookup Hierarchy Caching

Description: Fusion Applications Configuration rule for Weblogic Domain Enable Group Membership Lookup Hierarchy Caching

Severity: Warning

Rationale: Weblogic Domain Enable Group Membership Lookup Hierarchy Caching

5.7.25 Weblogic Domain File Name

Description: Fusion Applications Configuration rule for Weblogic Domain File Name

Severity: Warning

Rationale: Weblogic Domain File Name

5.7.26 Weblogic Domain Group Hierarchy Cache Ttl

Description: Fusion Applications Configuration rule for Weblogic Domain Group Hierarchy Cache TTL

Severity: Warning

Rationale: Weblogic Domain Group Hierarchy Cache TTL

5.7.27 Weblogic Domain Max Capacity

Description: Fusion Applications Configuration rule for Weblogic Domain Max Capacity

Severity: Warning

Rationale: Weblogic Domain Max Capacity

5.7.28 Weblogic Domain Max Group Hierarchies In Cache

Description: Fusion Applications Configuration rule for Weblogic Domain Max Group Hierarchies In Cache

Severity: Warning

Rationale: Weblogic Domain Max Group Hierarchies In Cache

5.7.29 Weblogic Domain Secs To Trust An Idle Conn.

Description: Fusion Applications Configuration rule for Weblogic Domain Secs To Trust An Idle Conn.

Severity: Warning

Rationale: Weblogic Domain Secs To Trust An Idle Conn.

5.7.30 Weblogic Domain State Check Interval

Description: Fusion Applications Configuration rule for Weblogic Domain State Check Interval

Severity: Warning

Rationale: Weblogic Domain State Check Interval

5.7.31 Weblogic Domain Statement Cache Size

Description: Fusion Applications Configuration rule for Weblogic Domain Statement Cache Size

Severity: Warning

Rationale: Weblogic Domain Statement Cache Size

5.7.32 Weblogic Domain Statement Cache Type

Description: Fusion Applications Configuration rule for Weblogic Domain Statement Cache Type

Severity: Warning

Rationale: Weblogic Domain Statement Cache Type

5.7.33 Weblogic Domain Test Connections On Reserve

Description: Fusion Applications Configuration rule for Weblogic Domain Test Connections On Reserve

Severity: Warning

Rationale: Weblogic Domain Test Connections On Reserve

6

Host Compliance Standards

These are the compliance rules for the Host compliance standards

6.1 Configuration Monitoring For Core Linux Packages

The compliance rules for the Configuration Monitoring For Core Linux Packages standard follow.

6.1.1 Monitor Configuration Files For Os Booting Packages

Description: Monitors configuration files for OS booting/startup related packages that come with Linux.

Severity: Critical

Rationale: When file changes occur to the configuration files of booting/startup related packages on a Linux host outside of upgrade windows, the modification can lead to serious disruptions and or security vulnerabilities.

6.1.2 Monitor Configuration Files For Core Os Packages

Description: Monitors configuration files for core OS packages that come with Linux. These packages include Kernel-related elements and core commands.

Severity: Critical

Rationale: When file changes occur to the configuration files of core OS related packages on a Linux host outside of upgrade windows, the modification can lead to serious disruptions and or security vulnerabilities.

6.2 Configuration Monitoring For Exadata Compute Node

The compliance rules for the Configuration Monitoring For Exadata Compute Node standard follow.

6.2.1 Monitor Configuration Files For Exadata Compute Node Cell Os

Description: Monitors configuration files that are part of the Exadata compute node's Cell OS. This rule is monitoring configuration files that are related to basic cell operations.

Severity: Critical

Rationale: When a configuration file changes occurs, the modification can lead to serious service disruptions and or security vulnerabilities.

6.2.2 Monitor Configuration Files For Exadata Compute Node Database

Description: Monitors configuration files that are part of the Exadata compute node's bundled Oracle Database. This rule is monitoring configuration files that are related to the Database, Clusterware, Storage Management, and Cluster Verification utility

Severity: Critical

Rationale: When a configuration file changes occurs, the modification can lead to serious service disruptions and or security vulnerabilities. These configuration files may impact the functioning of the bundled database on this Exadata compute node or the Database cluster this node belongs to.

6.2.3 Monitor Configuration Files For Exadata Compute Node Megaraid

Description: Monitors configuration files that are part of the Exadata compute node's LSI MegaRAID support. This rule is monitoring configuration files that are related to the MegaRAID Storage Manager and MegaRAID XTools.

Severity: Critical

Rationale: When a configuration file changes occurs, the modification can lead to serious service disruptions and or security vulnerabilities. These configuration files may impact the functioning of the RAID storage functionality on this node.

6.2.4 Monitor Configuration Files For Exadata Compute Node Management And Diagnostics Systems

Description: Monitors configuration files that are part of the Exadata compute node elements for changes to the files. This rule specifically is monitoring the configuration files for the various tools and systems that are part of the Compute Node used for management or diagnostics.

Severity: Critical

Rationale: When a configuration file changes occurs, the modification can lead to serious service disruptions and or security vulnerabilities. These configuration files may impact the functioning of a management or monitoring tool that could be used to report other issues.

6.2.5 Monitor Host-Specific Configuration Files For Exadata Compute Node Management And Diagnostics Systems

Description: Monitors configuration files that are part of the Exadata compute node elements for changes to the files. This rule specifically is monitoring the configuration files for the various tools and systems that are part of the Compute Node used for management or diagnostics that are specific for the given host. The facets being monitored include the hostname in the path and must be configured per host target association for the rule to function.

Severity: Critical

Rationale: When a configuration file changes occurs, the modification can lead to serious service disruptions and or security vulnerabilities. These configuration files may impact the functioning of a management or monitoring tool that could be used to report other issues.

6.3 Configuration Monitoring For Exadata Compute Node Networking

The compliance rules for the Configuration Monitoring For Exadata Compute Node Networking standard follow.

6.3.1 Monitor Configuration Files For Exadata Compute Node Cell Os Networking

Description: Monitors configuration files that are part of the Exadata compute node's Cell OS. This rule is monitoring configuration files that are related to the Cell's networking configuration

Severity: Critical

Rationale: When a configuration file changes occurs, the modification can lead to serious service disruptions and or security vulnerabilities. Unintended modification of these configuration files can lead to components in an Exadata rack being unreachable.

6.3.2 Monitor Configuration Files For Exadata Compute Node Infiniband

Description: Monitors configuration files that are part of the Exadata compute node Infiniband support. This rule is monitoring Open Infiniband configuration files and Infiniband Diagnostics Tools.

Severity: Critical

Rationale: When a configuration file changes occurs, the modification can lead to serious service disruptions and or security vulnerabilities. These configuration files may impact the functioning of the Exadata component communications.

6.4 Configuration Monitoring For Exadata Compute Node Time

The compliance rules for the Configuration Monitoring For Exadata Compute Node Time standard follow.

6.4.1 Monitor Configuration Files For Exadata Compute Node Cell Os Time

Description: Monitors configuration files that are part of the Exadata compute node's Cell OS. This rule is monitoring configuration files related to clock synchronization for the Cell.

Severity: Critical

Rationale: When a configuration file changes occurs, the modification can lead to serious service disruptions and or security vulnerabilities. Time synchronization is very important in complex systems. Clock out of sync issues caused by misconfigured network time daemon can lead to failures and system downtime.

6.5 Configuration Monitoring For Network Time Linux Packages

The compliance rules for the Configuration Monitoring For Network Time Linux Packages standard follow.

6.5.1 Monitor Configuration Files For Network Time Packages

Description: Monitors configuration files for network time related packages that come with Linux such as FTP. These packages ensure your clocks are in sync.

Severity: Critical

Rationale: When file changes occur to the configuration files of a network time related package on a Linux host outside of upgrade windows, the modification can lead to serious disruptions and or security vulnerabilities. Most distributed software programs depend on the host clocks being in sync.

6.6 Configuration Monitoring For Networking Linux Packages

The compliance rules for the Configuration Monitoring For Networking Linux Packages standard follow.

6.6.1 Monitor Configuration Files For File Transfer Packages

Description: Monitors configuration files for file transfer related packages that come with Linux such as FTP.

Severity: Critical

Rationale: When file changes occur to the configuration files of a file transfer related package on a Linux host outside of upgrade windows, the modification can lead to serious disruptions and or security vulnerabilities.

6.6.2 Monitor Configuration Files For Networking Packages

Description: Monitors configuration files for networking related packages that come with Linux.

Severity: Critical

Rationale: When file changes occur to the configuration files of a networking related package on a Linux host outside of upgrade windows, the modification can lead to serious disruptions and or security vulnerabilities.

6.7 Configuration Monitoring For Security Linux Packages

The compliance rules for the Configuration Monitoring For Security Linux Packages standard follow.

6.7.1 Monitor Configuration Files For Security Packages

Description: Monitors configuration files for security related packages that come with Linux.

Severity: Critical

Rationale: When file changes occur to the configuration files of security related packages on a Linux host outside of upgrade windows, the modification can lead to serious disruptions and or security vulnerabilities.

6.8 Configuration Monitoring For User Access Linux Packages

The compliance rules for the Configuration Monitoring For User Access Linux Packages standard follow.

6.8.1 Monitor Configuration Files For User Access Packages

Description: Monitors configuration files for user access packages that come with Linux. These packages include SUDO as well as user management and configuration packages.

Severity: Critical

Rationale: When file changes occur to the configuration files of user access related packages on a Linux host outside of upgrade windows, the modification can lead to serious disruptions and or security vulnerabilities.

6.9 File Integrity Monitoring For Exadata Compute Node

The compliance rules for the File Integrity Monitoring For Exadata Compute Node standard follow.

6.9.1 Monitor Executable Files For Core Exadata Compute Node

Description: Monitors executable files that are part of the Exadata compute node elements for changes to the files. Executable files include binary programs, Shell, Perl, and Python scripts. This rule only covers Exadata specific elements that are on top of any base operating system elements.

Severity: Critical

Rationale: When file changes occur to the executables of a production Exadata Compute Node outside of upgrade windows, the modification can lead to serious disruptions and or security vulnerabilities.

6.9.2 Monitor Library Files For Core Exadata Compute Node

Description: Monitors library files that are part of the Exadata compute node elements. Library files include .SO, Java JAR files, Python and Perl library modules. This rule only covers Exadata specific elements that are on top of any base operating system elements.

Severity: Critical

Rationale: When file changes occur to the libraries of a production Exadata Compute Node outside of upgrade windows, the modification can lead to serious disruptions and or security vulnerabilities.

6.10 File Integrity Monitoring For Important Linux Packages

The compliance rules for the File Integrity Monitoring For Important Linux Packages standard follow.

6.10.1 Monitor Executable Files For Core Os Packages

Description: Monitors executable files for core OS packages that come with Linux. Executable files include programs, Shell, Python, and Perl scripts. These packages include Kernel-related elements, Boot Loaders and core commands.

Severity: Critical

Rationale: When file changes occur to the executables of core OS related packages on a Linux host outside of upgrade windows, the modification can lead to serious disruptions and or security vulnerabilities.

6.10.2 Monitor Executable Files For Networking Packages

Description: Monitors executable files for networking related packages that come with Linux. Executable files include programs, Shell, Python, and Perl scripts.

Severity: Critical

Rationale: When file changes occur to the executables of a networking related package on a Linux host outside of upgrade windows, the modification can lead to serious disruptions and or security vulnerabilities.

6.10.3 Monitor Executable Files For Security Packages

Description: Monitors executable files for security related packages that come with Linux. Executable files include programs, Shell, Python, and Perl scripts.

Severity: Critical

Rationale: When file changes occur to the executables of security related packages on a Linux host outside of upgrade windows, the modification can lead to serious disruptions and or security vulnerabilities.

6.10.4 Monitor Executable Files For User Access Packages

Description: Monitors executable files for user access packages that come with Linux. Executable files include programs, Shell, Python, and Perl scripts. These packages include SUDO as well as user management and configuration packages.

Severity: Critical

Rationale: When file changes occur to the executables of user access related packages on a Linux host outside of upgrade windows, the modification can lead to serious disruptions and or security vulnerabilities.

6.10.5 Monitor Library Files For Core Os Packages

Description: Monitors library files for core OS packages that come with Linux. Library files include .SO, Java JAR files, Python and Perl library modules. These packages include Kernel-related elements, Boot Loaders and core commands.

Severity: Critical

Rationale: When file changes occur to the libraries of core OS packages on a Linux host outside of upgrade windows, the modification can lead to serious disruptions and or security vulnerabilities.

6.10.6 Monitor Library Files For Networking Packages

Description: Monitors library files for networking related packages that come with Linux. Library files include .SO, Java JAR files, Python and Perl library modules.

Severity: Critical

Rationale: When file changes occur to the libraries of a networking related packages on a Linux host outside of upgrade windows, the modification can lead to serious disruptions and or security vulnerabilities.

6.10.7 Monitor Library Files For Security Packages

Description: Monitors library files for security-related packages that come with Linux. Library files include .SO, Java JAR files, Python and Perl library modules.

Severity: Critical

Rationale: When file changes occur to the libraries of security related packages on a Linux host outside of upgrade windows, the modification can lead to serious disruptions and or security vulnerabilities.

6.10.8 Monitor Library Files For User Access Packages

Description: Monitors library files for user access packages that come with Linux. Library files include .SO, Java JAR files, Python and Perl library modules. These packages include SUDO as well as user management and configuration packages.

Severity: Critical

Rationale: When file changes occur to the libraries of user access packages on a Linux host outside of upgrade windows, the modification can lead to serious disruptions and or security vulnerabilities.

6.11 Secure Configuration For Host

The compliance rules for the Secure Configuration For Host standard follow.

6.11.1 Nfts File System

Description: Ensure that the file system on a Windows operating system uses NTFS

Severity: Critical

Rationale: Other than NTFS, file systems on Windows platforms may have serious security risks.

6.11.2 Secure Ports

Description: Ensure that no unintended ports are left open

Severity: Critical

Rationale: Open ports may allow a malicious user to take over the host.

6.11.3 Secure Services

Description: Ensure that there are no insecure services (for example, telnet and ftp) running on the server

Severity: Warning

Rationale: Insecure services may allow a malicious user to take over the host.

6.11.4 Executable Stack Disabled

Description: Ensure that the OS configuration parameter, which enables execution of code on the user stack, is not enabled

Severity: Warning

Rationale: Enabling code execution on the user stack may allow a malicious user to exploit stack buffer overflows. Overflows can cause portions of a system to fail, or even execute arbitrary code.

6.12 Security Recommendations For Oracle Products

The compliance rules for the Security Recommendations For Oracle Products standard follow.

6.12.1 Security Recommendations

Description: Checks targets in your host for missing security patches

Severity: Critical

Rationale: To help ensure a secure and reliable configuration, all relevant and current security patches should be applied.

7

Oracle Access Management Cluster Compliance Standards

These are the compliance rules for the Oracle Access Management Cluster compliance standards

7.1 Oracle Access Manager Configuration Compliance For Oracle Fusion Applications

The compliance rules for the Oracle Access Manager Configuration Compliance For Oracle Fusion Applications standard follow.

7.1.1 Webgate-Agent Communication Mode

Description: Webgate/Agent communication to Oracle Access Manager servers should be in either SIMPLE or CERT mode.

Severity: Warning

Rationale: Webgate/Agent communication to Oracle Access Manager servers should be in either SIMPLE or CERT mode.

7.1.2 Denyonnotprotected In Webgate Profile

Description: DenyOnNotProtected in Webgate profile should be set to true

Severity: Warning

Rationale: DenyOnNotProtected in Webgate profile should be set to true.

7.1.3 Oam Agent Cache Headers Settings

Description: This rule checks if both Cache Pragma Header and Cache Control Header are deleted for Oracle Fusion Applications.

Severity: Minor Warning

Rationale: Having Cache Pragma Header or Cache Control Header not deleted could potentially affect performance.

7.1.4 Oam Agent Maximum Connections

Description: This rule checks if the Maximum Connections that each OAM Agent establishs with OAM Server is greater than 20 for Oracle Fusion Applications.

Severity: Minor Warning

Rationale: Setting Maximum Connections greater than 20 could potentially affect performance.

7.1.5 Oam Agent Server Maximum Connections

Description: This rule checks if the Maximum Connections that each OAM Agent Server establishs with OAM Server is greater than 10 for Oracle Fusion Applications.

Severity: Minor Warning

Rationale: Setting Maximum Connections greater than 10 could potentially affect performance.

7.1.6 Sso Only Mode

Description: This compliance standard rule verifies if SSO only Mode is set to true for Oracle Fusion Applications.

Severity: Minor Warning

Rationale: This is introduced specially for Fusion Applications. This will eliminate the groups fetch from LDAP during login time. This will disable fine grained authorization feature in Oracle Access Manager currently not used by Fusion Applications.

7.1.7 Webgate To Oracle Access Manager Connectivity Parameters

Description: Webgate to Oracle Access Manager connectivity parameters

Severity: Warning

Rationale: Ensure that Webgate to Oracle Access Manager connectivity parameters are set to proper values.

8

Oracle Access Management Server Compliance Standards

These are the compliance rules for the Oracle Access Management Server compliance standards

8.1 Oracle Access Manager Server Agent Configuration Compliance

The compliance rules for the Oracle Access Manager Server Agent Configuration Compliance standard follow.

8.1.1 Oracle Access Manager Config Tool Validation

Description: Oracle Access Manager config tool validation

Severity: Minor Warning

Rationale: Oracle Access Manager should configure using IDM config tool.

8.2 Oracle Access Manager Server Configuration Compliance

The compliance rules for the Oracle Access Manager Server Configuration Compliance standard follow.

8.2.1 Oracle Access Manager Performance Tunning Params

Description: Oracle Access Manager Performance Tunning Params

Severity: Warning

Rationale: Oracle Access Manager Performance Tunning Params should set to the optimal values.

8.2.2 Oracle Access Manager Weblogic Domain Max Heap Size

Description: Oracle Access Manager Configuration rule for Weblogic Domain Max Heap Size

Severity: Warning

Rationale: Oracle Access Manager Weblogic Domain Max Heap Size should set to 4096

8.2.3 Oracle Access Manager Weblogic Domain Production Mode

Description: Oracle Access Manager Configuration rule for Weblogic Domain Production Mode

Severity: Warning

Rationale: WebLogic Domain hosting Oracle Access manager should run in Production mode instead of Development mode.

8.2.4 Oracle Access Manager Weblogic Domain Start Heap Size

Description: Oracle Access Manager Configuration rule for Weblogic Domain Start Heap Size

Severity: Warning

Rationale: Oracle Access Manager Weblogic Domain Start Heap Size should set to 1024

8.2.5 Weblogic Server Authenticator Sequence

Description: WebLogic Server Authenticator sequence

Severity: Warning

Rationale: WebLogic Server Authenticator sequence should be in the sequence - OAMIDAsserter, OUD Authenticator (or LDAP Authenticator), Default Authenticator, Default Identity Asserter

9

Oracle Database Machine Compliance Standards

These are the compliance rules for the Oracle Database Machine compliance standards

9.1 Db Machine Compliance

The compliance rules for the Db Machine Compliance standard follow.

9.1.1 Misconfigured Grid Disks

Description: Check if grid disks are configured uniformly on all cells in a cell group.

Severity: Minor Warning

Rationale: Within a cell group (set of cellsmonitored by an ASM disk group), all grid disks should be configured the sameon every cell. Mis configurations may result in poor performance

9.1.2 Overlap Of Cell Groups

Description: Check if cell usage by ASM is not uniform.

Severity: Minor Warning

Rationale: ASM diskgroup use of grid disksfrom Exadata cells should be arranged so that disk groups should either share all the cells or none of the cells. This configuration results in the most optimum performance.

10

Oracle Identity Manager Compliance Standards

These are the compliance rules for the Oracle Identity Manager compliance standards

10.1 Oracle Identity Manager Server Configuration Compliance

The compliance rules for the Oracle Identity Manager Server Configuration Compliance standard follow.

10.1.1 Disable Caching Configuration

Description: This compliance standard rule verifies whether certain Caching components "threadLocalCacheEnabled" and "StoredProcAPI" have been disabled or not for Oracle Identity Manager.

Severity: Minor Warning

Rationale: Setting Caching components "threadLocalCacheEnabled" and "StoredProcAPI" to "true" is not recommended.

10.1.2 Disable Reloading Of Adapters And Plug-In Configuration

Description: This compliance standard rule verifies whether Adapters and Plug-in Reloading are disabled or not for Oracle Identity Manager.

Severity: Minor Warning

Rationale: By default, reloading of adapters and plug-in configuration is enabled for ease of development. This should be disabled in the production environment to improve performance of the Oracle Weblogic Server for the Oracle Identity Manager.

10.1.3 Enable Caching Configuration

Description: This compliance standard rule verifies whether caching for metadata has been enabled or not for Oracle Identity Manager.

Severity: Minor Warning

Rationale: Setting Caching components to "false" could potentially affect the performance.

10.1.4 Oracle Identity Manager Dbworkmanager Maximum Threads

Description: Oracle Identity Manager Configuration rule for DBWorkManager Maximum Threads

Severity: Warning

Rationale: Oracle Identity Manager DBWorkManager Maximum Threads should set to 80

10.1.5 Oracle Identity Manager Database Tuning Disk Asynchronous Io

Description: Oracle Identity Manager Configuration rule for Database Tuning Disk Asynchronous IO

Severity: Warning

Rationale: Oracle Identity Manager Database Tuning Disk Asynchronous IO

10.1.6 Oracle Identity Manager Database Tuning Maxdispatchers

Description: Oracle Identity Manager Configuration rule for Database Tuning maxdispatchers

Severity: Warning

Rationale: Oracle Identity Manager Database Tuning maxdispatchers

10.1.7 Oracle Identity Manager Database Tuning Maxsharedservers

Description: Oracle Identity Manager Configuration rule for Database Tuning maxsharedservers

Severity: Warning

Rationale: Oracle Identity Manager Database Tuning maxsharedservers

10.1.8 Oracle Identity Manager Database Tuning Pgaaggregatetarget

Description: Oracle Identity Manager Configuration rule for Database Tuning pgaaggregatetarget

Severity: Warning

Rationale: Oracle Identity Manager Database Tuning pgaaggregatetarget

10.1.9 Oracle Identity Manager Database Tuning Sgatarget

Description: Oracle Identity Manager Configuration rule for Database Tuning sgatarget

Severity: Warning

Rationale: Oracle Identity Manager Database Tuning sgatarget

10.1.10 Oracle Identity Manager Direct Db Max Connections

Description: Oracle Identity Manager Configuration rule for Direct DB Max Connections

Severity: Warning

Rationale: Oracle Identity Manager Direct DB Max Connections should set to 150

10.1.11 Oracle Identity Manager Direct Db Min Connections

Description: Oracle Identity Manager Configuration rule for Direct DB Min Connections

Severity: Warning

Rationale: Oracle Identity Manager Direct DB Min Connections should set to 50

10.1.12 Oracle Identity Manager Jvm Jbo.Ampool.Doampooling

Description: Oracle Identity Manager Configuration rule for jbo.ampool.doampooling

Severity: Warning

Rationale: Oracle Identity Manager JVM configuration property jbo.ampool.doampooling should set to -1

10.1.13 Oracle Identity Manager Jvm Jbo.Ampool.Maxavailablesize

Description: Oracle Identity Manager Configuration rule for jbo.ampool.maxavailablesize

Severity: Warning

Rationale: Oracle Identity Manager JVM configuration property jbo.ampool.maxavailablesize should set to 120

10.1.14 Oracle Identity Manager Jvm Jbo.Ampool.Minavailablesize

Description: Oracle Identity Manager JVM Configuration rule for jbo.ampool.minavailablesize

Severity: Warning

Rationale: Oracle Identity Manager JVM configuration property jbo.ampool.minavailablesize should set to 1

10.1.15 Oracle Identity Manager Jvm Jbo.Ampool.Timetolive

Description: Oracle Identity Manager JVM Configuration rule for jbo.ampool.timetolive

Severity: Warning

Rationale: Oracle Identity Manager JVM configuration property jbo.ampool.timetolive should set to -1

10.1.16 Oracle Identity Manager Jvm Jbo.Connectfailover

Description: Oracle Identity Manager rule for jbo.connectfailover

Severity: Warning

Rationale: Oracle Identity Manager JVM configuration property jbo.connectfailover should set to false

10.1.17 Oracle Identity Manager Jvm Jbo.Doconnectionpooling

Description: Oracle Identity Manager Configuration rule for jbo.doconnectionpooling

Severity: Warning

Rationale: Oracle Identity Manager JVM configuration property jbo.doconnectionpooling should set to true

10.1.18 Oracle Identity Manager Jvm Jbo.Load.Components.Lazily

Description: Oracle Identity Manager Configuration rule for jbo.load.components.lazily

Severity: Warning

Rationale: Oracle Identity Manager JVM configuration property jbo.load.components.lazily should set to true

10.1.19 Oracle Identity Manager Jvm Jbo.Max.Cursors

Description: Oracle Identity Manager Configuration rule for jbo.max.cursors

Severity: Warning

Rationale: Oracle Identity Manager JVM configuration property jbo.max.cursors should set to 5

10.1.20 Oracle Identity Manager Jvm Jbo.Recyclethreshold

Description: Oracle Identity Manager Configuration rule for jbo.recyclethreshold

Severity: Warning

Rationale: Oracle Identity Manager JVM configuration property jbo.recyclethreshold should set to 60

10.1.21 Oracle Identity Manager Jvm Jbo.Txn.Disconnect_Level

Description: Oracle Identity Manager Configuration rule for jbo.txn.disconnect_level

Severity: Warning

Rationale: Oracle Identity Manager JVM configuration property jbo.txn.disconnect_level should set to 1

10.1.22 Oracle Identity Manager Uiworkmanager Maximum Threads

Description: Oracle Identity Manager Configuration rule for UIWorkManager Maximum Threads

Severity: Warning

Rationale: Oracle Identity Manager UIWorkManager Maximum Threads should set to 20

10.1.23 Oracle Identity Manager Weblogic Domain Inactive Connection Timeout

Description: Oracle Identity Manager Configuration rule for Weblogic Domain Inactive Connection Timeout

Severity: Warning

Rationale: Oracle Identity Manager Weblogic Domain Inactive Connection Timeout should set to 30

10.1.24 Oracle Identity Manager Weblogic Domain Initial Capacity

Description: Oracle Identity Manager Configuration rule for Weblogic Domain Initial Capacity

Severity: Warning

Rationale: Oracle Identity Manager Weblogic Domain Initial Capacity should set to 50

10.1.25 Oracle Identity Manager Weblogic Domain Max Capacity

Description: Oracle Identity Manager Configuration rule for Weblogic Domain Max Capacity

Severity: Warning

Rationale: Oracle Identity Manager Weblogic Domain Max Capacity should set to 150

10.1.26 Oracle Identity Manager Weblogic Domain Max Heap Size

Description: Oracle Identity Manager Configuration rule for Weblogic Domain Max Heap Size

Severity: Warning

Rationale: Oracle Identity Manager Weblogic Domain Max Heap Size should set to 4096

10.1.27 Oracle Identity Manager Weblogic Domain Min Capacity

Description: Oracle Identity Manager Configuration rule for Weblogic Domain Min Capacity

Severity: Warning

Rationale: Oracle Identity Manager Weblogic Domain Min Capacity should set to 50

10.1.28 Oracle Identity Manager Weblogic Domain Min Heap Size

Description: Oracle Identity Manager Configuration rule for Weblogic Domain Min Heap Size

Severity: Warning

Rationale: Oracle Identity Manager Weblogic Domain Min Heap Size should set to 1024

10.1.29 Oracle Identity Manager Weblogic Jms Maximum Number Of Messages

Description: Oracle Identity Manager Configuration rule for Weblogic JMS Maximum number of messages

Severity: Warning

Rationale: Oracle Identity Manager Weblogic JMS Maximum number of messages should set to 400000

10.1.30 Oracle Identity Manager Weblogic Jms Message Buffer Size

Description: Oracle Identity Manager Configuration rule for Weblogic JMS Message Buffer Size

Severity: Warning

Rationale: Oracle Identity Manager Weblogic JMS Message Buffer Size should be 200 MB

10.1.31 Oracle Identity Manager Oracle.Jdbc.Implicitstatementcachesize

Description: Oracle Identity Manager Configuration rule for oracle.jdbc.implicitStatementCacheSize

Severity: Warning

Rationale: Oracle Identity Manager Configuration rule for oracle.jdbc.implicitStatementCacheSize should set to 5

10.1.32 Oracle Identity Manager Oracle.Jdbc.Maxcachedbuffersize

Description: Oracle Identity Manager Configuration rule for oracle.jdbc.maxCachedBufferSize

Severity: Warning

Rationale: Oracle Identity Manager Configuration rule for oracle.jdbc.maxCachedBufferSize should set to 19

11

Oracle Identity Manager Cluster Compliance Standards

These are the compliance rules for the Oracle Identity Manager Cluster compliance standards

11.1 Oracle Identity Manager Cluster Configuration Compliance

The compliance rules for the Oracle Identity Manager Cluster Configuration Compliance standard follow.

11.1.1 Blocks Size

Description: Ensures Blocks size is at least 8192 bytes for the Oracle Database which Oracle Identity Manager is connecting to.

Severity: Minor Warning

Rationale: Having Blocks size less than 8192 bytes may slower the performance.

11.1.2 Change Log Adapter Parameters

Description: Change Log Adapter Parameters

Severity: Warning

Rationale: Make sure the Max Pool Size Should be 500, Operation Timeout should be 1500000 and Max Pool Wait whould be 1000

11.1.3 Cursor Sharing

Description: Ensures configuration property CURSOR_SHARING is set to FORCE for the Oracle Database which Oracle Identity Manager is connecting to.

Severity: Minor Warning

Rationale: Having CURSOR_SHARING to non-FORCE may slower the performance.

11.1.4 Database Statistics

Description: Gathering Database Statistics

Severity: Warning

Rationale: Database statistics is essential for the Oracle optimizer to select an optimal plan in running the SQL queries. It is recommended that the statistics be collected regularly for OIM and also OIM dependent schemas *_MDS, *_SOAINFRA, *_OPSS and *_ORASDPM.

11.1.5 Initial Number Of Database Writer Processes

Description: Ensures the initial number of Database Writer Process is at least 2 for the Oracle Database which Oracle Identity Manager is connecting to.

Severity: Minor Warning

Rationale: Having initial number of Database Writer Process less than 2 may slower the performance.

11.1.6 Keep Buffer Pool

Description: Ensures KEEP Buffer Pool is at least 800M for the Oracle Database which Oracle Identity Manager is connecting to.

Severity: Minor Warning

Rationale: Having KEEP Buffer Pool size below 800M may slower the performance.

11.1.7 Log Buffer

Description: Ensures Log Buffer is at least 15MB for the Oracle Database which Oracle Identity Manager is connecting to.

Severity: Minor Warning

Rationale: Having Log Buffer size below 15MB may slower the performance.

11.1.8 Maximum Number Of Open Cursors

Description: Ensures the maximum number of Open Cursors is less than 2000 for the Oracle Database which Oracle Identity Manager is connecting to.

Severity: Minor Warning

Rationale: Having maximum number of Open Cursors greater than 2000 may slower the performance.

11.1.9 Maximum Number Of Blocks Read In One I/O Operation

Description: Ensures the maximum number of blocks read in one I/O operation is at most 16 for the Oracle Database which Oracle Identity Manager is connecting to.

Severity: Minor Warning

Rationale: Having more than 16 blocks read in one I/O operation may slower the performance.

11.1.10 Query Rewrite Integrity

Description: Ensures the Query Rewrite Integrity is set to TRUSTED for the Oracle Database which Oracle Identity Manager is connecting to.

Severity: Minor Warning

Rationale: Having Query Rewrite Integrity set to non-TRUSTED may slower the performance.

11.1.11 Redo Logs

Description: Redo Logs

Severity: Warning

Rationale: Start with an initial size of 512 MB and continue to monitor redo logs for contention or frequent log switches.

11.1.12 Secure File Storage For Orchestration

Description: LOB segments in Orchestration related tables (ORCHPROCESS, ORCHEVENTS) should be stored in SECUREFILE. Migrate LOB columns ORCHESTRATION and CONTEXVAL in ORCHPROCESS table and RESULT column in ORCHEVENTS table to SECUREFILE from BASICFILE.

Severity: Warning

Rationale: LOB segments in Orchestration related tables (ORCHPROCESS, ORCHEVENTS) should be stored in SECUREFILE.

11.1.13 Session Cursors To Cache

Description: Ensures the number of Session Cursors to cache is at least 800 for the Oracle Database which Oracle Identity Manager is connecting to.

Severity: Minor Warning

Rationale: Having number of Session Cursors to cache below 800 may slower the performance.

11.1.14 Text Index Optimization(Catalog)

Description: Text Index optimization(Catalog)

Severity: Warning

Rationale: Make sure FAST_OPTIMIZE_CAT_TAGS and REBUILD_OPTIMIZE_CAT_TAGS jobs scheduled via DBMS_SCHEDULER should be enabled.These jobs help optimizing the text index on regular basis, removes the old data and minimizes the fragmentation, which can improve the search performance of Access Request Catalog.

11.1.15 User Adapter Parameters

Description: User Adapter Parameters

Severity: Warning

Rationale: Make sure the Max Pool Size Should be 500, Operation Timeout should be 1500000 and Max Pool Wait whould be 1000

12

Oracle Internet Directory Compliance Standards

These are the compliance rules for the Oracle Internet Directory compliance standards

12.1 Oracle Internet Directory Configuration Compliance For Oracle Fustion Applications

The compliance rules for the Oracle Internet Directory Configuration Compliance For Oracle Fustion Applications standard follow.

12.1.1 Maximum Database Connections

Description: This compliance standard rule checks if the Maximum Database Connestions setting is set to less than 10 for Oracle Fusion Applications.

Severity: Minor Warning

Rationale: Setting Maximum Database Connections greater than 10 could potentially affect the performance.

12.1.2 Oracle Internet Directory Server Processes

Description: This compliance standard rule checks if the number Oracle Internet Directory server processes is equal to the CPU sockets for Oracle Fusion Applications.

Severity: Minor Warning

Rationale: Setting the number Oracle Internet Directory server processes not equal to the number of CPU sockets could potentially affect the performance.

13

Oracle Listener Compliance Standards

These are the compliance rules for the Oracle Listener compliance standards

13.1 Basic Security Configuration For Oracle Listener

The compliance rules for the Basic Security Configuration For Oracle Listener standard follow.

13.1.1 Check Network Data Integrity On Server

Description: Ensures that the crypto_checksum_server parameter is set to recommended value in sqlnet.ora.

Severity: Warning

Rationale: This option ensures the integrity check for communication to prevent data modification.

13.1.2 Encrypt Network Communication On Server

Description: Ensures that the encryption_server parameter is set to recommended value in sqlnet.ora

Severity: Warning

Rationale: This option ensures that regardless of the settings on the user, if communication takes place it must be encrypted

13.1.3 Force Client Ssl Authentication

Description: Ensures that the ssl_client_authentication parameter is set to TRUE

Severity: Warning

Rationale: If TRUE Both the client and server authenticate to each other using certificates.It is preferable to have mutually authenticated SSL connections verifying the identity of both parties. If possible use client and server certificates for SSL connections. If client certificates are not supported in the enterprise, then set to FALSE.

13.1.4 Listener Logfile Permission

Description: Ensures that the listener logfile cannot be read by or written to by public

Severity: Critical

Rationale: The information in the logfile can reveal important network and database connection details. Allowing access to the log file can expose them to public scrutiny with possible security implications.

13.1.5 Listener Logfile Permission(Windows)

Description: Ensures that the listener logfile cannot be read by or written to by public

Severity: Critical

Rationale: The information in the logfile can reveal important network and database connection details. Allowing access to the log file can expose them to public scrutiny with possible security implications.

13.1.6 Listener Trace Directory Permission

Description: Ensures that the listener trace directory does not have public read/write permissions

Severity: Critical

Rationale: Allowing access to the trace directory can expose them to public scrutiny with possible security implications.

13.1.7 Listener Trace Directory Permission(Windows)

Description: Ensures that the listener trace directory does not have public read/write permissions

Severity: Critical

Rationale: Allowing access to the trace directory can expose them to public scrutiny with possible security implications.

13.1.8 Listener Trace File Permission

Description: Ensures that the listener trace file is not accessible to public

Severity: Critical

Rationale: Allowing access to the trace files can expose them to public scrutiny with possible security implications.

13.1.9 Listener Trace File Permission(Windows)

Description: Ensures that the listener trace file is not accessible to public

Severity: Critical

Rationale: Allowing access to the trace files can expose them to public scrutiny with possible security implications.

13.1.10 Ssl Cipher Suites Supported

Description: Ensures that the ssl_cipher_suites parameter is set to recommended value in sqlnet.ora

Severity: Warning

Rationale: This option is used to specify a cipher suite that will be used by the SSL connection. If the recommended cipher suite is not used, the SSL connection could be compromised.

13.1.11 Ssl Versions Supported

Description: Ensures that the ssl_version parameter is set to latest version .

Severity: Warning

Rationale: Usage of the most current version of SSL is recommended older versions of the SSL protocol are prone to attack or roll back. Do not set this parameter with Any.

13.2 High Security Configuration For Oracle Listener

The compliance rules for the High Security Configuration For Oracle Listener standard follow.

13.2.1 Accept Only Secure Registration Request

Description: Ensures that registration requests are accepted only for TCPS or IPC.

Severity: Warning

Rationale: Not configuring SECURE_REGISTER_listener_name parameter makes listener to accept registration request for any transport of a connection.

13.2.2 Algorithm For Network Data Integrity Check On Server

Description: Ensures that the crypto_checksum_type_server parameter is set to SHA1 in sqlnet.ora

Severity: Warning

Rationale: This option ensures the integrity check for communication is done using SHA1 Algorithm

13.2.3 Limit Loading External Dll And Libraries

Description: Ensures that the parameter EXTPROC_DLLS in listener.ora is set to ONLY

Severity: Warning

Rationale: To achieve a higher level of security in a production environment, to restrict the DLLs that the extproc agent can load by listing them explicitly in the listener.ora file.

13.2.4 Listener Default Name

Description: Ensures that the default name of the listener is not used

Severity: Warning

Rationale: Having a listener with the default name increases the risk of unauthorized access and denial of service attacks.

13.2.5 Listener Direct Administration

Description: Ensures that no runtime modifications to the listener configuration is allowed

Severity: Critical

Rationale: An attacker who has access to a running listener can perform runtime modifications (for example, SET operations) using the lsnrctl program.

13.2.6 Listener Inbound Connect Timeout

Description: Ensures that all incomplete inbound connections to Oracle Listener has a limited lifetime

Severity: Warning

Rationale: This limit protects the listener from consuming and holding resources for client connection requests that do not complete. A malicious user could use this to flood the listener with requests that result in a denial of service to authorized users.

13.2.7 Listener Logfile Owner

Description: Ensures that the listener log file is owned by the Oracle software owner

Severity: Critical

Rationale: The information in the logfile can reveal important network and database connection details. Having a log file not owned by the Oracle software owner can expose them to public scrutiny with possible security implications.

13.2.8 Listener Logging Status

Description: Ensures that listener logging is enabled

Severity: Warning

Rationale: Without listener logging attacks on the listener can go unnoticed.

13.2.9 Listener Password

Description: Ensures that access to listener is password protected

Severity: Warning

Rationale: Without password protection, a user can gain access to the listener. Once someone has access to the listener, he/she can stop the listener. He/she can also set a password and prevent others from managing the listener.

13.2.10 Listener Trace Directory Owner

Description: Ensures that the listener trace directory is a valid directory owned by Oracle software owner

Severity: Critical

Rationale: Having a trace directory not owned by the Oracle software owner can expose the trace files to public scrutiny with possible security implications.

13.2.11 Listener Trace File Owner

Description: Ensures that the listener trace file owner is same as the Oracle software owner

Severity: Critical

Rationale: Having trace files not owned by the Oracle software owner can expose them to public scrutiny with possible security implications.

13.2.12 Listener.Ora Permission

Description: Ensures that the file permissions for listener.ora are restricted to the owner of Oracle software

Severity: Critical

Rationale: If the listener.ora file is public readable, passwords may be extracted from this file. This can also lead to exposure of detailed information on the Listener, database,and application configuration. Also, if public has write permissions, a malicious user can remove any password that has been set on the listener.

13.2.13 Listener.Ora Permission(Windows)

Description: Ensures that the file permissions for listener.ora are restricted to the owner of Oracle software

Severity: Critical

Rationale: If the listener.ora file is public readable, passwords may be extracted from this file. This can also lead to exposure of detailed information on the Listener, database,and application configuration. Also, if public has write permissions, a malicious user can remove any password that has been set on the listener.

13.2.14 Oracle Net Inbound Connect Timeout

Description: Ensures that all incomplete inbound connections to Oracle Net has a limited lifetime

Severity: Warning

Rationale: Without this parameter or assigning it with a higher value , a client connection to the database server can stay open indefinitely or for the specified duration without authentication. Connections without authentication can introduce possible denial-of-service attacks, whereby malicious clients attempt to flood database servers with connect requests that consume resources.

13.2.15 Oracle Net Ssl_Cert_Revocation

Description: Ensures that the ssl_cert_revocation parameter is set to recommended value in sqlnet.ora

Severity: Warning

Rationale: This option Ensures revocation is required for checking CRLs for client certificate authentication. Revoked certificates can pose a threat to the integrity of the SSL channel and should not be trusted

13.2.16 Oracle Net Tcp Validnode Checking

Description: Ensures that tcp.validnode_checking parameter is set to yes.

Severity: Minor Warning

Rationale: Not setting valid node check can potentially allow anyone to connect to the sever, including a malicious user.

13.2.17 Restrict Sqlnet.Ora Permission

Description: Ensures that the sqlnet.ora file is not accessible to public

Severity: Critical

Rationale: If sqlnet.ora is public readable a malicious user may attempt to read this hence could lead to sensitive information getting exposed .For example, log and trace destination information of the client and server.

13.2.18 Restrict Sqlnet.Ora Permission(Windows)

Description: Ensures that the sqlnet.ora file is not accessible to public

Severity: Critical

Rationale: If sqlnet.ora is public readable a malicious user may attempt to read this hence could lead to sensitive information getting exposed .For example, log and trace destination information of the client and server.

13.2.19 Secure Remote Listener Administration

Description: Ensures that administration requests are accepted only for TCPS or IPC.

Severity: Warning

Rationale: Not configuring SECURE_CONTROL_listener_name parameter makes listener to serve control command for any transport of a connection.

13.2.20 Use Of Hostname In Listener.Ora

Description: Ensures that the listener host is specified as IP address and not hostname in the listener.ora

Severity: Warning

Rationale: An insecure Domain Name System (DNS) Server can be taken advantage of for mounting a spoofing attack. Name server failure can result in the listener unable to resolved the host.

13.2.21 Use Secure Transport For Administration And Registration

Description: Ensures that Administration and Registration requests are accepted only for TCPS or IPC transports

Severity: Warning

Rationale: Makes listener to accept administration and registration request for any transport of a connection

13.2.22 Tcp.Excludeded_Nodes

Description: Ensures that tcp.excludeded_nodes parameter is set.

Severity: Warning

Rationale: Not setting valid node check can potentially allow anyone to connect to the sever, including a malicious user.

13.2.23 Tcp.Invited_Nodes

Description: Ensures that tcp.invited_nodes parameter is set.

Severity: Warning

Rationale: Not setting valid node check can potentially allow anyone to connect to the sever, including a malicious user.

14

Oracle Real Application Cluster Database Compliance Standards

These are the compliance rules for the Oracle Real Application Cluster Database compliance standards

14.1 Basic Security Configuration For Oracle Cluster Database

The compliance rules for the Basic Security Configuration For Oracle Cluster Database standard follow.

14.1.1 Access To Dba_Roles View

Description: Ensures restricted access to DBA_ROLES view

Severity: Minor Warning

Rationale: DBA_ROLES view contains details of all roles in the database. Knowledge of the structure of roles in the database can be taken advantage of by a malicious user.

14.1.2 Access To Dba_Role_Privs View

Description: Ensures restricted access to DBA_ROLE_PRIVS view

Severity: Minor Warning

Rationale: The DBA_ROLE_PRIVS view lists the roles granted to users and other roles. Knowledge of the structure of roles in the database can be taken advantage of by a malicious user.

14.1.3 Access To Dba_Sys_Privs View

Description: Ensures restricted access to DBA_SYS_PRIVS view

Severity: Minor Warning

Rationale: DBA_SYS_PRIVS view can be queried to find system privileges granted to roles and users. Knowledge of the structure of roles in the database can be taken advantage of bya malicious user.

14.1.4 Access To Dba_Tab_Privs View

Description: Ensures restricted access to DBA_TAB_PRIVS view

Severity: Minor Warning

Rationale: Lists privileges granted to users or roles on objects in the database. Knowledge of the structure of roles in the database can be taken advantage of by a malicious user.

14.1.5 Access To Dba_Users View

Description: Ensures restricted access to DBA_USERS view

Severity: Minor Warning

Rationale: Contains user password hashes and other account information. Access to this information can be used to mount brute-force attacks.

14.1.6 Access To Stats$Sqltext Table

Description: Ensures restricted access to STATS$SQLTEXT table

Severity: Minor Warning

Rationale: This table provides full text of the recently-executed SQL statements. The SQL statements can reveal sensitive information.

14.1.7 Access To Stats$Sql_Summary Table

Description: Ensures restricted access to STATS$SQL_SUMMARY table

Severity: Minor Warning

Rationale: Contains first few lines of SQL text of the most resource intensive commands given to the server. Sql statements executed without bind variables can show up here exposing privileged information.

14.1.8 Access To Sys.Aud$ Table

Description: Ensures restricted access to SYS.AUD$ table

Severity: Minor Warning

Rationale: A knowlegeable and malicious user can gain access to sensitive audit information.

14.1.9 Access To Sys.Source$ Table

Description: Ensures restricted access to SYS.SOURCE$ table

Severity: Minor Warning

Rationale: Contains source of all stored packages units in the database.

14.1.10 Access To Sys.User$ Table

Description: Ensures restricted access to SYS.USER$ table

Severity: Minor Warning

Rationale: Username and password hash may be read from the SYS.USER$ table, enabling a hacker to launch a brute-force attack.

14.1.11 Access To Sys.User_History$ Table

Description: Ensures restricted access to SYS.USER_HISTORY$ table

Severity: Minor Warning

Rationale: Username and password hash may be read from the SYS.USER_HISTORY$ table, enabling a hacker to launch a brute-force attack.

14.1.12 Allowed Logon Version

Description: Ensures that the server allows logon from clients with a matching version or higher only.

Severity: Warning

Rationale: Setting the parameter SQLNET.ALLOWED_LOGON_VERSION in sqlnet.ora to a version lower than the server version will force the server to use a less secure authentication protocol

14.1.13 Audit File Destination

Description: Ensures that access to the audit files directory is restricted to the owner of the Oracle software set and the DBA group.

Severity: Critical

Rationale: The AUDIT_FILE_DEST initialization parameter specifies the directory where the Oracle auditing facility creates the audit files. Giving public read permission to this directory may reveal important information such as logging information of startup, shutdown, and privileged connections.

14.1.14 Audit File Destination(Windows)

Description: Ensures that access to the audit files directory is restricted to the owner of the Oracle software set and the DBA group.

Severity: Critical

Rationale: The AUDIT_FILE_DEST initialization parameter specifies the directory where the Oracle auditing facility creates the audit files. Giving public read permission to this directory may reveal important information such as logging information of startup, shutdown, and privileged connections.

14.1.15 Auditing Of Sys Operations Enabled

Description: Ensures sessions for users who connect as SYS are fully audited

Severity: Warning

Rationale: The AUDIT_SYS_OPERATIONS parameter enables or disables the auditing of operations issued by user SYS, and users connecting with SYSDBA or SYSOPER privileges.

14.1.16 Background Dump Destination(Windows)

Description: Ensures that access to the trace files directory is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: Background processes such as the log writer process and the database writer process use trace files to record occurrences and exceptions of database operations, as well as errors. The trace files are stored in the directory specified by the BACKGROUND_DUMP_DEST initialization parameter. Giving public read permission to this directory may reveal important and sensitive internal details of the database and applications.

14.1.17 Check Network Data Integrity On Server

Description: Ensures that the crypto_checksum_server parameter is set to recommended value in sqlnet.ora.

Severity: Warning

Rationale: This option ensures the integrity check for communication to prevent data modification.

14.1.18 Control File Permission

Description: Ensures that access to the control files directory is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: Control files are binary configuration files that control access to data files. Control files are stored in the directory specified by the CONTROL_FILES initialization parameter. A public write privilege on this directory could pose a serious security risk.

14.1.19 Control File Permission(Windows)

Description: Ensures that access to the control files directory is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: Control files are binary configuration files that control access to data files. Control files are stored in the directory specified by the CONTROL_FILES initialization parameter. A public write privilege on this directory could pose a serious security risk.

14.1.20 Core Dump Destination

Description: Ensures that access to the core dump files directory is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: Core dump files are stored in the directory specified by the CORE_DUMP_DEST initialization parameter. A public read privilege on this directory could expose sensitive information from the core dump files.

14.1.21 Core Dump Destination(Windows)

Description: Ensures that access to the core dump files directory is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: Core dump files are stored in the directory specified by the CORE_DUMP_DEST initialization parameter. A public read privilege on this directory could expose sensitive information from the core dump files.

14.1.22 Data Dictionary Protected

Description: Ensures data dictionary protection is enabled

Severity: Critical

Rationale: The 07_DICTIONARY_ACCESSIBILITY parameter controls access to the data dictionary. Setting the 07_DICTIONARY_ACCESSIBILITY to TRUE allows users with ANY system privileges to access the data dictionary. As a result, these user accounts can be exploited to gain unauthorized access to data.

14.1.23 Default Passwords

Description: Ensure there are no default passwords for known accounts

Severity: Warning

Rationale: A malicious user can gain access to the database using default passwords.

14.1.24 Enable Database Auditing

Description: Ensures database auditing is enabled

Severity: Minor Warning

Rationale: The AUDIT_TRAIL parameter enables or disables database auditing. For database version 12c and above Unified Auditing can be used. Auditing enhances security because it enforces accountability, provides evidence of misuse, and is frequently required for regulatory compliance. Auditing also enables system administrators to implement enhanced protections, early detection of suspicious activities, and finely-tuned security responses.

14.1.25 Encrypt Network Communication On Server

Description: Ensures that the encryption_server parameter is set to recommended value in sqlnet.ora

Severity: Warning

Rationale: This option ensures that regardless of the settings on the user, if communication takes place it must be encrypted

14.1.26 Execute Privileges On Dbms_Job To Public

Description: Ensures PUBLIC is not granted EXECUTE privileges on DBMS_JOB package

Severity: Critical

Rationale: Granting EXECUTE privilege to PUBLIC on DBMS_JOB package allows users to schedule jobs on the database.

14.1.27 Execute Privileges On Dbms_Sys_Sql To Public

Description: Ensures PUBLIC is not granted EXECUTE privileges on DBMS_SYS_SQL package

Severity: Critical

Rationale: The DBMS_SYS_SQL package can be used to run PL/SQL and SQL as the owner of the procedure rather than the caller.

14.1.28 Force Client Ssl Authentication

Description: Ensures that the ssl_client_authentication parameter is set to TRUE

Severity: Warning

Rationale: If TRUE Both the client and server authenticate to each other using certificates.It is preferable to have mutually authenticated SSL connections verifying the identity of both parties. If possible use client and server certificates for SSL connections. If client certificates are not supported in the enterprise, then set to FALSE.

14.1.29 Initialization Parameter File Permission

Description: Ensures that access to the initialization paramater file is restricted to the owner of the Oracle software set and the DBA group

Severity: Warning

Rationale: Oracle traditionally stores initialization parameters in a text initialization parameter file. A publicly accessible initialization parameter file can be scanned for sensitive initialization parameters exposing the security policies of the database. The IFILE can also be searched for the weaknesses of the Oracle database configuration setting.

14.1.30 Initialization Parameter File Permission(Windows)

Description: Ensures that access to the initialization paramater file is restricted to the owner of the Oracle software set and the DBA group

Severity: Warning

Rationale: Oracle traditionally stores initialization parameters in a text initialization parameter file. A publicly accessible initialization parameter file can be scanned for sensitive initialization parameters exposing the security policies of the database. The IFILE can also be searched for the weaknesses of the Oracle database configuration setting.

14.1.31 Oracle Home Datafile Permission

Description: Ensures that access to the datafiles is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: The datafiles contain all the database data. If datafiles are readable to public, they can be read by a user who has no database privileges on the data.

14.1.32 Oracle Home Datafile Permission(Windows)

Description: Ensures that access to the datafiles is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: The datafiles contain all the database data. If datafiles are readable to public, they can be read by a user who has no database privileges on the data.

14.1.33 Oracle Home Executable Files Owner

Description: Ensures that the ownership of all files and directories in the ORACLE_HOME/bin folder is the same as the Oracle software installation owner

Severity: Critical

Rationale: Incorrect file permissions on some of the Oracle files can cause major security issues.

14.1.34 Oracle Home File Permission

Description: Ensures that all files in the ORACLE_HOME directories (except for ORACLE_HOME/bin) do not have public read, write and execute permissions

Severity: Warning

Rationale: Incorrect file permissions on some of the Oracle files can cause major security issues.

14.1.35 Oracle Home File Permission(Windows)

Description: Ensures that all files in the ORACLE_HOME directories (except for ORACLE_HOME/bin) do not have public read, write and execute permissions

Severity: Warning

Rationale: Incorrect file permissions on some of the Oracle files can cause major security issues.

14.1.36 Oracle Net Client Log Directory Permission

Description: Ensures that the client log directory is a valid directory owned by Oracle set with no permissions to public

Severity: Critical

Rationale: Log files provide information contained in an error stack. An error stack refers to the information that is produced by each layer in an Oracle communications stack as the result of a network error. The information in log files can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

14.1.37 Oracle Net Client Log Directory Permission(Windows)

Description: Ensures that the client log directory is a valid directory owned by Oracle set with no permissions to public

Severity: Critical

Rationale: Log files provide information contained in an error stack. An error stack refers to the information that is produced by each layer in an Oracle communications stack as the result of a network error. The information in log files can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

14.1.38 Oracle Net Client Trace Directory Permission

Description: Ensures that the client trace directory is a valid directory owned by Oracle set with no permissions to public

Severity: Critical

Rationale: Tracing produces a detailed sequence of statements that describe network events as they are executed. Tracing an operation enables you to obtain more information on the internal operations of the components of Oracle Net Services than is provided in a log file. The information in this file can reveal important network and

database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

14.1.39 Oracle Net Client Trace Directory Permission(Windows)

Description: Ensures that the client trace directory is a valid directory owned by Oracle set with no permissions to public

Severity: Critical

Rationale: Tracing produces a detailed sequence of statements that describe network events as they are executed. Tracing an operation enables you to obtain more information on the internal operations of the components of Oracle Net Services than is provided in a log file. The information in this file can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

14.1.40 Oracle Net Server Log Directory Permission

Description: Ensures that the server log directory is a valid directory owned by Oracle set with no permissions to public

Severity: Critical

Rationale: Log files provide information contained in an error stack. An error stack refers to the information that is produced by each layer in an Oracle communications stack as the result of a network error. The information in log files can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

14.1.41 Oracle Net Server Log Directory Permission(Windows)

Description: Ensures that the server log directory is a valid directory owned by Oracle set with no permissions to public

Severity: Critical

Rationale: Log files provide information contained in an error stack. An error stack refers to the information that is produced by each layer in an Oracle communications stack as the result of a network error. The information in log files can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

14.1.42 Oracle Net Server Trace Directory Permission

Description: Ensures that the server trace directory is a valid directory owned by Oracle set with no permissions to public

Severity: Critical

Rationale: Tracing produces a detailed sequence of statements that describe network events as they are executed. Tracing an operation enables you to obtain more information on the internal operations of the components of Oracle Net Services than is provided in a log file. The information in this file can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

14.1.43 Oracle Net Server Trace Directory Permission(Windows)

Description: Ensures that the server trace directory is a valid directory owned by Oracle set with no permissions to public

Severity: Critical

Rationale: Tracing produces a detailed sequence of statements that describe network events as they are executed. Tracing an operation enables you to obtain more information on the internal operations of the components of Oracle Net Services than is provided in a log file. The information in this file can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

14.1.44 Protocol Error Further Action

Description: Ensures that the SEC_PROTOCOL_ERROR_FURTHER_ACTION parameter is set to either DROP or DELAY

Severity: Critical

Rationale: If default value CONTINUE is used, the server process continues execution even if bad packets are received. The database server may be subject to a Denial of Service (DoS) if bad packets continue to be sent by a malicious client

14.1.45 Protocol Error Trace Action

Description: Ensures that the sec_protocol_error_trace_action parameter is set to either LOG or ALERT

Severity: Critical

Rationale: SEC_PROTOCOL_ERROR_TRACE_ACTION specifies the action that the database should take when bad packets are received from a possibly malicious client. NONE should not be used as the database server ignores the bad packets and does not generate any trace files or log messages. If default value TRACE is used then the database server generates a detailed trace file and should only be used when debugging

14.1.46 Password Complexity Verification Function Usage

Description: Ensures PASSWORD_VERIFY_FUNCTION resource for the profile is set

Severity: Critical

Rationale: Having passwords that do not meet minimum complexity requirements offer substantially less protection than complex passwords.

14.1.47 Password Grace Time

Description: Ensures that all profiles have PASSWORD_GRACE_TIME set to a reasonable number of days

Severity: Critical

Rationale: A high value for the PASSWORD_GRACE_TIME parameter may cause serious database security issues by allowing the user to keep the same password for a long time.

14.1.48 Password Lifetime

Description: Ensures that all profiles have PASSWORD_LIFE_TIME set to a reasonable number of days

Severity: Warning

Rationale: A long password life time gives hackers a long time to try and cook the password. May cause serious database security issues.

14.1.49 Password Locking Time

Description: Ensures PASSWORD_LOCK_TIME is set to a reasonable number of days for all profiles

Severity: Warning

Rationale: Having a low value increases the likelihood of Denial of Service attacks.

14.1.50 Public Trace Files

Description: Ensures database trace files are not public readable

Severity: Critical

Rationale: If trace files are readable by the PUBLIC group, a malicious user may attempt to read the trace files that could lead to sensitive information being exposed.

14.1.51 Remote Os Authentication

Description: Ensure REMOTE_OS_AUTHENT initialization parameter is set to FALSE

Severity: Critical

Rationale: A malicious user can gain access to the database if remote OS authentication is allowed.

14.1.52 Remote Os Role

Description: Ensure REMOTE_OS_ROLES initialization parameter is set to FALSE

Severity: Critical

Rationale: A malicious user can gain access to the database if remote users can be granted privileged roles.

14.1.53 Restricted Privilege To Execute Utl_Http

Description: Ensure PUBLIC does not have execute privileges on the UTL_HTTP package

Severity: Critical

Rationale: Privileges granted to the PUBLIC role automatically apply to all users. A malicious user can gain access to email, network and http modules using the EXECUTE privilege.

14.1.54 Restricted Privilege To Execute Utl_Smtp

Description: Ensure PUBLIC does not have execute privileges on the UTL_SMTP package

Severity: Critical

Rationale: Privileges granted to the PUBLIC role automatically apply to all users. A malicious user can gain access to email, network and http modules using the EXECUTE privilege.

14.1.55 Restricted Privilege To Execute Utl_Tcp

Description: Ensure PUBLIC does not have execute privileges on the UTL_TCP package

Severity: Critical

Rationale: Privileges granted to the PUBLIC role automatically apply to all users. A malicious user can gain access to email, network and http modules using the EXECUTE privilege.

14.1.56 Ssl Cipher Suites Supported

Description: Ensures that the ssl_cipher_suites parameter is set to recommended value in sqlnet.ora

Severity: Warning

Rationale: This option is used to specify a cipher suite that will be used by the SSL connection. If the recommended cipher suite is not used, the SSL connection could be compromised.

14.1.57 Ssl Versions Supported

Description: Ensures that the ssl_version parameter is set to latest version .

Severity: Warning

Rationale: Usage of the most current version of SSL is recommended older versions of the SSL protocol are prone to attack or roll back. Do not set this parameter with Any.

14.1.58 Server Parameter File Permission

Description: Ensures that access to the server paramater file is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: A server parameter file (SPFILE) lets you store and manage your initialization parameters persistently in a server-side disk file. A publicly accessible SPFILE can be scanned for sensitive initialization parameters exposing the security policies of the database. The SPFILE can also be searched for the weaknesses of the Oracle database configuration setting.

14.1.59 Server Parameter File Permission(Windows)

Description: Ensures that access to the server paramater file is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: A server parameter file (SPFILE) lets you store and manage your initialization parameters persistently in a server-side disk file. A publicly accessible SPFILE can be scanned for sensitive initialization parameters exposing the security

policies of the database. The SPFILE can also be searched for the weaknesses of the Oracle database configuration setting.

14.1.60 Use Of Appropriate Umask On Unix Systems

Description: On UNIX systems, ensure that the owner of the Oracle software has an appropriate umask value of 022 set

Severity: Warning

Rationale: If umask is not set to an appropriate value (like 022), log or trace files might become accessible to public exposing sensitive information.

14.1.61 Use Of Database Links With Cleartext Password

Description: Ensures database links with clear text passwords are not used

Severity: Warning

Rationale: The table SYS.LINK$ contains the clear text password used by the database link. A malicious user can read clear text password from SYS.LINK$ table that can lead to undesirable consequences.

14.1.62 User Dump Destination

Description: Ensures that access to the trace files directory is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: The trace files for server processes are stored in the directory specified by the USER_DUMP_DEST initialization parameter. Giving public read permission to this directory may reveal important and sensitive internal details of the database and applications.

14.1.63 User Dump Destination(Windows)

Description: Ensures that access to the trace files directory is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: The trace files for server processes are stored in the directory specified by the USER_DUMP_DEST initialization parameter. Giving public read permission to this directory may reveal important and sensitive internal details of the database and applications.

14.1.64 Using Externally Identified Accounts

Description: Ensures that the OS authentication prefix is set to a value other than OPS $

Severity: Warning

Rationale: The OS_AUTHENT_PREFIX parameter specifies a prefix used to authenticate users attempting to connect to the server. When a connection request is attempted, Oracle compares the prefixed username with usernames in the database. Using a prefix, especially OPS$, tends to result in an insecure configuration as an account can be authenticated either as an operating system user or with the password used in the IDENTIFIED BY clause. Attackers are aware of this and will attack these accounts.

14.1.65 Utility File Directory Initialization Parameter Setting

Description: Ensures that the Utility File Directory (UTL_FILE_DIR) initialization parameter is not set to one of '*', '.', core dump trace file locations

Severity: Critical

Rationale: Specifies the directories which the UTL_FILE package can access. Having the parameter set to asterisk (*), period (.), or to sensitive directories, could expose them to all users having execute privilege on the UTL_FILE package.

14.1.66 Well Known Accounts

Description: Checks for accessibility of well-known accounts

Severity: Warning

Rationale: A knowledgeable malicious user can gain access to the database using a well-known account.

14.2 Configuration Best Practices For Oracle Rac Database

The compliance rules for the Configuration Best Practices For Oracle Rac Database standard follow.

14.2.1 Force Logging Disabled

Description: When Data Guard is being used, checks the primary database for disabled force logging

Severity: Warning

Rationale: The primary database is not in force logging mode. As a result unlogged direct writes in the primary database cannot be propagated to the standby database.

14.2.2 Insufficient Number Of Control Files

Description: Checks for use of a single control file

Severity: Critical

Rationale: The control file is one of the most important files in an Oracle database. It maintains many physical characteristics and important recovery information about the database. If youlose the only copy of the control file due to a media error, there will be unnecessary down time and other risks.

14.3 High Security Configuration For Oracle Cluster Database

The compliance rules for the High Security Configuration For Oracle Cluster Database standard follow.

14.3.1 $Oracle_Home/Network/Admin File Permission

Description: Ensures the files in $ORACLE_HOME/network/admin ownership is restricted to the Oracle software set, group is restricted to DBA group and Public does not have write permission

Severity: Warning

Rationale: Not restricting ownership of network/admin to the Oracle software set and DBA group may cause security issues by exposing net configuration data to malicious users

14.3.2 $Oracle_Home/Network/Admin File Permission(Windows)

Description: Ensures the files in $ORACLE_HOME/network/admin ownership is restricted to the Oracle software set, group is restricted to DBA group and Public does not have write permission

Severity: Warning

Rationale: Not restricting ownership of network/admin to the Oracle software set and DBA group may cause security issues by exposing net configuration data to malicious users

14.3.3 Access To *_Catalog_* Roles

Description: Ensure grant of *_CATALOG_* is restricted

Severity: Critical

Rationale: *_CATALOG_* Roles have critical access to database objects, that can lead to exposure of vital information in database system.

14.3.4 Access To All_Source View

Description: Ensures restricted access to ALL_SOURCE view

Severity: Minor Warning

Rationale: ALL_SOURCE view contains source of all stored packages in the database.

14.3.5 Access To Dba_* Views

Description: Ensures SELECT privilege is never granted to any DBA_ view

Severity: Warning

Rationale: The DBA_* views provide access to privileges and policy settings of the database. Some of these views also allow viewing of sensitive PL/SQL code that can be used to understand the security policies.

14.3.6 Access To Role_Role_Privs View

Description: Ensures restricted access to ROLE_ROLE_PRIVS view

Severity: Minor Warning

Rationale: Lists roles granted to other roles. Knowledge of the structure of roles in the database can be taken advantage of by a malicious user.

14.3.7 Access To Sys.Link$ Table

Description: Ensures restricted access to LINK$ table

Severity: Minor Warning

Rationale: A knowlegeable and malicious user can gain access to user passwords from the SYS.LINK$ table.

14.3.8 Access To User_Role_Privs View

Description: Ensures restricted access to USER_ROLE_PRIVS view

Severity: Minor Warning

Rationale: Lists the roles granted to the current user. Knowledge of the structure of roles in the database can be taken advantage of by a malicious user.

14.3.9 Access To User_Tab_Privs View

Description: Ensures restricted access to USER_TAB_PRIVS view

Severity: Minor Warning

Rationale: Lists the grants on objects for which the user is the owner, grantor or grantee. Knowledge of the grants in the database can be taken advantage of by a malicious user.

14.3.10 Access To V$ Synonyms

Description: Ensures SELECT privilege is not granted to any V$ synonyms

Severity: Critical

Rationale: V$ tables contain sensitive information about Oracle database and should only be accessible by system administrators. Check for any user that has access and revoke where possible

14.3.11 Access To V$ Views

Description: Ensures SELECT privilege is not granted to any V$ Views

Severity: Critical

Rationale: V$ tables contain sensitive information about Oracle database and should only be accessible by system administrators. Check for any user that has access and revoke where possible

14.3.12 Access To X_$ Views

Description: Ensure access on X$ views is restricted

Severity: Critical

Rationale: This can lead to revealing of internal database structure information.

14.3.13 Algorithm For Network Data Integrity Check On Server

Description: Ensures that the crypto_checksum_type_server parameter is set to SHA1 in sqlnet.ora

Severity: Warning

Rationale: This option ensures the integrity check for communication is done using SHA1 Algorithm

14.3.14 Audit Alter Any Table Privilege

Description: Ensures ALTER ANY TABLE Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing ALTER ANY TABLE will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

14.3.15 Audit Alter User Privilege

Description: Ensures ALTER USER Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing ALTER USER will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

14.3.16 Audit Aud$ Privilege

Description: Ensures AUD$ is being audited by access for all users

Severity: Critical

Rationale: Auditing AUD$ will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

14.3.17 Audit Create Any Library Privilege

Description: Ensures CREATE ANY LIBRARY is being audited by access for all users

Severity: Critical

Rationale: Auditing CREATE ANY LIBRARY will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

14.3.18 Audit Create Library Privilege

Description: Ensures CREATE LIBRARY Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing CREATE LIBRARY will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

14.3.19 Audit Create Role Privilege

Description: Ensures CREATE ROLE Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing the creation of roles will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

14.3.20 Audit Create Session Privilege

Description: Ensures CREATE SESSION Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing CREATE SESSION will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

14.3.21 Audit Create User Privilege

Description: Ensures CREATE USER Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing CREATE USER will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

14.3.22 Audit Drop Any Procedure Privilege

Description: Ensures DROP ANY PROCEDURE Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing DROP ANY PROCEDURE will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

14.3.23 Audit Drop Any Role Privilege

Description: Ensures DROP ANY ROLE Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing the creation of roles will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

14.3.24 Audit Drop Any Table Privilege

Description: Ensures DROP ANY TABLE Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing DROP ANY TABLE will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

14.3.25 Audit Execute Any Procedure Privilege

Description: Ensures EXECUTE ANY PROCEDURE Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing the creation of roles will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

14.3.26 Audit Grant Any Object Privilege

Description: Ensures every use of GRANT ANY OBJECT privilege is being audited for non-Administrative (SYSDBA) users.

Severity: Critical

Rationale: Auditing GRANT ANY OBJECT privilege will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

14.3.27 Audit Grant Any Privilege

Description: Ensures GRANT ANY PRIVILEGE is being audited by access for all users

Severity: Critical

Rationale: Auditing GRANT ANY PRIVILEGE will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

14.3.28 Audit Insert Failure

Description: Ensures that insert failures are audited for critical data objects

Severity: Warning

Rationale: Not auditing insert failures for critical data objects may allow a malicious user to infiltrate system security..

14.3.29 Audit Select Any Dictionary Privilege

Description: Ensures SELECT ANY DICTIONARY Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing SELECT ANY DICTIONARY will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

14.3.30 Background Dump Destination

Description: Ensures that access to the trace files directory is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: Background processes such as the log writer process and the database writer process use trace files to record occurrences and exceptions of database operations, as well as errors. The trace files are stored in the directory specified by the BACKGROUND_DUMP_DEST initialization parameter. Giving public read permission to this directory may reveal important and sensitive internal details of the database and applications.

14.3.31 Case Sensitive Logon

Description: Ensures that the sec_case_sensitive_logon parameter is set to true

Severity: Critical

Rationale: This increases the complexity of passwords and helps defend against brute force password attacks

14.3.32 Connect Time

Description: Ensure that users profile settings CONNECT_TIME have appropriate value set for the particular database and application

Severity: Critical

Rationale: Sessions held open for excessive periods of time can consume system resources and cause a denial of service for other users of the Oracle database. The CONNECT_TIME parameter limits the upper bound on how long a session can be held open. This parameter is specified in minutes. Sessions that have exceeded their connect time are aborted and rolled back

14.3.33 Cpu Per Session

Description: Ensures that all profiles have CPU_PER_SESSION set to a reasonable number of CPU cycles

Severity: Critical

Rationale: Allowing a single application or user to consume excessive CPU resources will result in a denial of service to the Oracle database

14.3.34 Db Securefile

Description: Ensure that all LOB files created by Oracle are created as SecureFiles

Severity: Critical

Rationale: For LOBs to get treated as SecureFiles, set COMPATIBILE Initialization Param to 11.1 or higher. If there is a LOB column with two partitions (one that has a tablespace for which ASSM is enabled and one that has a tablespace for which ASSM is not enabled), then LOBs in the partition with the ASSM-enabled tablespace will be treated as SecureFiles and LOBs in the other partition will be treated as BasicFile LOBs. Setting db_securefile to ALWAYS makes sure that any LOB file created is a secure file

14.3.35 Dispatchers

Description: Ensures that the DISPATCHERS parameter is not set

Severity: Critical

Rationale: This will disable default ports ftp: 2100 and http: 8080. Removing the XDB ports will reduce the attack surface of the Oracle server. It is recommended to disable these ports if production usage is not required

14.3.36 Execute Privileges On Dbms_Lob To Public

Description: Ensures PUBLIC group is not granted EXECUTE privileges to the DBMS_LOB package

Severity: Critical

Rationale: The DBMS_LOB package can be used to access any file on the system as the owner of the Oracle software installation.

14.3.37 Execute Privileges On Utl_File To Public

Description: Ensure PUBLIC does not have EXECUTE privilege on the UTL_FILE package

Severity: Critical

Rationale: Privileges granted to the PUBLIC role automatically apply to all users. A malicious user can read and write arbitrary files in the system when granted the UTL_FILE privilege.

14.3.38 Execute Privilege On Sys.Dbms_Export_Extension To Public

Description: Ensure PUBLIC does not have execute privileges on the SYS.DBMS_EXPORT_EXTENSION package

Severity: Critical

Rationale: Privileges granted to the PUBLIC role automatically apply to all users. DBMS_EXPORT_EXTENSION can allow sql injection. Thus a malicious will be able to take advantage.

14.3.39 Execute Privilege On Sys.Dbms_Random Public

Description: Ensure PUBLIC does not have execute privileges on the SYS.DBMS_RANDOM package

Severity: Critical

Rationale: Privileges granted to the PUBLIC role automatically apply to all users. DBMS_RANDOM can allow sql injection. Thus a malicious will be able to take advantage.

14.3.40 Granting Select Any Table Privilege

Description: Ensures SELECT ANY PRIVILEGE is never granted to any user or role

Severity: Warning

Rationale: The SELECT ANY TABLE privilege can be used to grant users or roles with the ability to view data in tables that are not owned by them. A malicious user with access to any user account that has this privilege can use this to gain access to sensitive data.

14.3.41 Ifile Referenced File Permission

Description: Ensures that access to the files referenced by the IFILE parameter is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: The IFILE initialization parameter can be used to embed the contents of another initialization parameter file into the current initialization parameter file. A publicly accessible initialization parameter file can be scanned for sensitive initialization parameters exposing the security policies of the database. Initialization parameter file can also be searched for the weaknesses of the Oracle database configuration setting.

14.3.42 Ifile Referenced File Permission(Windows)

Description: Ensures that access to the files referenced by the IFILE parameter is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: The IFILE initialization parameter can be used to embed the contents of another initialization parameter file into the current initialization parameter file. A publicly accessible initialization parameter file can be scanned for sensitive initialization parameters exposing the security policies of the database. Initialization parameter file can also be searched for the weaknesses of the Oracle database configuration setting.

14.3.43 Logical Reads Per Session

Description: Ensure that users profile settings LOGICAL_READS_ PER_SESSION have appropriate value set for the particular database and application

Severity: Critical

Rationale: Allowing a single application or user to perform excessive amounts of reads to disk will result in a denial of service to the Oracle database

14.3.44 Limit Os Authentication

Description: Ensures database accounts does not rely on OS authentication

Severity: Critical

Rationale: If the host operating system has a required userid for database account for which password is set EXTERNAL, then Oracle does not check its credentials anymore. It simplyassumes the host must have done its authentication and lets the user into the database without any further checking.

14.3.45 Log Archive Destination Owner

Description: Ensures that the server's archive logs directory is a valid directory owned by Oracle software owner

Severity: Critical

Rationale: LogMiner can be used to extract database information from the archive logs if the directory specified by LOG_ARCHIVE_DEST parameter (in init.ora file) is not owned by the owner of the Oracle software installation or has permissions for others.

14.3.46 Log Archive Destination Permission

Description: Ensures that the server's archive logs are not accessible to public

Severity: Critical

Rationale: LogMiner can be used to extract database information from the archive logs if the directory specified by LOG_ARCHIVE_DEST parameter (in init.ora file) is not owned by the owner of the Oracle software installation or has permissions for others.

14.3.47 Log Archive Destination Permission(Windows)

Description: Ensures that the server's archive logs are not accessible to public

Severity: Critical

Rationale: LogMiner can be used to extract database information from the archive logs if the directory specified by LOG_ARCHIVE_DEST parameter (in init.ora file) is not owned by the owner of the Oracle software installation or has permissions for others.

14.3.48 Log Archive Duplex Destination Owner

Description: Ensures that the server's archive logs directory is a valid directory owned by Oracle software owner

Severity: Critical

Rationale: LogMiner can be used to extract database information from the archive logs if the directory specified by LOG_ARCHIVE_DUPLEX_DEST parameter (in init.ora file) is not owned by the owner of the Oracle software installation or has permissions for others.

14.3.49 Log Archive Duplex Destination Permission

Description: Ensures that the server's archive logs are not accessible to public

Severity: Critical

Rationale: LogMiner can be used to extract database information from the archive logs if the directory specified by LOG_ARCHIVE_DUPLEX_DEST parameter (in init.ora file) is not owned by the owner of the Oracle software installation or has permissions for others.

14.3.50 Log Archive Duplex Destination Permission(Windows)

Description: Ensures that the server's archive logs are not accessible to public

Severity: Critical

Rationale: LogMiner can be used to extract database information from the archive logs if the directory specified by LOG_ARCHIVE_DUPLEX_DEST parameter (in init.ora file) is not owned by the owner of the Oracle software installation or has permissions for others.

14.3.51 Naming Database Links

Description: Ensures that the name of a database link is the same as that of the remote database

Severity: Warning

Rationale: Database link names that do not match the global names of the databases to which they are connecting can cause an administrator to inadvertently give access to a production server from a test or development server. Knowledge of this can be used by a malicious user to gain access to the target database.

14.3.52 Oracle_Home Network Admin Owner

Description: Ensures $ORACLE_HOME/network/admin ownership is restricted to the Oracle software set and DBA group

Severity: Warning

Rationale: Not restricting ownership of network/admin to the Oracle software set and DBA group may cause security issues by exposing net configuration data to malicious users

14.3.53 Os Roles

Description: Ensure roles are stored, managed, and protected in the database rather than files external to the DBMS.

Severity: Warning

Rationale: If Roles are managed by OS, it can cause serious security issues.

14.3.54 Oracle Agent Snmp Read-Only Configuration File Owner

Description: Ensures Oracle Agent SNMP read-only configuration file (snmp_ro.ora) is owned by Oracle software owner

Severity: Warning

Rationale: The Oracle Agent SNMP read-only configuration file (snmp_ro.ora) contains the listening address of the agent, the names of SQL*Net listener and Oracle database servicesit knows about, plus tracing parameters. A publicly accessible SNMP read-only configuration file can be used to extract sensitive data like the tracing directory location, dbsnmp address, etc.

14.3.55 Oracle Agent Snmp Read-Only Configuration File Permission

Description: Ensures Oracle Agent SNMP read-only configuration file (snmp_ro.ora) permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: The Oracle Agent SNMP read-only configuration file (snmp_ro.ora) contains the listening address of the agent, the names of SQL*Net listener and Oracle database servicesit knows about, plus tracing parameters. A publicly accessible SNMP read-only configuration file can be used to extract sensitive data like the tracing directory location, dbsnmp address, etc.

14.3.56 Oracle Agent Snmp Read-Only Configuration File Permission(Windows)

Description: Ensures Oracle Agent SNMP read-only configuration file (snmp_ro.ora) permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: The Oracle Agent SNMP read-only configuration file (snmp_ro.ora) contains the listening address of the agent, the names of SQL*Net listener and Oracle database servicesit knows about, plus tracing parameters. A publicly accessible SNMP read-only configuration file can be used to extract sensitive data like the tracing directory location, dbsnmp address, etc.

14.3.57 Oracle Agent Snmp Read-Write Configuration File Owner

Description: Ensures Oracle Agent SNMP read-write configuration file (snmp_rw.ora) is owned by Oracle software owner

Severity: Warning

Rationale: The Oracle Agent SNMP read-write configuration file (snmp_ro.ora) contains the listening address of the agent, the names of SQL*Net listener and Oracle

database services it knows about, plus tracing parameters. A publicly accessible SNMP read-write configuration file can be used to extract sensitive data like the tracing directory location, dbsnmp address, etc.

14.3.58 Oracle Agent Snmp Read-Write Configuration File Permission

Description: Ensures Oracle Agent SNMP read-write configuration file (snmp_rw.ora) permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: The Oracle Agent SNMP read-write configuration file (snmp_ro.ora) contains the listening address of the agent, the names of SQL*Net listener and Oracle database services it knows about, plus tracing parameters. A publicly accessible SNMP read-write configuration file can be used to extract sensitive data like the tracing directory location, dbsnmp address, etc.

14.3.59 Oracle Agent Snmp Read-Write Configuration File Permission(Windows)

Description: Ensures Oracle Agent SNMP read-write configuration file (snmp_rw.ora) permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: The Oracle Agent SNMP read-write configuration file (snmp_ro.ora) contains the listening address of the agent, the names of SQL*Net listener and Oracle database services it knows about, plus tracing parameters. A publicly accessible SNMP read-write configuration file can be used to extract sensitive data like the tracing directory location, dbsnmp address, etc.

14.3.60 Oracle Http Server Distributed Configuration File Owner

Description: Ensures Oracle HTTP Server distributed configuration file ownership is restricted to the Oracle software set and DBA group

Severity: Warning

Rationale: The Oracle HTTP Server distributed configuration file (usually .htaccess) is used for access control and authentication of web folders. This file can be modified to gain access to pages containing sensitive information.

14.3.61 Oracle Http Server Distributed Configuration Files Permission

Description: Ensures Oracle HTTP Server Distributed Configuration Files permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: The Oracle HTTP Server distributed configuration file (usually .htaccess) is used for access control and authentication of web folders. This file can be modified to gain access to pages containing sensitive information.

14.3.62 Oracle Http Server Mod_Plsql Configuration File Owner

Description: Ensures Oracle HTTP Server mod_plsql configuration file (wdbsvr.app) is owned by Oracle software owner

Severity: Warning

Rationale: The Oracle Agent SNMP read-write configuration file (snmp_rw.ora) contains the listening address of the agent, the names of SQL*Net listener and Oracle

database services it knows about, plus tracing parameters. A publicly accessible SNMP read-write configuration file can be used to extract sensitive data like the tracing directory location, dbsnmp address, etc.

14.3.63 Oracle Http Server Mod_Plsql Configuration File Permission

Description: Ensures Oracle HTTP Server mod_plsql Configuration file (wdbsvr.app) permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: The Oracle Agent SNMP read-write configuration file (snmp_rw.ora) contains the listening address of the agent, the names of SQL*Net listener and Oracle database services it knows about, plus tracing parameters. A publicly accessible SNMP read-write configuration file can be used to extract sensitive data like the tracing directory location, dbsnmp address, etc.

14.3.64 Oracle Http Server Mod_Plsql Configuration File Permission(Windows)

Description: Oracle HTTP Server mod_plsql Configuration file (wdbsvr.app) permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: The Oracle HTTP Server mod_plsql configuration file (wdbsvr.app) contains the Database Access Descriptors used for authentication. A publicly accessible mod_plsql configuration file can allow a malicious user to modify the Database Access Descriptor settings to gain access to PL/SQL applications or launch a Denial Of Service attack.

14.3.65 Oracle Home Executable Files Permission

Description: Ensures that all files in the ORACLE_HOME/bin folder do not have public write permission

Severity: Warning

Rationale: Incorrect file permissions on some of the Oracle files can cause major security issues.

14.3.66 Oracle Home Executable Files Permission(Windows)

Description: Ensures that all files in the ORACLE_HOME/bin folder do not have public write permission

Severity: Warning

Rationale: Incorrect file permissions on some of the Oracle files can cause major security issues.

14.3.67 Oracle Net Client Log Directory Owner

Description: Ensures that the client log directory is a valid directory owned by Oracle set

Severity: Critical

Rationale: Log files provide information contained in an error stack. An error stack refers to the information that is produced by each layer in an Oracle communications stack as the result of a network error. The information in log files can reveal important

network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

14.3.68 Oracle Net Client Trace Directory Owner

Description: Ensures that the client trace directory is a valid directory owned by Oracle set

Severity: Critical

Rationale: Tracing produces a detailed sequence of statements that describe network events as they are executed. Tracing an operation enables you to obtain more information on the internal operations of the components of Oracle Net Services than is provided in a log file. The information in this file can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

14.3.69 Oracle Net Inbound Connect Timeout

Description: Ensures that all incomplete inbound connections to Oracle Net has a limited lifetime

Severity: Warning

Rationale: Without this parameter or assigning it with a higher value , a client connection to the database server can stay open indefinitely or for the specified duration without authentication. Connections without authentication can introduce possible denial-of-service attacks, whereby malicious clients attempt to flood database servers with connect requests that consume resources.

14.3.70 Oracle Net Ssl_Cert_Revocation

Description: Ensures that the ssl_cert_revocation parameter is set to recommended value in sqlnet.ora

Severity: Warning

Rationale: This option Ensures revocation is required for checking CRLs for client certificate authentication. Revoked certificates can pose a threat to the integrity of the SSL channel and should not be trusted

14.3.71 Oracle Net Ssl_Server_Dn_Match

Description: Ensures ssl_server_dn_match is enabled in sqlnet.ora and in turn SSL ensures that the certificate is from the server

Severity: Warning

Rationale: If ssl_server_dn_match parameter is disabled, then SSL performs the check but allows the connection, regardless if there is a match. Not enforcing the match allows the server to potentially fake its identity.

14.3.72 Oracle Net Server Log Directory Owner

Description: Ensures that the server log directory is a valid directory owned by Oracle set

Severity: Critical

Rationale: Log files provide information contained in an error stack. An error stack refers to the information that is produced by each layer in an Oracle communications

stack as the result of a network error. The information in log files can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

14.3.73 Oracle Net Server Trace Directory Owner

Description: Ensures that the server trace directory is a valid directory owned by Oracle set

Severity: Critical

Rationale: Tracing produces a detailed sequence of statements that describe network events as they are executed. Tracing an operation enables you to obtain more information on the internal operations of the components of Oracle Net Services than is provided in a log file. The information in this file can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

14.3.74 Oracle Net Sqlnet Expire Time

Description: Ensures that sqlnet.expire_time parameter is set to recommended value.

Severity: Warning

Rationale: if sqlnet.expire_time is not set or set to 0, then database never checks for dead connection and they keeps consuming database server resources.

14.3.75 Oracle Net Tcp Validnode Checking

Description: Ensures that tcp.validnode_checking parameter is set to yes.

Severity: Minor Warning

Rationale: Not setting valid node check can potentially allow anyone to connect to the sever, including a malicious user.

14.3.76 Oracle Xsql Configuration File Owner

Description: Ensures Oracle XSQL configuration file (XSQLConfig.xml) is owned by Oracle software owner

Severity: Warning

Rationale: The Oracle XSQL configuration file (XSQLConfig.xml) contains sensitive database connection information. A publicly accessible XSQL configuration file can expose the database username and password that can be used access sensitive data or to launch further attacks.

14.3.77 Oracle Xsql Configuration File Permission

Description: Ensures Oracle XSQL configuration file (XSQLConfig.xml) permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: The Oracle XSQL configuration file (XSQLConfig.xml) contains sensitive database connection information. A publicly accessible XSQL configuration file can expose the database username and password that can be used access sensitive data or to launch further attacks.

14.3.78 Oracle Xsql Configuration File Permission(Windows)

Description: Ensures Oracle XSQL Configuration File (XSQLConfig.xml) permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: The Oracle XSQL configuration file (XSQLConfig.xml) contains sensitive database connection information. A publicly accessible XSQL configuration file can expose the database username and password that can be used access sensitive data or to launch further attacks.

14.3.79 Otrace Data Files

Description: Avoids negative impact on database performance and disk space usage, caused by data collected by otrace

Severity: Warning

Rationale: Performance and resource utilization data collection can have a negative impact on database performance and disk space usage.

14.3.80 Private Sga

Description: Ensure that users PRIVATE_SGA profile settings have appropriate values set for the particular database and application

Severity: Critical

Rationale: Allowing a single application or user to consume the excessive amounts of the System Global Area will result in a denial of service to the Oracle database

14.3.81 Password Reuse Max

Description: Ensures that all profiles have PASSWORD_REUSE_MAX set to a reasonable number of times

Severity: Warning

Rationale: Old passwords are usually the best guesses for the current password. A low value for the PASSWORD_REUSE_MAX parameter may cause serious database security issues by allowing users to reuse their old passwords more often.

14.3.82 Password Reuse Time

Description: Ensures that all profiles have PASSWORD_REUSE_TIME set to a reasonable number of days

Severity: Critical

Rationale: A low value for the PASSWORD_REUSE_TIME parameter may cause serious database security issues by allowing users to reuse their old passwords more often.

14.3.83 Proxy Account

Description: Ensures that the proxy accounts have limited privileges

Severity: Warning

Rationale: The proxy user only needs to connect to the database. Once connected it will use the privileges of the user it is connecting on behalf of. Granting any other privilege than the CREATE SESSION privilege to the proxy user is unnecessary and open to misuse.

14.3.84 Return Server Release Banner

Description: Ensures that value of parameter SEC_RETURN_SERVER_RELEASE_BANNER is FALSE

Severity: Critical

Rationale: If the Parameter SEC_RETURN_SERVER_RELEASE_BANNER is TRUE oracle database returns complete database version information to clients. Knowing the exact patch set can aid an attacker

14.3.85 Remote Password File

Description: Ensures privileged users are authenticated by the operating system; that is, Oracle ignores any password file

Severity: Minor Warning

Rationale: The REMOTE_LOGIN_PASSWORDFILE parameter specifies whether or not Oracle checks for a password file. Because password files contain the passwords for users, including SYS, the most secure way of preventing an attacker from connecting through brute-force password-related attacks is to require privileged users be authenticated by the operating system.

14.3.86 Restrict Sqlnet.Ora Permission

Description: Ensures that the sqlnet.ora file is not accessible to public

Severity: Critical

Rationale: If sqlnet.ora is public readable a malicious user may attempt to read this hence could lead to sensitive information getting exposed .For example, log and trace destination information of the client and server.

14.3.87 Restrict Sqlnet.Ora Permission(Windows)

Description: Ensures that the sqlnet.ora file is not accessible to public

Severity: Critical

Rationale: If sqlnet.ora is public readable a malicious user may attempt to read this hence could lead to sensitive information getting exposed .For example, log and trace destination information of the client and server.

14.3.88 Sessions_Per_User

Description: Ensures that all profiles have SESSIONS_PER_USER set to a reasonable number of CPU cycles

Severity: Critical

Rationale: Allowing a single application or user to perform excessive amounts of reads to disk will result in a denial of service to the Oracle database

14.3.89 Sql*Plus Executable Owner

Description: Ensures SQL*Plus ownership is restricted to the Oracle software set and DBA group

Severity: Warning

Rationale: SQL*Plus allows a user to execute any SQL on the database. Not restricting ownership of SQL*Plus to the Oracle software set and DBA group may cause security issues by exposing sensitive data to malicious users.

14.3.90 Sql*Plus Executable Permission

Description: Ensures that SQL*Plus executable file permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: SQL*Plus allows a user to execute any SQL on the database. Public execute permissions on SQL*Plus can cause security issues by exposing sensitive data to malicious users.

14.3.91 Sql*Plus Executable Permission(Windows)

Description: Ensures that SQL*Plus executable file permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: SQL*Plus allows a user to execute any SQL on the database. Public execute permissions on SQL*Plus can cause security issues by exposing sensitive data to malicious users.

14.3.92 Secure Os Audit Level

Description: On UNIX systems, ensures that AUDIT_SYSLOG_LEVEL is set to a non-default value when OS-level auditing is enabled.

Severity: Warning

Rationale: Setting the AUDIT_SYSLOG_LEVEL initialization parameter to the default value (NONE) will result in DBAs gaining access to the OS audit records

14.3.93 System Privileges To Public

Description: Ensure system privileges are not granted to PUBLIC

Severity: Critical

Rationale: Privileges granted to the public role automatically apply to all users. There are security risks granting SYSTEM privileges to all users.

14.3.94 Tkprof Executable Owner

Description: Ensures tkprof executable file is owned by Oracle software owner

Severity: Warning

Rationale: Not restricting ownership of tkprof to the Oracle software set and DBA group may cause information leak.

14.3.95 Tkprof Executable Permission

Description: Ensures tkprof executable file permissions are restricted to read and execute for the group, and inaccessible to public

Severity: Warning

Rationale: Excessive permission for tkprof leaves information within, unprotected.

14.3.96 Tkprof Executable Permission(Windows)

Description: Ensures tkprof executable file permissions are restricted to read and execute for the group, and inaccessible to public

Severity: Warning

Rationale: Excessive permission for tkprof leaves information within, unprotected.

14.3.97 Unlimited Tablespace Quota

Description: Ensures database users are allocated a limited tablespace quota

Severity: Warning

Rationale: Granting unlimited tablespace quotas can cause the filling up of the allocated disk space. This can lead to an unresponsive database.

14.3.98 Use Of Automatic Log Archival Features

Description: Ensures that archiving of redo logs is done automatically and prevents suspension of instance operations when redo logs fill. Only applicable if database is in archivelog mode

Severity: Critical

Rationale: Setting the LOG_ARCHIVE_START initialization parameter to TRUE ensures that the archiving of redo logs is done automatically and prevents suspension of instance operations when redo logs fill. This feature is only applicable if the database is in archivelog mode.

14.3.99 Use Of Sql92 Security Features

Description: Ensures use of SQL92 security features

Severity: Warning

Rationale: If SQL92 security features are not enabled, a user might be able to execute an UPDATE or DELETE statement using a WHERE clause without having select privilege on a table.

14.3.100 Utility File Directory Initialization Parameter Setting In Oracle9I Release 1 And Later

Description: Ensure that the UTL_FILE_DIR initialization parameter is not used in Oracle9i Release 1 and later

Severity: Critical

Rationale: Specifies the directories which UTL_FILE package can access. Having the parameter set to asterisk (*), period (.), or to sensitive directories could expose them to all users having execute privilege on UTL_FILE package.

14.3.101 Webcache Initialization File Owner

Description: Ensures Webcache initialization file (webcache.xml) is owned by Oracle software owner

Severity: Warning

Rationale: Webcache stores sensitive information in the initialization file (webcache.xml). A publicly accessible Webcache initialization file can be used to extract sensitive data like the administrator password hash.

14.3.102 Webcache Initialization File Permission

Description: Ensures the Webcache initialization file (webcache.xml) permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: Webcache stores sensitive information in the initialization file (webcache.xml). A publicly accessible Webcache initialization file can be used to extract sensitive data like the administrator password hash.

14.3.103 Webcache Initialization File Permission(Windows)

Description: Ensures the Webcache initialization file (webcache.xml) permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: Webcache stores sensitive information in the initialization file (webcache.xml). A publicly accessible Webcache initialization file can be used to extract sensitive data like the administrator password hash.

14.3.104 Tcp.Excludeded_Nodes

Description: Ensures that tcp.excludeded_nodes parameter is set.

Severity: Warning

Rationale: Not setting valid node check can potentially allow anyone to connect to the sever, including a malicious user.

14.3.105 Tcp.Invited_Nodes

Description: Ensures that tcp.invited_nodes parameter is set.

Severity: Warning

Rationale: Not setting valid node check can potentially allow anyone to connect to the sever, including a malicious user.

14.4 Patchable Configuration For Rac Database

The compliance rules for the Patchable Configuration For Rac Database standard follow.

14.4.1 Patchability

Description: Ensure the RAC Database target has a patchable configuration

Severity: Warning

Rationale: Unpatchable RAC Database target could not be patched by using the provided EM Patching feature

14.5 Storage Best Practices For Oracle Rac Database

The compliance rules for the Storage Best Practices For Oracle Rac Database standard follow.

14.5.1 Default Permanent Tablespace Set To A System Tablespace

Description: Checks if the DEFAULT_PERMANENT_TABLESPACE database property is set to a system tablespace

Severity: Warning

Rationale: If not specified explicitly, DEFAULT_PERMANENT_TABLESPACE is defaulted to the SYSTEM tablespace. This is not the recommended setting. With this setting, any user that is not explicitly assigned a tablespace uses the system tablespace. Doing so may result in performance degradation for the database. This is also a security issue. Non-system users may store data and consume all available space in the system tablespace, thus causing the database to stop working.

14.5.2 Default Temporary Tablespace Set To A System Tablespace

Description: Checks if the DEFAULT_TEMP_TABLESPACE database property is set to a system tablespace

Severity: Warning

Rationale: If not specified explicitly, DEFAULT_TEMP_TABLESPACE would default to SYSTEM tablespace and this is not a recommended setting. With this setting, any user that is not explicitly assigned a temporary tablespace uses the system tablespace as their temporary tablespace. System tablespaces should not be used to store temporary data. This is also a security issue. Non-system users may store data and consume all available space in the system tablespace, thus causing the database to stop working.

14.5.3 Dictionary Managed Tablespaces

Description: Checks for dictionary managed tablespaces

Severity: Minor Warning

Rationale: These tablespaces are dictionary managed. Oracle recommends using locally managed tablespaces, with AUTO segment-space management, to enhance performance and ease of space management.

14.5.4 Insufficient Number Of Redo Logs

Description: Checks for use of less than three redo logs

Severity: Warning

Rationale: The online redo log files are used to record changes in the database. When archiving is enabled, these online redo logs need to be archived before they can be reused. Every database requires at least two online redo log groups to be up and running. When the size and number of online redo logs are inadequate, LGWR will wait for ARCH to complete its writing to the archived log destination, before it overwrites that log. This can cause severe performance slowdowns during peak activity periods.

14.5.5 Insufficient Redo Log Size

Description: Checks for redo log files less than 1 Mb

Severity: Critical

Rationale: Small redo logs cause system checkpoints to continuously put a high load on the buffer cache and I/O system.

14.5.6 Non-System Data Segments In System Tablespaces

Description: Checks for data segments owned by non-system users located in tablespaces SYSTEM, SYSAUX and SYSEXT.

Severity: Minor Warning

Rationale: These segments belonging to non-system users are stored in system tablespaces SYSTEM or SYSAUX or SYSEXT. This violation makes it more difficult to manage these data segments and may result in performance degradation in the system tablespace. This is also a security issue. If non-system users are storing data in a system tablespace it is possible that all available space in the system tablespace may be consumed, thus causing the database to stop working.

14.5.7 Non-System Users With System Tablespace As Default Tablespace

Description: Checks for non-system users using SYSTEM or SYSAUX as the default tablespace

Severity: Minor Warning

Rationale: These non-system users use a system tablespace as the default tablespace. This violation will result in non-system data segments being added to the system tablespace, making it more difficult to manage these data segments and possibly resulting in performance degradation in the system tablespace. This is also a security issue. All Available space in the system tablespace may beconsumed, thus causing the database to stop working.

14.5.8 Non-Uniform Default Extent Size For Tablespaces

Description: Checks for dictionary managed or migrated locally managed tablespaces with non-uniform default extent size

Severity: Minor Warning

Rationale: Dictionary managed or migrated locally managed tablespaces using non-uniform default extent sizes have been found. This means that the extents in a single tablespace will vary insize leading to fragmentation, inefficient space usage and performance degradation.

14.5.9 Rollback In System Tablespace

Description: Checks for rollback segments in SYSTEM tablespace

Severity: Minor Warning

Rationale: The SYSTEM tablespace should be reserved only for the Oracle data dictionary and its associated objects. It should NOT be used to store any other types of objects such as user tables, user indexes, user views, rollback segments, undo segments or temporary segments.

14.5.10 Tablespace Not Using Automatic Segment-Space Management

Description: Checks for locally managed tablespaces that are using MANUAL segment space management

Severity: Minor Warning

Rationale: Automatic segment-space management is a simpler and more efficient way of managing space within a segment. It completely eliminates any need to specify and tune the PCTUSED, FREELISTS and FREELIST GROUPS storage parameters for schema objects created in the tablespace. In a RAC environment there is the additional benefit of avoiding the hard partitioning of space inherent with using free list groups.

14.5.11 Tablespaces Containing Rollback And Data Segments

Description: Checks for tablespaces containing both rollback and data segments

Severity: Minor Warning

Rationale: These tablespaces contain both rollback and data segments. Mixing segment types in this way makes it more difficult to manage space and may degrade performance in the tablespace. Use of a dedicated tablespace for rollback segments enhances availability and performance.

14.5.12 Users With Permanent Tablespace As Temporary Tablespace

Description: Checks for users using a permanent tablespace as the temporary tablespace

Severity: Minor Warning

Rationale: These users use a permanent tablespace as the temporary tablespace. Using temporary tablespaces allows space management for sort operations to be more efficient. Using a permanent tablespace for these operations may result in performance degradation, especially for Real Application Clusters. There is an additional security concern. This makes it possible for users to use all available space in the system tablespace, causing the database to stop working.

15

Oracle Single Instance Database Compliance Standards

These are the compliance rules for the Oracle Single Instance Database compliance standards

15.1 Basic Security Configuration For Oracle Cluster Database Instance

The compliance rules for the Basic Security Configuration For Oracle Cluster Database Instance standard follow.

15.1.1 Allowed Logon Version

Description: Ensures that the server allows logon from clients with a matching version or higher only.

Severity: Warning

Rationale: Setting the parameter SQLNET.ALLOWED_LOGON_VERSION in sqlnet.ora to a version lower than the server version will force the server to use a less secure authentication protocol

15.1.2 Audit File Destination

Description: Ensures that access to the audit files directory is restricted to the owner of the Oracle software set and the DBA group.

Severity: Critical

Rationale: The AUDIT_FILE_DEST initialization parameter specifies the directory where the Oracle auditing facility creates the audit files. Giving public read permission to this directory may reveal important information such as logging information of startup, shutdown, and privileged connections.

15.1.3 Audit File Destination(Windows)

Description: Ensures that access to the audit files directory is restricted to the owner of the Oracle software set and the DBA group.

Severity: Critical

Rationale: The AUDIT_FILE_DEST initialization parameter specifies the directory where the Oracle auditing facility creates the audit files. Giving public read permission to this directory may reveal important information such as logging information of startup, shutdown, and privileged connections.

15.1.4 Auditing Of Sys Operations Enabled

Description: Ensures sessions for users who connect as SYS are fully audited

Severity: Warning

Rationale: The AUDIT_SYS_OPERATIONS parameter enables or disables the auditing of operations issued by user SYS, and users connecting with SYSDBA or SYSOPER privileges.

15.1.5 Background Dump Destination(Windows)

Description: Ensures that access to the trace files directory is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: Background processes such as the log writer process and the database writer process use trace files to record occurrences and exceptions of database operations, as well as errors. The trace files are stored in the directory specified by the BACKGROUND_DUMP_DEST initialization parameter. Giving public read permission to this directory may reveal important and sensitive internal details of the database and applications.

15.1.6 Check Network Data Integrity On Server

Description: Ensures that the crypto_checksum_server parameter is set to recommended value in sqlnet.ora.

Severity: Warning

Rationale: This option ensures the integrity check for communication to prevent data modification.

15.1.7 Core Dump Destination

Description: Ensures that access to the core dump files directory is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: Core dump files are stored in the directory specified by the CORE_DUMP_DEST initialization parameter. A public read privilege on this directory could expose sensitive information from the core dump files.

15.1.8 Core Dump Destination(Windows)

Description: Ensures that access to the core dump files directory is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: Core dump files are stored in the directory specified by the CORE_DUMP_DEST initialization parameter. A public read privilege on this directory could expose sensitive information from the core dump files.

15.1.9 Data Dictionary Protected

Description: Ensures data dictionary protection is enabled

Severity: Critical

Rationale: The 07_DICTIONARY_ACCESSIBILITY parameter controls access to the data dictionary. Setting the 07_DICTIONARY_ACCESSIBILITY to TRUE allows users

with ANY system privileges to access the data dictionary. As a result, these user accounts can be exploited to gain unauthorized access to data.

15.1.10 Enable Database Auditing

Description: Ensures database auditing is enabled

Severity: Minor Warning

Rationale: The AUDIT_TRAIL parameter enables or disables database auditing. For database version 12c and above Unified Auditing can be used. Auditing enhances security because it enforces accountability, provides evidence of misuse, and is frequently required for regulatory compliance. Auditing also enables system administrators to implement enhanced protections, early detection of suspicious activities, and finely-tuned security responses.

15.1.11 Encrypt Network Communication On Server

Description: Ensures that the encryption_server parameter is set to recommended value in sqlnet.ora

Severity: Warning

Rationale: This option ensures that regardless of the settings on the user, if communication takes place it must be encrypted

15.1.12 Force Client Ssl Authentication

Description: Ensures that the ssl_client_authentication parameter is set to TRUE

Severity: Warning

Rationale: If TRUE Both the client and server authenticate to each other using certificates.It is preferable to have mutually authenticated SSL connections verifying the identity of both parties. If possible use client and server certificates for SSL connections. If client certificates are not supported in the enterprise, then set to FALSE.

15.1.13 Initialization Parameter File Permission

Description: Ensures that access to the initialization paramater file is restricted to the owner of the Oracle software set and the DBA group

Severity: Warning

Rationale: Oracle traditionally stores initialization parameters in a text initialization parameter file. A publicly accessible initialization parameter file can be scanned for sensitive initialization parameters exposing the security policies of the database. The IFILE can also be searched for the weaknesses of the Oracle database configuration setting.

15.1.14 Initialization Parameter File Permission(Windows)

Description: Ensures that access to the initialization paramater file is restricted to the owner of the Oracle software set and the DBA group

Severity: Warning

Rationale: Oracle traditionally stores initialization parameters in a text initialization parameter file. A publicly accessible initialization parameter file can be scanned for sensitive initialization parameters exposing the security policies of the database. The

IFILE can also be searched for the weaknesses of the Oracle database configuration setting.

15.1.15 Oracle Home Executable Files Owner

Description: Ensures that the ownership of all files and directories in the ORACLE_HOME/bin folder is the same as the Oracle software installation owner

Severity: Critical

Rationale: Incorrect file permissions on some of the Oracle files can cause major security issues.

15.1.16 Oracle Home File Permission

Description: Ensures that all files in the ORACLE_HOME directories (except for ORACLE_HOME/bin) do not have public read, write and execute permissions

Severity: Warning

Rationale: Incorrect file permissions on some of the Oracle files can cause major security issues.

15.1.17 Oracle Home File Permission(Windows)

Description: Ensures that all files in the ORACLE_HOME directories (except for ORACLE_HOME/bin) do not have public read, write and execute permissions

Severity: Warning

Rationale: Incorrect file permissions on some of the Oracle files can cause major security issues.

15.1.18 Oracle Net Client Log Directory Permission

Description: Ensures that the client log directory is a valid directory owned by Oracle set with no permissions to public

Severity: Critical

Rationale: Log files provide information contained in an error stack. An error stack refers to the information that is produced by each layer in an Oracle communications stack as the result of a network error. The information in log files can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

15.1.19 Oracle Net Client Log Directory Permission(Windows)

Description: Ensures that the client log directory is a valid directory owned by Oracle set with no permissions to public

Severity: Critical

Rationale: Log files provide information contained in an error stack. An error stack refers to the information that is produced by each layer in an Oracle communications stack as the result of a network error. The information in log files can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

15.1.20 Oracle Net Client Trace Directory Permission

Description: Ensures that the client trace directory is a valid directory owned by Oracle set with no permissions to public

Severity: Critical

Rationale: Tracing produces a detailed sequence of statements that describe network events as they are executed. Tracing an operation enables you to obtain more information on the internal operations of the components of Oracle Net Services than is provided in a log file. The information in this file can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

15.1.21 Oracle Net Client Trace Directory Permission(Windows)

Description: Ensures that the client trace directory is a valid directory owned by Oracle set with no permissions to public

Severity: Critical

Rationale: Tracing produces a detailed sequence of statements that describe network events as they are executed. Tracing an operation enables you to obtain more information on the internal operations of the components of Oracle Net Services than is provided in a log file. The information in this file can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

15.1.22 Oracle Net Server Log Directory Permission

Description: Ensures that the server log directory is a valid directory owned by Oracle set with no permissions to public

Severity: Critical

Rationale: Log files provide information contained in an error stack. An error stack refers to the information that is produced by each layer in an Oracle communications stack as the result of a network error. The information in log files can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

15.1.23 Oracle Net Server Log Directory Permission(Windows)

Description: Ensures that the server log directory is a valid directory owned by Oracle set with no permissions to public

Severity: Critical

Rationale: Log files provide information contained in an error stack. An error stack refers to the information that is produced by each layer in an Oracle communications stack as the result of a network error. The information in log files can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

15.1.24 Oracle Net Server Trace Directory Permission

Description: Ensures that the server trace directory is a valid directory owned by Oracle set with no permissions to public

Severity: Critical

Rationale: Tracing produces a detailed sequence of statements that describe network events as they are executed. Tracing an operation enables you to obtain more information on the internal operations of the components of Oracle Net Services than is provided in a log file. The information in this file can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

15.1.25 Oracle Net Server Trace Directory Permission(Windows)

Description: Ensures that the server trace directory is a valid directory owned by Oracle set with no permissions to public

Severity: Critical

Rationale: Tracing produces a detailed sequence of statements that describe network events as they are executed. Tracing an operation enables you to obtain more information on the internal operations of the components of Oracle Net Services than is provided in a log file. The information in this file can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

15.1.26 Protocol Error Further Action

Description: Ensures that the SEC_PROTOCOL_ERROR_FURTHER_ACTION parameter is set to either DROP or DELAY

Severity: Critical

Rationale: If default value CONTINUE is used, the server process continues execution even if bad packets are received. The database server may be subject to a Denial of Service (DoS) if bad packets continue to be sent by a malicious client

15.1.27 Protocol Error Trace Action

Description: Ensures that the sec_protocol_error_trace_action parameter is set to either LOG or ALERT

Severity: Critical

Rationale: SEC_PROTOCOL_ERROR_TRACE_ACTION specifies the action that the database should take when bad packets are received from a possibly malicious client. NONE should not be used as the database server ignores the bad packets and does not generate any trace files or log messages. If default value TRACE is used then the database server generates a detailed trace file and should only be used when debugging

15.1.28 Public Trace Files

Description: Ensures database trace files are not public readable

Severity: Critical

Rationale: If trace files are readable by the PUBLIC group, a malicious user may attempt to read the trace files that could lead to sensitive information being exposed.

15.1.29 Remote Os Authentication

Description: Ensure REMOTE_OS_AUTHENT initialization parameter is set to FALSE

Severity: Critical

Rationale: A malicious user can gain access to the database if remote OS authentication is allowed.

15.1.30 Remote Os Role

Description: Ensure REMOTE_OS_ROLES initialization parameter is set to FALSE

Severity: Critical

Rationale: A malicious user can gain access to the database if remote users can be granted privileged roles.

15.1.31 Ssl Cipher Suites Supported

Description: Ensures that the ssl_cipher_suites parameter is set to recommended value in sqlnet.ora

Severity: Warning

Rationale: This option is used to specify a cipher suite that will be used by the SSL connection. If the recommended cipher suite is not used, the SSL connection could be compromised.

15.1.32 Ssl Versions Supported

Description: Ensures that the ssl_version parameter is set to latest version .

Severity: Warning

Rationale: Usage of the most current version of SSL is recommended older versions of the SSL protocol are prone to attack or roll back. Do not set this parameter with Any.

15.1.33 Server Parameter File Permission

Description: Ensures that access to the server paramater file is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: A server parameter file (SPFILE) lets you store and manage your initialization parameters persistently in a server-side disk file. A publicly accessible SPFILE can be scanned for sensitive initialization parameters exposing the security policies of the database. The SPFILE can also be searched for the weaknesses of the Oracle database configuration setting.

15.1.34 Server Parameter File Permission(Windows)

Description: Ensures that access to the server paramater file is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: A server parameter file (SPFILE) lets you store and manage your initialization parameters persistently in a server-side disk file. A publicly accessible SPFILE can be scanned for sensitive initialization parameters exposing the security policies of the database. The SPFILE can also be searched for the weaknesses of the Oracle database configuration setting.

15.1.35 Use Of Appropriate Umask On Unix Systems

Description: On UNIX systems, ensure that the owner of the Oracle software has an appropriate umask value of 022 set

Severity: Warning

Rationale: If umask is not set to an appropriate value (like 022), log or trace files might become accessible to public exposing sensitive information.

15.1.36 User Dump Destination

Description: Ensures that access to the trace files directory is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: The trace files for server processes are stored in the directory specified by the USER_DUMP_DEST initialization parameter. Giving public read permission to this directory may reveal important and sensitive internal details of the database and applications.

15.1.37 User Dump Destination(Windows)

Description: Ensures that access to the trace files directory is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: The trace files for server processes are stored in the directory specified by the USER_DUMP_DEST initialization parameter. Giving public read permission to this directory may reveal important and sensitive internal details of the database and applications.

15.1.38 Using Externally Identified Accounts

Description: Ensures that the OS authentication prefix is set to a value other than OPS $

Severity: Warning

Rationale: The OS_AUTHENT_PREFIX parameter specifies a prefix used to authenticate users attempting to connect to the server. When a connection request is attempted, Oracle compares the prefixed username with usernames in the database. Using a prefix, especially OPS$, tends to result in an insecure configuration as an account can be authenticated either as an operating system user or with the password used in the IDENTIFIED BY clause. Attackers are aware of this and will attack these accounts.

15.1.39 Utility File Directory Initialization Parameter Setting

Description: Ensures that the Utility File Directory (UTL_FILE_DIR) initialization parameter is not set to one of '*', '.', core dump trace file locations

Severity: Critical

Rationale: Specifies the directories which the UTL_FILE package can access. Having the parameter set to asterisk (*), period (.), or to sensitive directories, could expose them to all users having execute privilege on the UTL_FILE package.

15.2 Basic Security Configuration For Oracle Database

The compliance rules for the Basic Security Configuration For Oracle Database standard follow.

15.2.1 Access To Dba_Roles View

Description: Ensures restricted access to DBA_ROLES view

Severity: Minor Warning

Rationale: DBA_ROLES view contains details of all roles in the database. Knowledge of the structure of roles in the database can be taken advantage of by a malicious user.

15.2.2 Access To Dba_Role_Privs View

Description: Ensures restricted access to DBA_ROLE_PRIVS view

Severity: Minor Warning

Rationale: The DBA_ROLE_PRIVS view lists the roles granted to users and other roles. Knowledge of the structure of roles in the database can be taken advantage of by a malicious user.

15.2.3 Access To Dba_Sys_Privs View

Description: Ensures restricted access to DBA_SYS_PRIVS view

Severity: Minor Warning

Rationale: DBA_SYS_PRIVS view can be queried to find system privileges granted to roles and users. Knowledge of the structure of roles in the database can be taken advantage of bya malicious user.

15.2.4 Access To Dba_Tab_Privs View

Description: Ensures restricted access to DBA_TAB_PRIVS view

Severity: Minor Warning

Rationale: Lists privileges granted to users or roles on objects in the database. Knowledge of the structure of roles in the database can be taken advantage of by a malicious user.

15.2.5 Access To Dba_Users View

Description: Ensures restricted access to DBA_USERS view

Severity: Minor Warning

Rationale: Contains user password hashes and other account information. Access to this information can be used to mount brute-force attacks.

15.2.6 Access To Stats$Sqltext Table

Description: Ensures restricted access to STATS$SQLTEXT table

Severity: Minor Warning

Rationale: This table provides full text of the recently-executed SQL statements. The SQL statements can reveal sensitive information.

15.2.7 Access To Stats$Sql_Summary Table

Description: Ensures restricted access to STATS$SQL_SUMMARY table

Severity: Minor Warning

Rationale: Contains first few lines of SQL text of the most resource intensive commands given to the server. Sql statements executed without bind variables can show up here exposing privileged information.

15.2.8 Access To Sys.Aud$ Table

Description: Ensures restricted access to SYS.AUD$ table

Severity: Minor Warning

Rationale: A knowlegeable and malicious user can gain access to sensitive audit information.

15.2.9 Access To Sys.Source$ Table

Description: Ensures restricted access to SYS.SOURCE$ table

Severity: Minor Warning

Rationale: Contains source of all stored packages units in the database.

15.2.10 Access To Sys.User$ Table

Description: Ensures restricted access to SYS.USER$ table

Severity: Minor Warning

Rationale: Username and password hash may be read from the SYS.USER$ table, enabling a hacker to launch a brute-force attack.

15.2.11 Access To Sys.User_History$ Table

Description: Ensures restricted access to SYS.USER_HISTORY$ table

Severity: Minor Warning

Rationale: Username and password hash may be read from the SYS.USER_HISTORY$ table, enabling a hacker to launch a brute-force attack.

15.2.12 Allowed Logon Version

Description: Ensures that the server allows logon from clients with a matching version or higher only.

Severity: Warning

Rationale: Setting the parameter SQLNET.ALLOWED_LOGON_VERSION in sqlnet.ora to a version lower than the server version will force the server to use a less secure authentication protocol

15.2.13 Audit File Destination

Description: Ensures that access to the audit files directory is restricted to the owner of the Oracle software set and the DBA group.

Severity: Critical

Rationale: The AUDIT_FILE_DEST initialization parameter specifies the directory where the Oracle auditing facility creates the audit files. Giving public read permission to this directory may reveal important information such as logging information of startup, shutdown, and privileged connections.

15.2.14 Audit File Destination(Windows)

Description: Ensures that access to the audit files directory is restricted to the owner of the Oracle software set and the DBA group.

Severity: Critical

Rationale: The AUDIT_FILE_DEST initialization parameter specifies the directory where the Oracle auditing facility creates the audit files. Giving public read permission to this directory may reveal important information such as logging information of startup, shutdown, and privileged connections.

15.2.15 Auditing Of Sys Operations Enabled

Description: Ensures sessions for users who connect as SYS are fully audited

Severity: Warning

Rationale: The AUDIT_SYS_OPERATIONS parameter enables or disables the auditing of operations issued by user SYS, and users connecting with SYSDBA or SYSOPER privileges.

15.2.16 Background Dump Destination(Windows)

Description: Ensures that access to the trace files directory is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: Background processes such as the log writer process and the database writer process use trace files to record occurrences and exceptions of database operations, as well as errors. The trace files are stored in the directory specified by the BACKGROUND_DUMP_DEST initialization parameter. Giving public read permission to this directory may reveal important and sensitive internal details of the database and applications.

15.2.17 Check Network Data Integrity On Server

Description: Ensures that the crypto_checksum_server parameter is set to recommended value in sqlnet.ora.

Severity: Warning

Rationale: This option ensures the integrity check for communication to prevent data modification.

15.2.18 Control File Permission

Description: Ensures that access to the control files directory is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: Control files are binary configuration files that control access to data files. Control files are stored in the directory specified by the CONTROL_FILES initialization parameter. A public write privilege on this directory could pose a serious security risk.

15.2.19 Control File Permission(Windows)

Description: Ensures that access to the control files directory is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: Control files are binary configuration files that control access to data files. Control files are stored in the directory specified by the CONTROL_FILES initialization parameter. A public write privilege on this directory could pose a serious security risk.

15.2.20 Core Dump Destination

Description: Ensures that access to the core dump files directory is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: Core dump files are stored in the directory specified by the CORE_DUMP_DEST initialization parameter. A public read privilege on this directory could expose sensitive information from the core dump files.

15.2.21 Core Dump Destination(Windows)

Description: Ensures that access to the core dump files directory is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: Core dump files are stored in the directory specified by the CORE_DUMP_DEST initialization parameter. A public read privilege on this directory could expose sensitive information from the core dump files.

15.2.22 Data Dictionary Protected

Description: Ensures data dictionary protection is enabled

Severity: Critical

Rationale: The 07_DICTIONARY_ACCESSIBILITY parameter controls access to the data dictionary. Setting the 07_DICTIONARY_ACCESSIBILITY to TRUE allows users with ANY system privileges to access the data dictionary. As a result, these user accounts can be exploited to gain unauthorized access to data.

15.2.23 Default Passwords

Description: Ensure there are no default passwords for known accounts

Severity: Warning

Rationale: A malicious user can gain access to the database using default passwords.

15.2.24 Enable Database Auditing

Description: Ensures database auditing is enabled

Severity: Minor Warning

Rationale: The AUDIT_TRAIL parameter enables or disables database auditing. For database version 12c and above Unified Auditing can be used. Auditing enhances security because it enforces accountability, provides evidence of misuse, and is frequently required for regulatory compliance. Auditing also enables system administrators to implement enhanced protections, early detection of suspicious activities, and finely-tuned security responses.

15.2.25 Encrypt Network Communication On Server

Description: Ensures that the encryption_server parameter is set to recommended value in sqlnet.ora

Severity: Warning

Rationale: This option ensures that regardless of the settings on the user, if communication takes place it must be encrypted

15.2.26 Execute Privileges On Dbms_Job To Public

Description: Ensures PUBLIC is not granted EXECUTE privileges on DBMS_JOB package

Severity: Critical

Rationale: Granting EXECUTE privilege to PUBLIC on DBMS_JOB package allows users to schedule jobs on the database.

15.2.27 Execute Privileges On Dbms_Sys_Sql To Public

Description: Ensures PUBLIC is not granted EXECUTE privileges on DBMS_SYS_SQL package

Severity: Critical

Rationale: The DBMS_SYS_SQL package can be used to run PL/SQL and SQL as the owner of the procedure rather than the caller.

15.2.28 Force Client Ssl Authentication

Description: Ensures that the ssl_client_authentication parameter is set to TRUE

Severity: Warning

Rationale: If TRUE Both the client and server authenticate to each other using certificates.It is preferable to have mutually authenticated SSL connections verifying the identity of both parties. If possible use client and server certificates for SSL connections. If client certificates are not supported in the enterprise, then set to FALSE.

15.2.29 Initialization Parameter File Permission

Description: Ensures that access to the initialization paramater file is restricted to the owner of the Oracle software set and the DBA group

Severity: Warning

Rationale: Oracle traditionally stores initialization parameters in a text initialization parameter file. A publicly accessible initialization parameter file can be scanned for sensitive initialization parameters exposing the security policies of the database. The

IFILE can also be searched for the weaknesses of the Oracle database configuration setting.

15.2.30 Initialization Parameter File Permission(Windows)

Description: Ensures that access to the initialization paramater file is restricted to the owner of the Oracle software set and the DBA group

Severity: Warning

Rationale: Oracle traditionally stores initialization parameters in a text initialization parameter file. A publicly accessible initialization parameter file can be scanned for sensitive initialization parameters exposing the security policies of the database. The IFILE can also be searched for the weaknesses of the Oracle database configuration setting.

15.2.31 Oracle Home Datafile Permission

Description: Ensures that access to the datafiles is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: The datafiles contain all the database data. If datafiles are readable to public, they can be read by a user who has no database privileges on the data.

15.2.32 Oracle Home Datafile Permission(Windows)

Description: Ensures that access to the datafiles is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: The datafiles contain all the database data. If datafiles are readable to public, they can be read by a user who has no database privileges on the data.

15.2.33 Oracle Home Executable Files Owner

Description: Ensures that the ownership of all files and directories in the ORACLE_HOME/bin folder is the same as the Oracle software installation owner

Severity: Critical

Rationale: Incorrect file permissions on some of the Oracle files can cause major security issues.

15.2.34 Oracle Home File Permission

Description: Ensures that all files in the ORACLE_HOME directories (except for ORACLE_HOME/bin) do not have public read, write and execute permissions

Severity: Warning

Rationale: Incorrect file permissions on some of the Oracle files can cause major security issues.

15.2.35 Oracle Home File Permission(Windows)

Description: Ensures that all files in the ORACLE_HOME directories (except for ORACLE_HOME/bin) do not have public read, write and execute permissions

Severity: Warning

Rationale: Incorrect file permissions on some of the Oracle files can cause major security issues.

15.2.36 Oracle Net Client Log Directory Permission

Description: Ensures that the client log directory is a valid directory owned by Oracle set with no permissions to public

Severity: Critical

Rationale: Log files provide information contained in an error stack. An error stack refers to the information that is produced by each layer in an Oracle communications stack as the result of a network error. The information in log files can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

15.2.37 Oracle Net Client Log Directory Permission(Windows)

Description: Ensures that the client log directory is a valid directory owned by Oracle set with no permissions to public

Severity: Critical

Rationale: Log files provide information contained in an error stack. An error stack refers to the information that is produced by each layer in an Oracle communications stack as the result of a network error. The information in log files can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

15.2.38 Oracle Net Client Trace Directory Permission

Description: Ensures that the client trace directory is a valid directory owned by Oracle set with no permissions to public

Severity: Critical

Rationale: Tracing produces a detailed sequence of statements that describe network events as they are executed. Tracing an operation enables you to obtain more information on the internal operations of the components of Oracle Net Services than is provided in a log file. The information in this file can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

15.2.39 Oracle Net Client Trace Directory Permission(Windows)

Description: Ensures that the client trace directory is a valid directory owned by Oracle set with no permissions to public

Severity: Critical

Rationale: Tracing produces a detailed sequence of statements that describe network events as they are executed. Tracing an operation enables you to obtain more information on the internal operations of the components of Oracle Net Services than is provided in a log file. The information in this file can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

15.2.40 Oracle Net Server Log Directory Permission

Description: Ensures that the server log directory is a valid directory owned by Oracle set with no permissions to public

Severity: Critical

Rationale: Log files provide information contained in an error stack. An error stack refers to the information that is produced by each layer in an Oracle communications stack as the result of a network error. The information in log files can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

15.2.41 Oracle Net Server Log Directory Permission(Windows)

Description: Ensures that the server log directory is a valid directory owned by Oracle set with no permissions to public

Severity: Critical

Rationale: Log files provide information contained in an error stack. An error stack refers to the information that is produced by each layer in an Oracle communications stack as the result of a network error. The information in log files can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

15.2.42 Oracle Net Server Trace Directory Permission

Description: Ensures that the server trace directory is a valid directory owned by Oracle set with no permissions to public

Severity: Critical

Rationale: Tracing produces a detailed sequence of statements that describe network events as they are executed. Tracing an operation enables you to obtain more information on the internal operations of the components of Oracle Net Services than is provided in a log file. The information in this file can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

15.2.43 Oracle Net Server Trace Directory Permission(Windows)

Description: Ensures that the server trace directory is a valid directory owned by Oracle set with no permissions to public

Severity: Critical

Rationale: Tracing produces a detailed sequence of statements that describe network events as they are executed. Tracing an operation enables you to obtain more information on the internal operations of the components of Oracle Net Services than is provided in a log file. The information in this file can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

15.2.44 Protocol Error Further Action

Description: Ensures that the SEC_PROTOCOL_ERROR_FURTHER_ACTION parameter is set to either DROP or DELAY

Severity: Critical

Rationale: If default value CONTINUE is used, the server process continues execution even if bad packets are received. The database server may be subject to a Denial of Service (DoS) if bad packets continue to be sent by a malicious client

15.2.45 Protocol Error Trace Action

Description: Ensures that the sec_protocol_error_trace_action parameter is set to either LOG or ALERT

Severity: Critical

Rationale: SEC_PROTOCOL_ERROR_TRACE_ACTION specifies the action that the database should take when bad packets are received from a possibly malicious client. NONE should not be used as the database server ignores the bad packets and does not generate any trace files or log messages. If default value TRACE is used then the database server generates a detailed trace file and should only be used when debugging

15.2.46 Password Complexity Verification Function Usage

Description: Ensures PASSWORD_VERIFY_FUNCTION resource for the profile is set

Severity: Critical

Rationale: Having passwords that do not meet minimum complexity requirements offer substantially less protection than complex passwords.

15.2.47 Password Grace Time

Description: Ensures that all profiles have PASSWORD_GRACE_TIME set to a reasonable number of days

Severity: Critical

Rationale: A high value for the PASSWORD_GRACE_TIME parameter may cause serious database security issues by allowing the user to keep the same password for a long time.

15.2.48 Password Lifetime

Description: Ensures that all profiles have PASSWORD_LIFE_TIME set to a reasonable number of days

Severity: Warning

Rationale: A long password life time gives hackers a long time to try and cook the password. May cause serious database security issues.

15.2.49 Password Locking Time

Description: Ensures PASSWORD_LOCK_TIME is set to a reasonable number of days for all profiles

Severity: Warning

Rationale: Having a low value increases the likelihood of Denial of Service attacks.

15.2.50 Public Trace Files

Description: Ensures database trace files are not public readable

Severity: Critical

Rationale: If trace files are readable by the PUBLIC group, a malicious user may attempt to read the trace files that could lead to sensitive information being exposed.

15.2.51 Remote Os Authentication

Description: Ensure REMOTE_OS_AUTHENT initialization parameter is set to FALSE

Severity: Critical

Rationale: A malicious user can gain access to the database if remote OS authentication is allowed.

15.2.52 Remote Os Role

Description: Ensure REMOTE_OS_ROLES initialization parameter is set to FALSE

Severity: Critical

Rationale: A malicious user can gain access to the database if remote users can be granted privileged roles.

15.2.53 Restricted Privilege To Execute Utl_Http

Description: Ensure PUBLIC does not have execute privileges on the UTL_HTTP package

Severity: Critical

Rationale: Privileges granted to the PUBLIC role automatically apply to all users. A malicious user can gain access to email, network and http modules using the EXECUTE privilege.

15.2.54 Restricted Privilege To Execute Utl_Smtp

Description: Ensure PUBLIC does not have execute privileges on the UTL_SMTP package

Severity: Critical

Rationale: Privileges granted to the PUBLIC role automatically apply to all users. A malicious user can gain access to email, network and http modules using the EXECUTE privilege.

15.2.55 Restricted Privilege To Execute Utl_Tcp

Description: Ensure PUBLIC does not have execute privileges on the UTL_TCP package

Severity: Critical

Rationale: Privileges granted to the PUBLIC role automatically apply to all users. A malicious user can gain access to email, network and http modules using the EXECUTE privilege.

15.2.56 Ssl Cipher Suites Supported

Description: Ensures that the ssl_cipher_suites parameter is set to recommended value in sqlnet.ora

Severity: Warning

Rationale: This option is used to specify a cipher suite that will be used by the SSL connection. If the recommended cipher suite is not used, the SSL connection could be compromised.

15.2.57 Ssl Versions Supported

Description: Ensures that the ssl_version parameter is set to latest version .

Severity: Warning

Rationale: Usage of the most current version of SSL is recommended older versions of the SSL protocol are prone to attack or roll back. Do not set this parameter with Any.

15.2.58 Server Parameter File Permission

Description: Ensures that access to the server paramater file is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: A server parameter file (SPFILE) lets you store and manage your initialization parameters persistently in a server-side disk file. A publicly accessible SPFILE can be scanned for sensitive initialization parameters exposing the security policies of the database. The SPFILE can also be searched for the weaknesses of the Oracle database configuration setting.

15.2.59 Server Parameter File Permission(Windows)

Description: Ensures that access to the server paramater file is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: A server parameter file (SPFILE) lets you store and manage your initialization parameters persistently in a server-side disk file. A publicly accessible SPFILE can be scanned for sensitive initialization parameters exposing the security policies of the database. The SPFILE can also be searched for the weaknesses of the Oracle database configuration setting.

15.2.60 Use Of Appropriate Umask On Unix Systems

Description: On UNIX systems, ensure that the owner of the Oracle software has an appropriate umask value of 022 set

Severity: Warning

Rationale: If umask is not set to an appropriate value (like 022), log or trace files might become accessible to public exposing sensitive information.

15.2.61 Use Of Database Links With Cleartext Password

Description: Ensures database links with clear text passwords are not used

Severity: Warning

Rationale: The table SYS.LINK$ contains the clear text password used by the database link. A malicious user can read clear text password from SYS.LINK$ table that can lead to undesirable consequences.

15.2.62 Use Of Remote Listener Instances

Description: Ensures listener instances on a remote machine separate from the database instance are not used

Severity: Warning

Rationale: The REMOTE_LISTENER initialization parameter can be used to allow a listener on a remote machine to access the database. This parameter is not applicable in a multi-master replication or RAC environment where this setting provides a load balancing mechanism for the listener.

15.2.63 User Dump Destination

Description: Ensures that access to the trace files directory is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: The trace files for server processes are stored in the directory specified by the USER_DUMP_DEST initialization parameter. Giving public read permission to this directory may reveal important and sensitive internal details of the database and applications.

15.2.64 User Dump Destination(Windows)

Description: Ensures that access to the trace files directory is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: The trace files for server processes are stored in the directory specified by the USER_DUMP_DEST initialization parameter. Giving public read permission to this directory may reveal important and sensitive internal details of the database and applications.

15.2.65 Using Externally Identified Accounts

Description: Ensures that the OS authentication prefix is set to a value other than OPS $

Severity: Warning

Rationale: The OS_AUTHENT_PREFIX parameter specifies a prefix used to authenticate users attempting to connect to the server. When a connection request is attempted, Oracle compares the prefixed username with usernames in the database. Using a prefix, especially OPS$, tends to result in an insecure configuration as an account can be authenticated either as an operating system user or with the password used in the IDENTIFIED BY clause. Attackers are aware of this and will attack these accounts.

15.2.66 Utility File Directory Initialization Parameter Setting

Description: Ensures that the Utility File Directory (UTL_FILE_DIR) initialization parameter is not set to one of '*', '.', core dump trace file locations

Severity: Critical

Rationale: Specifies the directories which the UTL_FILE package can access. Having the parameter set to asterisk (*), period (.), or to sensitive directories, could expose them to all users having execute privilege on the UTL_FILE package.

15.2.67 Well Known Accounts

Description: Checks for accessibility of well-known accounts

Severity: Warning

Rationale: A knowledgeable malicious user can gain access to the database using a well-known account.

15.3 Configuration Best Practices For Oracle Database

The compliance rules for the Configuration Best Practices For Oracle Database standard follow.

15.3.1 Disabled Automatic Statistics Collection

Description: Checks if the STATISTICS_LEVEL initialization parameter is set to BASIC

Severity: Critical

Rationale: Automatic statistics collection allows the optimizer to generate accurate execution plans and is essential for identifying and correcting performance problems. By default, STATISTICS_LEVEL is set to TYPICAL. If the STATISTICS_LEVEL initialization parameter is set to BASIC the collection of many important statistics, required by Oracle database features and functionality, are disabled.

15.3.2 Fast Recovery Area Location Not Set

Description: Checks whether recovery area is set

Severity: Warning

Rationale: NO_RECOVERY_AREA_IMPACT

15.3.3 Force Logging Disabled

Description: Checks the database for disabled force logging.

Severity: Warning

Rationale: The database is not in force logging mode. If the database is a Data Guard primary database, unlogged direct writes will not be propagated to the standby database.

15.3.4 Insufficient Number Of Control Files

Description: Checks for use of a single control file

Severity: Critical

Rationale: The control file is one of the most important files in an Oracle database. It maintains many physical characteristics and important recovery information about the database. If youlose the only copy of the control file due to a media error, there will be unnecessary down time and other risks.

15.3.5 Not Using Automatic Pga Management

Description: Checks if the PGA_AGGREGATE_TARGET initialization parameter has a value of 0 or if WORKAREA_SIZE_POLICY has value of MANUAL.

Severity: Warning

Rationale: Automatic PGA memory management simplifies and improves the way PGA memory is allocated. When enabled, Oracle can dynamically adjust the portion of the PGA memory dedicated to work areas while honoring the PGA_AGGREGATE_TARGET limit set by the DBA.'

15.3.6 Not Using Automatic Undo Management

Description: Checks for automatic undo space management not being used

Severity: Minor Warning

Rationale: Not using automatic undo management can cause unnecessary contention and performance issues in your database. This may include among other issues, contention for the rollback segment header blocks, in the form of buffer busy waits and increased probability of ORA-1555s (Snapshot Too Old).

15.3.7 Not Using Spfile

Description: Checks for spfile not being used

Severity: Minor Warning

Rationale: The SPFILE (server parameter file) enables you persist any dynamic changes to the Oracle initialization parameters using ALTER SYSTEM commands. This persistence is provided acrossdatabase shutdowns. When a database has an SPFILE configured, you do not have to remember to make the corresponding changes to the Oracle init.ora file. Plus, any changes that are made via ALTER SYSTEM commands are not lost after an shutdown and restart.

15.3.8 Statistics_Level Parameter Set To All

Description: Checks if the STATISTICS_LEVEL initialization parameter is set to ALL

Severity: Minor Warning

Rationale: Automatic statistics collection allows the optimizer to generate accurate execution plans and is essential for identifying and correcting performance problems. The STATISTICS_LEVEL initialization parameter is currently set to ALL, meaning additional timed OS and plan execution statistics are being collected. These statistics are not necessary and create additional overhead on the system.

15.3.9 Timed_Statistics Set To False

Description: Checks if the TIMED_STATISTICS initialization parameter is set to FALSE.

Severity: Critical

Rationale: Setting TIMED_STATISTICS to FALSE prevents time related statistics, e.g. execution time for various internal operations, from being collected. These statistics are useful for diagnosing and performance tuning. Setting TIMED_STATISTICS to TRUE will allow time related statistics to be collected, and will also provide more value to the trace file and generates more accurate statistics for long-running operations.

15.3.10 Use Of Non-Standard Initialization Parameters

Description: Checks for use of non-standard initialization parameters

Severity: Minor Warning

Rationale: Non-standard initialization parameters are being used. These may have been implemented based on poor advice or incorrect assumptions. In particular, parameters associated with SPIN_COUNT on latches and undocumented optimizer features can cause a great deal of problems that can require considerable investigation.

15.4 High Security Configuration For Oracle Cluster Database Instance

The compliance rules for the High Security Configuration For Oracle Cluster Database Instance standard follow.

15.4.1 $Oracle_Home/Network/Admin File Permission

Description: Ensures the files in $ORACLE_HOME/network/admin ownership is restricted to the Oracle software set, group is restricted to DBA group and Public does not have write permission

Severity: Warning

Rationale: Not restricting ownership of network/admin to the Oracle software set and DBA group may cause security issues by exposing net configuration data to malicious users

15.4.2 $Oracle_Home/Network/Admin File Permission(Windows)

Description: Ensures the files in $ORACLE_HOME/network/admin ownership is restricted to the Oracle software set, group is restricted to DBA group and Public does not have write permission

Severity: Warning

Rationale: Not restricting ownership of network/admin to the Oracle software set and DBA group may cause security issues by exposing net configuration data to malicious users

15.4.3 Algorithm For Network Data Integrity Check On Server

Description: Ensures that the crypto_checksum_type_server parameter is set to SHA1 in sqlnet.ora

Severity: Warning

Rationale: This option ensures the integrity check for communication is done using SHA1 Algorithm

15.4.4 Background Dump Destination

Description: Ensures that access to the trace files directory is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: Background processes such as the log writer process and the database writer process use trace files to record occurrences and exceptions of database operations, as well as errors. The trace files are stored in the directory specified by the BACKGROUND_DUMP_DEST initialization parameter. Giving public read permission to this directory may reveal important and sensitive internal details of the database and applications.

15.4.5 Case Sensitive Logon

Description: Ensures that the sec_case_sensitive_logon parameter is set to true

Severity: Critical

Rationale: This increases the complexity of passwords and helps defend against brute force password attacks

15.4.6 Db Securefile

Description: Ensure that all LOB files created by Oracle are created as SecureFiles

Severity: Critical

Rationale: For LOBs to get treated as SecureFiles, set COMPATIBILE Initialization Param to 11.1 or higher. If there is a LOB column with two partitions (one that has a tablespace for which ASSM is enabled and one that has a tablespace for which ASSM is not enabled), then LOBs in the partition with the ASSM-enabled tablespace will be treated as SecureFiles and LOBs in the other partition will be treated as BasicFile LOBs. Setting db_securefile to ALWAYS makes sure that any LOB file created is a secure file

15.4.7 Dispatchers

Description: Ensures that the DISPATCHERS parameter is not set

Severity: Critical

Rationale: This will disable default ports ftp: 2100 and http: 8080. Removing the XDB ports will reduce the attack surface of the Oracle server. It is recommended to disable these ports if production usage is not required

15.4.8 Ifile Referenced File Permission

Description: Ensures that access to the files referenced by the IFILE parameter is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: The IFILE initialization parameter can be used to embed the contents of another initialization parameter file into the current initialization parameter file. A publicly accessible initialization parameter file can be scanned for sensitive initialization parameters exposing the security policies of the database. Initialization parameter file can also be searched for the weaknesses of the Oracle database configuration setting.

15.4.9 Ifile Referenced File Permission(Windows)

Description: Ensures that access to the files referenced by the IFILE parameter is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: The IFILE initialization parameter can be used to embed the contents of another initialization parameter file into the current initialization parameter file. A publicly accessible initialization parameter file can be scanned for sensitive initialization parameters exposing the security policies of the database. Initialization parameter file can also be searched for the weaknesses of the Oracle database configuration setting.

15.4.10 Log Archive Destination Owner

Description: Ensures that the server's archive logs directory is a valid directory owned by Oracle software owner

Severity: Critical

Rationale: LogMiner can be used to extract database information from the archive logs if the directory specified by LOG_ARCHIVE_DEST parameter (in init.ora file) is not owned by the owner of the Oracle software installation or has permissions for others.

15.4.11 Log Archive Destination Permission

Description: Ensures that the server's archive logs are not accessible to public

Severity: Critical

Rationale: LogMiner can be used to extract database information from the archive logs if the directory specified by LOG_ARCHIVE_DEST parameter (in init.ora file) is not owned by the owner of the Oracle software installation or has permissions for others.

15.4.12 Log Archive Destination Permission(Windows)

Description: Ensures that the server's archive logs are not accessible to public

Severity: Critical

Rationale: LogMiner can be used to extract database information from the archive logs if the directory specified by LOG_ARCHIVE_DEST parameter (in init.ora file) is not owned by the owner of the Oracle software installation or has permissions for others.

15.4.13 Log Archive Duplex Destination Owner

Description: Ensures that the server's archive logs directory is a valid directory owned by Oracle software owner

Severity: Critical

Rationale: LogMiner can be used to extract database information from the archive logs if the directory specified by LOG_ARCHIVE_DUPLEX_DEST parameter (in init.ora file) is not owned by the owner of the Oracle software installation or has permissions for others.

15.4.14 Log Archive Duplex Destination Permission

Description: Ensures that the server's archive logs are not accessible to public

Severity: Critical

Rationale: LogMiner can be used to extract database information from the archive logs if the directory specified by LOG_ARCHIVE_DUPLEX_DEST parameter (in init.ora file) is not owned by the owner of the Oracle software installation or has permissions for others.

15.4.15 Log Archive Duplex Destination Permission(Windows)

Description: Ensures that the server's archive logs are not accessible to public

Severity: Critical

Rationale: LogMiner can be used to extract database information from the archive logs if the directory specified by LOG_ARCHIVE_DUPLEX_DEST parameter (in init.ora file) is not owned by the owner of the Oracle software installation or has permissions for others.

15.4.16 Naming Database Links

Description: Ensures that the name of a database link is the same as that of the remote database

Severity: Warning

Rationale: Database link names that do not match the global names of the databases to which they are connecting can cause an administrator to inadvertently give access to a production server from a test or development server. Knowledge of this can be used by a malicious user to gain access to the target database.

15.4.17 Oracle_Home Network Admin Owner

Description: Ensures $ORACLE_HOME/network/admin ownership is restricted to the Oracle software set and DBA group

Severity: Warning

Rationale: Not restricting ownership of network/admin to the Oracle software set and DBA group may cause security issues by exposing net configuration data to malicious users

15.4.18 Os Roles

Description: Ensure roles are stored, managed, and protected in the database rather than files external to the DBMS.

Severity: Warning

Rationale: If Roles are managed by OS, it can cause serious security issues.

15.4.19 Oracle Agent Snmp Read-Only Configuration File Owner

Description: Ensures Oracle Agent SNMP read-only configuration file (snmp_ro.ora) is owned by Oracle software owner

Severity: Warning

Rationale: The Oracle Agent SNMP read-only configuration file (snmp_ro.ora) contains the listening address of the agent, the names of SQL*Net listener and Oracle database servicesit knows about, plus tracing parameters. A publicly accessible SNMP

read-only configuration file can be used to extract sensitive data like the tracing directory location, dbsnmp address, etc.

15.4.20 Oracle Agent Snmp Read-Only Configuration File Permission

Description: Ensures Oracle Agent SNMP read-only configuration file (snmp_ro.ora) permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: The Oracle Agent SNMP read-only configuration file (snmp_ro.ora) contains the listening address of the agent, the names of SQL*Net listener and Oracle database servicesit knows about, plus tracing parameters. A publicly accessible SNMP read-only configuration file can be used to extract sensitive data like the tracing directory location, dbsnmp address, etc.

15.4.21 Oracle Agent Snmp Read-Only Configuration File Permission(Windows)

Description: Ensures Oracle Agent SNMP read-only configuration file (snmp_ro.ora) permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: The Oracle Agent SNMP read-only configuration file (snmp_ro.ora) contains the listening address of the agent, the names of SQL*Net listener and Oracle database servicesit knows about, plus tracing parameters. A publicly accessible SNMP read-only configuration file can be used to extract sensitive data like the tracing directory location, dbsnmp address, etc.

15.4.22 Oracle Agent Snmp Read-Write Configuration File Owner

Description: Ensures Oracle Agent SNMP read-write configuration file (snmp_rw.ora) is owned by Oracle software owner

Severity: Warning

Rationale: The Oracle Agent SNMP read-write configuration file (snmp_ro.ora) contains the listening address of the agent, the names of SQL*Net listener and Oracle database services it knows about, plus tracing parameters. A publicly accessible SNMP read-write configuration file can be used to extract sensitive data like the tracing directory location, dbsnmp address, etc.

15.4.23 Oracle Agent Snmp Read-Write Configuration File Permission

Description: Ensures Oracle Agent SNMP read-write configuration file (snmp_rw.ora) permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: The Oracle Agent SNMP read-write configuration file (snmp_ro.ora) contains the listening address of the agent, the names of SQL*Net listener and Oracle database services it knows about, plus tracing parameters. A publicly accessible SNMP read-write configuration file can be used to extract sensitive data like the tracing directory location, dbsnmp address, etc.

15.4.24 Oracle Agent Snmp Read-Write Configuration File Permission(Windows)

Description: Ensures Oracle Agent SNMP read-write configuration file (snmp_rw.ora) permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: The Oracle Agent SNMP read-write configuration file (snmp_ro.ora) contains the listening address of the agent, the names of SQL*Net listener and Oracle database services it knows about, plus tracing parameters. A publicly accessible SNMP read-write configuration file can be used to extract sensitive data like the tracing directory location, dbsnmp address, etc.

15.4.25 Oracle Http Server Distributed Configuration File Owner

Description: Ensures Oracle HTTP Server distributed configuration file ownership is restricted to the Oracle software set and DBA group

Severity: Warning

Rationale: The Oracle HTTP Server distributed configuration file (usually .htaccess) is used for access control and authentication of web folders. This file can be modified to gain access to pages containing sensitive information.

15.4.26 Oracle Http Server Distributed Configuration Files Permission

Description: Ensures Oracle HTTP Server Distributed Configuration Files permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: The Oracle HTTP Server distributed configuration file (usually .htaccess) is used for access control and authentication of web folders. This file can be modified to gain access to pages containing sensitive information.

15.4.27 Oracle Http Server Mod_Plsql Configuration File Owner

Description: Ensures Oracle HTTP Server mod_plsql configuration file (wdbsvr.app) is owned by Oracle software owner

Severity: Warning

Rationale: The Oracle Agent SNMP read-write configuration file (snmp_rw.ora) contains the listening address of the agent, the names of SQL*Net listener and Oracle database services it knows about, plus tracing parameters. A publicly accessible SNMP read-write configuration file can be used to extract sensitive data like the tracing directory location, dbsnmp address, etc.

15.4.28 Oracle Http Server Mod_Plsql Configuration File Permission

Description: Ensures Oracle HTTP Server mod_plsql Configuration file (wdbsvr.app) permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: The Oracle Agent SNMP read-write configuration file (snmp_rw.ora) contains the listening address of the agent, the names of SQL*Net listener and Oracle database services it knows about, plus tracing parameters. A publicly accessible SNMP read-write configuration file can be used to extract sensitive data like the tracing directory location, dbsnmp address, etc.

15.4.29 Oracle Http Server Mod_Plsql Configuration File Permission(Windows)

Description: Oracle HTTP Server mod_plsql Configuration file (wdbsvr.app) permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: The Oracle HTTP Server mod_plsql configuration file (wdbsvr.app) contains the Database Access Descriptors used for authentication. A publicly accessible mod_plsql configuration file can allow a malicious user to modify the Database Access Descriptor settings to gain access to PL/SQL applications or launch a Denial Of Service attack.

15.4.30 Oracle Home Executable Files Permission

Description: Ensures that all files in the ORACLE_HOME/bin folder do not have public write permission

Severity: Warning

Rationale: Incorrect file permissions on some of the Oracle files can cause major security issues.

15.4.31 Oracle Home Executable Files Permission(Windows)

Description: Ensures that all files in the ORACLE_HOME/bin folder do not have public write permission

Severity: Warning

Rationale: Incorrect file permissions on some of the Oracle files can cause major security issues.

15.4.32 Oracle Net Client Log Directory Owner

Description: Ensures that the client log directory is a valid directory owned by Oracle set

Severity: Critical

Rationale: Log files provide information contained in an error stack. An error stack refers to the information that is produced by each layer in an Oracle communications stack as the result of a network error. The information in log files can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

15.4.33 Oracle Net Client Trace Directory Owner

Description: Ensures that the client trace directory is a valid directory owned by Oracle set

Severity: Critical

Rationale: Tracing produces a detailed sequence of statements that describe network events as they are executed. Tracing an operation enables you to obtain more information on the internal operations of the components of Oracle Net Services than is provided in a log file. The information in this file can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

15.4.34 Oracle Net Inbound Connect Timeout

Description: Ensures that all incomplete inbound connections to Oracle Net has a limited lifetime

Severity: Warning

Rationale: Without this parameter or assigning it with a higher value , a client connection to the database server can stay open indefinitely or for the specified duration without authentication. Connections without authentication can introduce possible denial-of-service attacks, whereby malicious clients attempt to flood database servers with connect requests that consume resources.

15.4.35 Oracle Net Ssl_Cert_Revocation

Description: Ensures that the ssl_cert_revocation parameter is set to recommended value in sqlnet.ora

Severity: Warning

Rationale: This option Ensures revocation is required for checking CRLs for client certificate authentication. Revoked certificates can pose a threat to the integrity of the SSL channel and should not be trusted

15.4.36 Oracle Net Ssl_Server_Dn_Match

Description: Ensures ssl_server_dn_match is enabled in sqlnet.ora and in turn SSL ensures that the certificate is from the server

Severity: Warning

Rationale: If ssl_server_dn_match parameter is disabled, then SSL performs the check but allows the connection, regardless if there is a match. Not enforcing the match allows the server to potentially fake its identity.

15.4.37 Oracle Net Server Log Directory Owner

Description: Ensures that the server log directory is a valid directory owned by Oracle set

Severity: Critical

Rationale: Log files provide information contained in an error stack. An error stack refers to the information that is produced by each layer in an Oracle communications stack as the result of a network error. The information in log files can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

15.4.38 Oracle Net Server Trace Directory Owner

Description: Ensures that the server trace directory is a valid directory owned by Oracle set

Severity: Critical

Rationale: Tracing produces a detailed sequence of statements that describe network events as they are executed. Tracing an operation enables you to obtain more information on the internal operations of the components of Oracle Net Services than is provided in a log file. The information in this file can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

15.4.39 Oracle Net Sqlnet Expire Time

Description: Ensures that sqlnet.expire_time parameter is set to recommended value.

Severity: Warning

Rationale: if sqlnet.expire_time is not set or set to 0, then database never checks for dead connection and they keeps consuming database server resources.

15.4.40 Oracle Net Tcp Validnode Checking

Description: Ensures that tcp.validnode_checking parameter is set to yes.

Severity: Minor Warning

Rationale: Not setting valid node check can potentially allow anyone to connect to the sever, including a malicious user.

15.4.41 Oracle Xsql Configuration File Owner

Description: Ensures Oracle XSQL configuration file (XSQLConfig.xml) is owned by Oracle software owner

Severity: Warning

Rationale: The Oracle XSQL configuration file (XSQLConfig.xml) contains sensitive database connection information. A publicly accessible XSQL configuration file can expose the database username and password that can be used access sensitive data or to launch further attacks.

15.4.42 Oracle Xsql Configuration File Permission

Description: Ensures Oracle XSQL configuration file (XSQLConfig.xml) permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: The Oracle XSQL configuration file (XSQLConfig.xml) contains sensitive database connection information. A publicly accessible XSQL configuration file can expose the database username and password that can be used access sensitive data or to launch further attacks.

15.4.43 Oracle Xsql Configuration File Permission(Windows)

Description: Ensures Oracle XSQL Configuration File (XSQLConfig.xml) permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: The Oracle XSQL configuration file (XSQLConfig.xml) contains sensitive database connection information. A publicly accessible XSQL configuration file can expose the database username and password that can be used access sensitive data or to launch further attacks.

15.4.44 Otrace Data Files

Description: Avoids negative impact on database performance and disk space usage, caused by data collected by otrace

Severity: Warning

Rationale: Performance and resource utilization data collection can have a negative impact on database performance and disk space usage.

15.4.45 Return Server Release Banner

Description: Ensures that value of parameter SEC_RETURN_SERVER_RELEASE_BANNER is FALSE

Severity: Critical

Rationale: If the Parameter SEC_RETURN_SERVER_RELEASE_BANNER is TRUE oracle database returns complete database version information to clients. Knowing the exact patch set can aid an attacker

15.4.46 Remote Password File

Description: Ensures privileged users are authenticated by the operating system; that is, Oracle ignores any password file

Severity: Minor Warning

Rationale: The REMOTE_LOGIN_PASSWORDFILE parameter specifies whether or not Oracle checks for a password file. Because password files contain the passwords for users, including SYS, the most secure way of preventing an attacker from connecting through brute-force password-related attacks is to require privileged users be authenticated by the operating system.

15.4.47 Restrict Sqlnet.Ora Permission

Description: Ensures that the sqlnet.ora file is not accessible to public

Severity: Critical

Rationale: If sqlnet.ora is public readable a malicious user may attempt to read this hence could lead to sensitive information getting exposed .For example, log and trace destination information of the client and server.

15.4.48 Restrict Sqlnet.Ora Permission(Windows)

Description: Ensures that the sqlnet.ora file is not accessible to public

Severity: Critical

Rationale: If sqlnet.ora is public readable a malicious user may attempt to read this hence could lead to sensitive information getting exposed .For example, log and trace destination information of the client and server.

15.4.49 Sql*Plus Executable Owner

Description: Ensures SQL*Plus ownership is restricted to the Oracle software set and DBA group

Severity: Warning

Rationale: SQL*Plus allows a user to execute any SQL on the database. Not restricting ownership of SQL*Plus to the Oracle software set and DBA group may cause security issues by exposing sensitive data to malicious users.

15.4.50 Sql*Plus Executable Permission

Description: Ensures that SQL*Plus executable file permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: SQL*Plus allows a user to execute any SQL on the database. Public execute permissions on SQL*Plus can cause security issues by exposing sensitive data to malicious users.

15.4.51 Sql*Plus Executable Permission(Windows)

Description: Ensures that SQL*Plus executable file permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: SQL*Plus allows a user to execute any SQL on the database. Public execute permissions on SQL*Plus can cause security issues by exposing sensitive data to malicious users.

15.4.52 Secure Os Audit Level

Description: On UNIX systems, ensures that AUDIT_SYSLOG_LEVEL is set to a non-default value when OS-level auditing is enabled.

Severity: Warning

Rationale: Setting the AUDIT_SYSLOG_LEVEL initialization parameter to the default value (NONE) will result in DBAs gaining access to the OS audit records

15.4.53 Tkprof Executable Owner

Description: Ensures tkprof executable file is owned by Oracle software owner

Severity: Warning

Rationale: Not restricting ownership of tkprof to the Oracle software set and DBA group may cause information leak.

15.4.54 Tkprof Executable Permission

Description: Ensures tkprof executable file permissions are restricted to read and execute for the group, and inaccessible to public

Severity: Warning

Rationale: Excessive permission for tkprof leaves information within, unprotected.

15.4.55 Tkprof Executable Permission(Windows)

Description: Ensures tkprof executable file permissions are restricted to read and execute for the group, and inaccessible to public

Severity: Warning

Rationale: Excessive permission for tkprof leaves information within, unprotected.

15.4.56 Use Of Automatic Log Archival Features

Description: Ensures that archiving of redo logs is done automatically and prevents suspension of instance operations when redo logs fill. Only applicable if database is in archivelog mode

Severity: Critical

Rationale: Setting the LOG_ARCHIVE_START initialization parameter to TRUE ensures that the archiving of redo logs is done automatically and prevents suspension of instance operations when redo logs fill. This feature is only applicable if the database is in archivelog mode.

15.4.57 Use Of Sql92 Security Features

Description: Ensures use of SQL92 security features

Severity: Warning

Rationale: If SQL92 security features are not enabled, a user might be able to execute an UPDATE or DELETE statement using a WHERE clause without having select privilege on a table.

15.4.58 Utility File Directory Initialization Parameter Setting In Oracle9I Release 1 And Later

Description: Ensure that the UTL_FILE_DIR initialization parameter is not used in Oracle9i Release 1 and later

Severity: Critical

Rationale: Specifies the directories which UTL_FILE package can access. Having the parameter set to asterisk (*), period (.), or to sensitive directories could expose them to all users having execute privilege on UTL_FILE package.

15.4.59 Webcache Initialization File Owner

Description: Ensures Webcache initialization file (webcache.xml) is owned by Oracle software owner

Severity: Warning

Rationale: Webcache stores sensitive information in the initialization file (webcache.xml). A publicly accessible Webcache initialization file can be used to extract sensitive data like the administrator password hash.

15.4.60 Webcache Initialization File Permission

Description: Ensures the Webcache initialization file (webcache.xml) permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: Webcache stores sensitive information in the initialization file (webcache.xml). A publicly accessible Webcache initialization file can be used to extract sensitive data like the administrator password hash.

15.4.61 Webcache Initialization File Permission(Windows)

Description: Ensures the Webcache initialization file (webcache.xml) permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: Webcache stores sensitive information in the initialization file (webcache.xml). A publicly accessible Webcache initialization file can be used to extract sensitive data like the administrator password hash.

15.4.62 Tcp.Excludeded_Nodes

Description: Ensures that tcp.excludeded_nodes parameter is set.

Severity: Warning

Rationale: Not setting valid node check can potentially allow anyone to connect to the sever, including a malicious user.

15.4.63 Tcp.Invited_Nodes

Description: Ensures that tcp.invited_nodes parameter is set.

Severity: Warning

Rationale: Not setting valid node check can potentially allow anyone to connect to the sever, including a malicious user.

15.5 High Security Configuration For Oracle Database

The compliance rules for the High Security Configuration For Oracle Database standard follow.

15.5.1 "Domain Users" Group Member Of Local "Users" Group

Description: Ensures domain server local Users group does not have Domain Users group

Severity: Warning

Rationale: Including Domain Users group in local Users group of a domain server can cause serious security issues.

15.5.2 $Oracle_Home/Network/Admin File Permission

Description: Ensures the files in $ORACLE_HOME/network/admin ownership is restricted to the Oracle software set, group is restricted to DBA group and Public does not have write permission

Severity: Warning

Rationale: Not restricting ownership of network/admin to the Oracle software set and DBA group may cause security issues by exposing net configuration data to malicious users

15.5.3 $Oracle_Home/Network/Admin File Permission(Windows)

Description: Ensures the files in $ORACLE_HOME/network/admin ownership is restricted to the Oracle software set, group is restricted to DBA group and Public does not have write permission

Severity: Warning

Rationale: Not restricting ownership of network/admin to the Oracle software set and DBA group may cause security issues by exposing net configuration data to malicious users

15.5.4 Access To *_Catalog_* Roles

Description: Ensure grant of *_CATALOG_* is restricted

Severity: Critical

Rationale: *_CATALOG_* Roles have critical access to database objects, that can lead to exposure of vital information in database system.

15.5.5 Access To All_Source View

Description: Ensures restricted access to ALL_SOURCE view

Severity: Minor Warning

Rationale: ALL_SOURCE view contains source of all stored packages in the database.

15.5.6 Access To Dba_* Views

Description: Ensures SELECT privilege is never granted to any DBA_ view

Severity: Warning

Rationale: The DBA_* views provide access to privileges and policy settings of the database. Some of these views also allow viewing of sensitive PL/SQL code that can be used to understand the security policies.

15.5.7 Access To Role_Role_Privs View

Description: Ensures restricted access to ROLE_ROLE_PRIVS view

Severity: Minor Warning

Rationale: Lists roles granted to other roles. Knowledge of the structure of roles in the database can be taken advantage of by a malicious user.

15.5.8 Access To Sys.Link$ Table

Description: Ensures restricted access to LINK$ table

Severity: Minor Warning

Rationale: A knowlegeable and malicious user can gain access to user passwords from the SYS.LINK$ table.

15.5.9 Access To User_Role_Privs View

Description: Ensures restricted access to USER_ROLE_PRIVS view

Severity: Minor Warning

Rationale: Lists the roles granted to the current user. Knowledge of the structure of roles in the database can be taken advantage of by a malicious user.

15.5.10 Access To User_Tab_Privs View

Description: Ensures restricted access to USER_TAB_PRIVS view

Severity: Minor Warning

Rationale: Lists the grants on objects for which the user is the owner, grantor or grantee. Knowledge of the grants in the database can be taken advantage of by a malicious user.

15.5.11 Access To V$ Synonyms

Description: Ensures SELECT privilege is not granted to any V$ synonyms

Severity: Critical

Rationale: V$ tables contain sensitive information about Oracle database and should only be accessible by system administrators. Check for any user that has access and revoke where possible

15.5.12 Access To V$ Views

Description: Ensures SELECT privilege is not granted to any V$ Views

Severity: Critical

Rationale: V$ tables contain sensitive information about Oracle database and should only be accessible by system administrators. Check for any user that has access and revoke where possible

15.5.13 Access To X_$ Views

Description: Ensure access on X$ views is restricted

Severity: Critical

Rationale: This can lead to revealing of internal database structure information.

15.5.14 Algorithm For Network Data Integrity Check On Server

Description: Ensures that the crypto_checksum_type_server parameter is set to SHA1 in sqlnet.ora

Severity: Warning

Rationale: This option ensures the integrity check for communication is done using SHA1 Algorithm

15.5.15 Audit Alter Any Table Privilege

Description: Ensures ALTER ANY TABLE Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing ALTER ANY TABLE will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

15.5.16 Audit Alter User Privilege

Description: Ensures ALTER USER Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing ALTER USER will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

15.5.17 Audit Aud$ Privilege

Description: Ensures AUD$ is being audited by access for all users

Severity: Critical

Rationale: Auditing AUD$ will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

15.5.18 Audit Create Any Library Privilege

Description: Ensures CREATE ANY LIBRARY is being audited by access for all users

Severity: Critical

Rationale: Auditing CREATE ANY LIBRARY will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

15.5.19 Audit Create Library Privilege

Description: Ensures CREATE LIBRARY Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing CREATE LIBRARY will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

15.5.20 Audit Create Role Privilege

Description: Ensures CREATE ROLE Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing the creation of roles will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

15.5.21 Audit Create Session Privilege

Description: Ensures CREATE SESSION Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing CREATE SESSION will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

15.5.22 Audit Create User Privilege

Description: Ensures CREATE USER Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing CREATE USER will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

15.5.23 Audit Drop Any Procedure Privilege

Description: Ensures DROP ANY PROCEDURE Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing DROP ANY PROCEDURE will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

15.5.24 Audit Drop Any Role Privilege

Description: Ensures DROP ANY ROLE Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing the creation of roles will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

15.5.25 Audit Drop Any Table Privilege

Description: Ensures DROP ANY TABLE Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing DROP ANY TABLE will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

15.5.26 Audit Execute Any Procedure Privilege

Description: Ensures EXECUTE ANY PROCEDURE Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing the creation of roles will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

15.5.27 Audit Grant Any Object Privilege

Description: Ensures every use of GRANT ANY OBJECT privilege is being audited for non-Administrative (SYSDBA) users.

Severity: Critical

Rationale: Auditing GRANT ANY OBJECT privilege will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

15.5.28 Audit Grant Any Privilege

Description: Ensures GRANT ANY PRIVILEGE is being audited by access for all users

Severity: Critical

Rationale: Auditing GRANT ANY PRIVILEGE will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

15.5.29 Audit Insert Failure

Description: Ensures that insert failures are audited for critical data objects

Severity: Warning

Rationale: Not auditing insert failures for critical data objects may allow a malicious user to infiltrate system security..

15.5.30 Audit Select Any Dictionary Privilege

Description: Ensures SELECT ANY DICTIONARY Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing SELECT ANY DICTIONARY will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

15.5.31 Background Dump Destination

Description: Ensures that access to the trace files directory is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: Background processes such as the log writer process and the database writer process use trace files to record occurrences and exceptions of database operations, as well as errors. The trace files are stored in the directory specified by the BACKGROUND_DUMP_DEST initialization parameter. Giving public read permission to this directory may reveal important and sensitive internal details of the database and applications.

15.5.32 Case Sensitive Logon

Description: Ensures that the sec_case_sensitive_logon parameter is set to true

Severity: Critical

Rationale: This increases the complexity of passwords and helps defend against brute force password attacks

15.5.33 Connect Time

Description: Ensure that users profile settings CONNECT_TIME have appropriate value set for the particular database and application

Severity: Critical

Rationale: Sessions held open for excessive periods of time can consume system resources and cause a denial of service for other users of the Oracle database. The CONNECT_TIME parameter limits the upper bound on how long a session can be held open. This parameter is specified in minutes. Sessions that have exceeded their connect time are aborted and rolled back

15.5.34 Cpu Per Session

Description: Ensures that all profiles have CPU_PER_SESSION set to a reasonable number of CPU cycles

Severity: Critical

Rationale: Allowing a single application or user to consume excessive CPU resources will result in a denial of service to the Oracle database

15.5.35 Db Securefile

Description: Ensure that all LOB files created by Oracle are created as SecureFiles

Severity: Critical

Rationale: For LOBs to get treated as SecureFiles, set COMPATIBILE Initialization Param to 11.1 or higher. If there is a LOB column with two partitions (one that has a tablespace for which ASSM is enabled and one that has a tablespace for which ASSM is not enabled), then LOBs in the partition with the ASSM-enabled tablespace will be treated as SecureFiles and LOBs in the other partition will be treated as BasicFile LOBs. Setting db_securefile to ALWAYS makes sure that any LOB file created is a secure file

15.5.36 Dispatchers

Description: Ensures that the DISPATCHERS parameter is not set

Severity: Critical

Rationale: This will disable default ports ftp: 2100 and http: 8080. Removing the XDB ports will reduce the attack surface of the Oracle server. It is recommended to disable these ports if production usage is not required

15.5.37 Execute Privileges On Dbms_Lob To Public

Description: Ensures PUBLIC group is not granted EXECUTE privileges to the DBMS_LOB package

Severity: Critical

Rationale: The DBMS_LOB package can be used to access any file on the system as the owner of the Oracle software installation.

15.5.38 Execute Privileges On Utl_File To Public

Description: Ensure PUBLIC does not have EXECUTE privilege on the UTL_FILE package

Severity: Critical

Rationale: Privileges granted to the PUBLIC role automatically apply to all users. A malicious user can read and write arbitrary files in the system when granted the UTL_FILE privilege.

15.5.39 Execute Privilege On Sys.Dbms_Export_Extension To Public

Description: Ensure PUBLIC does not have execute privileges on the SYS.DBMS_EXPORT_EXTENSION package

Severity: Critical

Rationale: Privileges granted to the PUBLIC role automatically apply to all users. DBMS_EXPORT_EXTENSION can allow sql injection. Thus a malicious will be able to take advantage.

15.5.40 Execute Privilege On Sys.Dbms_Random Public

Description: Ensure PUBLIC does not have execute privileges on the SYS.DBMS_RANDOM package

Severity: Critical

Rationale: Privileges granted to the PUBLIC role automatically apply to all users. DBMS_RANDOM can allow sql injection. Thus a malicious will be able to take advantage.

15.5.41 Granting Select Any Table Privilege

Description: Ensures SELECT ANY PRIVILEGE is never granted to any user or role

Severity: Warning

Rationale: The SELECT ANY TABLE privilege can be used to grant users or roles with the ability to view data in tables that are not owned by them. A malicious user with access to any user account that has this privilege can use this to gain access to sensitive data.

15.5.42 Ifile Referenced File Permission

Description: Ensures that access to the files referenced by the IFILE parameter is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: The IFILE initialization parameter can be used to embed the contents of another initialization parameter file into the current initialization parameter file. A publicly accessible initialization parameter file can be scanned for sensitive initialization parameters exposing the security policies of the database. Initialization parameter file can also be searched for the weaknesses of the Oracle database configuration setting.

15.5.43 Ifile Referenced File Permission(Windows)

Description: Ensures that access to the files referenced by the IFILE parameter is restricted to the owner of the Oracle software set and the DBA group

Severity: Critical

Rationale: The IFILE initialization parameter can be used to embed the contents of another initialization parameter file into the current initialization parameter file. A publicly accessible initialization parameter file can be scanned for sensitive initialization parameters exposing the security policies of the database. Initialization parameter file can also be searched for the weaknesses of the Oracle database configuration setting.

15.5.44 Installation On Domain Controller

Description: Ensures that Oracle is not installed on a domain controller

Severity: Warning

Rationale: Installing Oracle on a domain controller can cause serious security issues.

15.5.45 Installed Oracle Home Drive Permissions

Description: On Windows, ensures that the installed Oracle Home drive is not accessible to Everyone Group

Severity: Warning

Rationale: Giving permission of Oracle installed drive to everyone can cause serious security issues.

15.5.46 Logical Reads Per Session

Description: Ensure that users profile settings LOGICAL_READS_ PER_SESSION have appropriate value set for the particular database and application

Severity: Critical

Rationale: Allowing a single application or user to perform excessive amounts of reads to disk will result in a denial of service to the Oracle database

15.5.47 Limit Os Authentication

Description: Ensures database accounts does not rely on OS authentication

Severity: Critical

Rationale: If the host operating system has a required userid for database account for which password is set EXTERNAL, then Oracle does not check its credentials anymore. It simplyassumes the host must have done its authentication and lets the user into the database without any further checking.

15.5.48 Log Archive Destination Owner

Description: Ensures that the server's archive logs directory is a valid directory owned by Oracle software owner

Severity: Critical

Rationale: LogMiner can be used to extract database information from the archive logs if the directory specified by LOG_ARCHIVE_DEST parameter (in init.ora file) is not owned by the owner of the Oracle software installation or has permissions for others.

15.5.49 Log Archive Destination Permission

Description: Ensures that the server's archive logs are not accessible to public

Severity: Critical

Rationale: LogMiner can be used to extract database information from the archive logs if the directory specified by LOG_ARCHIVE_DEST parameter (in init.ora file) is not owned by the owner of the Oracle software installation or has permissions for others.

15.5.50 Log Archive Destination Permission(Windows)

Description: Ensures that the server's archive logs are not accessible to public

Severity: Critical

Rationale: LogMiner can be used to extract database information from the archive logs if the directory specified by LOG_ARCHIVE_DEST parameter (in init.ora file) is not owned by the owner of the Oracle software installation or has permissions for others.

15.5.51 Log Archive Duplex Destination Owner

Description: Ensures that the server's archive logs directory is a valid directory owned by Oracle software owner

Severity: Critical

Rationale: LogMiner can be used to extract database information from the archive logs if the directory specified by LOG_ARCHIVE_DUPLEX_DEST parameter (in init.ora file) is not owned by the owner of the Oracle software installation or has permissions for others.

15.5.52 Log Archive Duplex Destination Permission

Description: Ensures that the server's archive logs are not accessible to public

Severity: Critical

Rationale: LogMiner can be used to extract database information from the archive logs if the directory specified by LOG_ARCHIVE_DUPLEX_DEST parameter (in init.ora file) is not owned by the owner of the Oracle software installation or has permissions for others.

15.5.53 Log Archive Duplex Destination Permission(Windows)

Description: Ensures that the server's archive logs are not accessible to public

Severity: Critical

Rationale: LogMiner can be used to extract database information from the archive logs if the directory specified by LOG_ARCHIVE_DUPLEX_DEST parameter (in init.ora file) is not owned by the owner of the Oracle software installation or has permissions for others.

15.5.54 Naming Database Links

Description: Ensures that the name of a database link is the same as that of the remote database

Severity: Warning

Rationale: Database link names that do not match the global names of the databases to which they are connecting can cause an administrator to inadvertently give access to a production server from a test or development server. Knowledge of this can be used by a malicious user to gain access to the target database.

15.5.55 Oracle_Home Network Admin Owner

Description: Ensures $ORACLE_HOME/network/admin ownership is restricted to the Oracle software set and DBA group

Severity: Warning

Rationale: Not restricting ownership of network/admin to the Oracle software set and DBA group may cause security issues by exposing net configuration data to malicious users

15.5.56 Os Roles

Description: Ensure roles are stored, managed, and protected in the database rather than files external to the DBMS.

Severity: Warning

Rationale: If Roles are managed by OS, it can cause serious security issues.

15.5.57 Oracle Agent Snmp Read-Only Configuration File Owner

Description: Ensures Oracle Agent SNMP read-only configuration file (snmp_ro.ora) is owned by Oracle software owner

Severity: Warning

Rationale: The Oracle Agent SNMP read-only configuration file (snmp_ro.ora) contains the listening address of the agent, the names of SQL*Net listener and Oracle database servicesit knows about, plus tracing parameters. A publicly accessible SNMP read-only configuration file can be used to extract sensitive data like the tracing directory location, dbsnmp address, etc.

15.5.58 Oracle Agent Snmp Read-Only Configuration File Permission

Description: Ensures Oracle Agent SNMP read-only configuration file (snmp_ro.ora) permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: The Oracle Agent SNMP read-only configuration file (snmp_ro.ora) contains the listening address of the agent, the names of SQL*Net listener and Oracle database servicesit knows about, plus tracing parameters. A publicly accessible SNMP read-only configuration file can be used to extract sensitive data like the tracing directory location, dbsnmp address, etc.

15.5.59 Oracle Agent Snmp Read-Only Configuration File Permission(Windows)

Description: Ensures Oracle Agent SNMP read-only configuration file (snmp_ro.ora) permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: The Oracle Agent SNMP read-only configuration file (snmp_ro.ora) contains the listening address of the agent, the names of SQL*Net listener and Oracle database servicesit knows about, plus tracing parameters. A publicly accessible SNMP read-only configuration file can be used to extract sensitive data like the tracing directory location, dbsnmp address, etc.

15.5.60 Oracle Agent Snmp Read-Write Configuration File Owner

Description: Ensures Oracle Agent SNMP read-write configuration file (snmp_rw.ora) is owned by Oracle software owner

Severity: Warning

Rationale: The Oracle Agent SNMP read-write configuration file (snmp_ro.ora) contains the listening address of the agent, the names of SQL*Net listener and Oracle database services it knows about, plus tracing parameters. A publicly accessible SNMP read-write configuration file can be used to extract sensitive data like the tracing directory location, dbsnmp address, etc.

15.5.61 Oracle Agent Snmp Read-Write Configuration File Permission

Description: Ensures Oracle Agent SNMP read-write configuration file (snmp_rw.ora) permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: The Oracle Agent SNMP read-write configuration file (snmp_ro.ora) contains the listening address of the agent, the names of SQL*Net listener and Oracle database services it knows about, plus tracing parameters. A publicly accessible SNMP read-write configuration file can be used to extract sensitive data like the tracing directory location, dbsnmp address, etc.

15.5.62 Oracle Agent Snmp Read-Write Configuration File Permission(Windows)

Description: Ensures Oracle Agent SNMP read-write configuration file (snmp_rw.ora) permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: The Oracle Agent SNMP read-write configuration file (snmp_ro.ora) contains the listening address of the agent, the names of SQL*Net listener and Oracle database services it knows about, plus tracing parameters. A publicly accessible SNMP read-write configuration file can be used to extract sensitive data like the tracing directory location, dbsnmp address, etc.

15.5.63 Oracle Http Server Distributed Configuration File Owner

Description: Ensures Oracle HTTP Server distributed configuration file ownership is restricted to the Oracle software set and DBA group

Severity: Warning

Rationale: The Oracle HTTP Server distributed configuration file (usually .htaccess) is used for access control and authentication of web folders. This file can be modified to gain access to pages containing sensitive information.

15.5.64 Oracle Http Server Distributed Configuration Files Permission

Description: Ensures Oracle HTTP Server Distributed Configuration Files permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: The Oracle HTTP Server distributed configuration file (usually .htaccess) is used for access control and authentication of web folders. This file can be modified to gain access to pages containing sensitive information.

15.5.65 Oracle Http Server Mod_Plsql Configuration File Owner

Description: Ensures Oracle HTTP Server mod_plsql configuration file (wdbsvr.app) is owned by Oracle software owner

Severity: Warning

Rationale: The Oracle Agent SNMP read-write configuration file (snmp_rw.ora) contains the listening address of the agent, the names of SQL*Net listener and Oracle database services it knows about, plus tracing parameters. A publicly accessible SNMP read-write configuration file can be used to extract sensitive data like the tracing directory location, dbsnmp address, etc.

15.5.66 Oracle Http Server Mod_Plsql Configuration File Permission

Description: Ensures Oracle HTTP Server mod_plsql Configuration file (wdbsvr.app) permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: The Oracle Agent SNMP read-write configuration file (snmp_rw.ora) contains the listening address of the agent, the names of SQL*Net listener and Oracle database services it knows about, plus tracing parameters. A publicly accessible SNMP read-write configuration file can be used to extract sensitive data like the tracing directory location, dbsnmp address, etc.

15.5.67 Oracle Http Server Mod_Plsql Configuration File Permission(Windows)

Description: Oracle HTTP Server mod_plsql Configuration file (wdbsvr.app) permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: The Oracle HTTP Server mod_plsql configuration file (wdbsvr.app) contains the Database Access Descriptors used for authentication. A publicly accessible mod_plsql configuration file can allow a malicious user to modify the Database Access Descriptor settings to gain access to PL/SQL applications or launch a Denial Of Service attack.

15.5.68 Oracle Home Executable Files Permission

Description: Ensures that all files in the ORACLE_HOME/bin folder do not have public write permission

Severity: Warning

Rationale: Incorrect file permissions on some of the Oracle files can cause major security issues.

15.5.69 Oracle Home Executable Files Permission(Windows)

Description: Ensures that all files in the ORACLE_HOME/bin folder do not have public write permission

Severity: Warning

Rationale: Incorrect file permissions on some of the Oracle files can cause major security issues.

15.5.70 Oracle Net Client Log Directory Owner

Description: Ensures that the client log directory is a valid directory owned by Oracle set

Severity: Critical

Rationale: Log files provide information contained in an error stack. An error stack refers to the information that is produced by each layer in an Oracle communications stack as the result of a network error. The information in log files can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

15.5.71 Oracle Net Client Trace Directory Owner

Description: Ensures that the client trace directory is a valid directory owned by Oracle set

Severity: Critical

Rationale: Tracing produces a detailed sequence of statements that describe network events as they are executed. Tracing an operation enables you to obtain more information on the internal operations of the components of Oracle Net Services than is provided in a log file. The information in this file can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

15.5.72 Oracle Net Inbound Connect Timeout

Description: Ensures that all incomplete inbound connections to Oracle Net has a limited lifetime

Severity: Warning

Rationale: Without this parameter or assigning it with a higher value , a client connection to the database server can stay open indefinitely or for the specified duration without authentication. Connections without authentication can introduce possible denial-of-service attacks, whereby malicious clients attempt to flood database servers with connect requests that consume resources.

15.5.73 Oracle Net Ssl_Cert_Revocation

Description: Ensures that the ssl_cert_revocation parameter is set to recommended value in sqlnet.ora

Severity: Warning

Rationale: This option Ensures revocation is required for checking CRLs for client certificate authentication. Revoked certificates can pose a threat to the integrity of the SSL channel and should not be trusted

15.5.74 Oracle Net Ssl_Server_Dn_Match

Description: Ensures ssl_server_dn_match is enabled in sqlnet.ora and in turn SSL ensures that the certificate is from the server

Severity: Warning

Rationale: If ssl_server_dn_match parameter is disabled, then SSL performs the check but allows the connection, regardless if there is a match. Not enforcing the match allows the server to potentially fake its identity.

15.5.75 Oracle Net Server Log Directory Owner

Description: Ensures that the server log directory is a valid directory owned by Oracle set

Severity: Critical

Rationale: Log files provide information contained in an error stack. An error stack refers to the information that is produced by each layer in an Oracle communications stack as the result of a network error. The information in log files can reveal important

network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

15.5.76 Oracle Net Server Trace Directory Owner

Description: Ensures that the server trace directory is a valid directory owned by Oracle set

Severity: Critical

Rationale: Tracing produces a detailed sequence of statements that describe network events as they are executed. Tracing an operation enables you to obtain more information on the internal operations of the components of Oracle Net Services than is provided in a log file. The information in this file can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

15.5.77 Oracle Net Sqlnet Expire Time

Description: Ensures that sqlnet.expire_time parameter is set to recommended value.

Severity: Warning

Rationale: if sqlnet.expire_time is not set or set to 0, then database never checks for dead connection and they keeps consuming database server resources.

15.5.78 Oracle Net Tcp Validnode Checking

Description: Ensures that tcp.validnode_checking parameter is set to yes.

Severity: Minor Warning

Rationale: Not setting valid node check can potentially allow anyone to connect to the sever, including a malicious user.

15.5.79 Oracle Xsql Configuration File Owner

Description: Ensures Oracle XSQL configuration file (XSQLConfig.xml) is owned by Oracle software owner

Severity: Warning

Rationale: The Oracle XSQL configuration file (XSQLConfig.xml) contains sensitive database connection information. A publicly accessible XSQL configuration file can expose the database username and password that can be used access sensitive data or to launch further attacks.

15.5.80 Oracle Xsql Configuration File Permission

Description: Ensures Oracle XSQL configuration file (XSQLConfig.xml) permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: The Oracle XSQL configuration file (XSQLConfig.xml) contains sensitive database connection information. A publicly accessible XSQL configuration file can expose the database username and password that can be used access sensitive data or to launch further attacks.

15.5.81 Oracle Xsql Configuration File Permission(Windows)

Description: Ensures Oracle XSQL Configuration File (XSQLConfig.xml) permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: The Oracle XSQL configuration file (XSQLConfig.xml) contains sensitive database connection information. A publicly accessible XSQL configuration file can expose the database username and password that can be used access sensitive data or to launch further attacks.

15.5.82 Otrace Data Files

Description: Avoids negative impact on database performance and disk space usage, caused by data collected by otrace

Severity: Warning

Rationale: Performance and resource utilization data collection can have a negative impact on database performance and disk space usage.

15.5.83 Private Sga

Description: Ensure that users PRIVATE_SGA profile settings have appropriate values set for the particular database and application

Severity: Critical

Rationale: Allowing a single application or user to consume the excessive amounts of the System Global Area will result in a denial of service to the Oracle database

15.5.84 Password Reuse Max

Description: Ensures that all profiles have PASSWORD_REUSE_MAX set to a reasonable number of times

Severity: Warning

Rationale: Old passwords are usually the best guesses for the current password. A low value for the PASSWORD_REUSE_MAX parameter may cause serious database security issues by allowing users to reuse their old passwords more often.

15.5.85 Password Reuse Time

Description: Ensures that all profiles have PASSWORD_REUSE_TIME set to a reasonable number of days

Severity: Critical

Rationale: A low value for the PASSWORD_REUSE_TIME parameter may cause serious database security issues by allowing users to reuse their old passwords more often.

15.5.86 Proxy Account

Description: Ensures that the proxy accounts have limited privileges

Severity: Warning

Rationale: The proxy user only needs to connect to the database. Once connected it will use the privileges of the user it is connecting on behalf of. Granting any other privilege than the CREATE SESSION privilege to the proxy user is unnecessary and open to misuse.

15.5.87 Return Server Release Banner

Description: Ensures that value of parameter SEC_RETURN_SERVER_RELEASE_BANNER is FALSE

Severity: Critical

Rationale: If the Parameter SEC_RETURN_SERVER_RELEASE_BANNER is TRUE oracle database returns complete database version information to clients. Knowing the exact patch set can aid an attacker

15.5.88 Remote Password File

Description: Ensures privileged users are authenticated by the operating system; that is, Oracle ignores any password file

Severity: Minor Warning

Rationale: The REMOTE_LOGIN_PASSWORDFILE parameter specifies whether or not Oracle checks for a password file. Because password files contain the passwords for users, including SYS, the most secure way of preventing an attacker from connecting through brute-force password-related attacks is to require privileged users be authenticated by the operating system.

15.5.89 Restrict Sqlnet.Ora Permission

Description: Ensures that the sqlnet.ora file is not accessible to public

Severity: Critical

Rationale: If sqlnet.ora is public readable a malicious user may attempt to read this hence could lead to sensitive information getting exposed .For example, log and trace destination information of the client and server.

15.5.90 Restrict Sqlnet.Ora Permission(Windows)

Description: Ensures that the sqlnet.ora file is not accessible to public

Severity: Critical

Rationale: If sqlnet.ora is public readable a malicious user may attempt to read this hence could lead to sensitive information getting exposed .For example, log and trace destination information of the client and server.

15.5.91 Sessions_Per_User

Description: Ensures that all profiles have SESSIONS_PER_USER set to a reasonable number

Severity: Critical

Rationale: Allowing an unlimited amount of sessions per user can consume Oracle resources and cause a denial of service. Limit the number of session for each individual user

15.5.92 Sql*Plus Executable Owner

Description: Ensures SQL*Plus ownership is restricted to the Oracle software set and DBA group

Severity: Warning

Rationale: SQL*Plus allows a user to execute any SQL on the database. Not restricting ownership of SQL*Plus to the Oracle software set and DBA group may cause security issues by exposing sensitive data to malicious users.

15.5.93 Sql*Plus Executable Permission

Description: Ensures that SQL*Plus executable file permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: SQL*Plus allows a user to execute any SQL on the database. Public execute permissions on SQL*Plus can cause security issues by exposing sensitive data to malicious users.

15.5.94 Sql*Plus Executable Permission(Windows)

Description: Ensures that SQL*Plus executable file permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: SQL*Plus allows a user to execute any SQL on the database. Public execute permissions on SQL*Plus can cause security issues by exposing sensitive data to malicious users.

15.5.95 Secure Os Audit Level

Description: On UNIX systems, ensures that AUDIT_SYSLOG_LEVEL is set to a non-default value when OS-level auditing is enabled.

Severity: Warning

Rationale: Setting the AUDIT_SYSLOG_LEVEL initialization parameter to the default value (NONE) will result in DBAs gaining access to the OS audit records

15.5.96 System Privileges To Public

Description: Ensure system privileges are not granted to PUBLIC

Severity: Critical

Rationale: Privileges granted to the public role automatically apply to all users. There are security risks granting SYSTEM privileges to all users.

15.5.97 Tkprof Executable Owner

Description: Ensures tkprof executable file is owned by Oracle software owner

Severity: Warning

Rationale: Not restricting ownership of tkprof to the Oracle software set and DBA group may cause information leak.

15.5.98 Tkprof Executable Permission

Description: Ensures tkprof executable file permissions are restricted to read and execute for the group, and inaccessible to public

Severity: Warning

Rationale: Excessive permission for tkprof leaves information within, unprotected.

15.5.99 Tkprof Executable Permission(Windows)

Description: Ensures tkprof executable file permissions are restricted to read and execute for the group, and inaccessible to public

Severity: Warning

Rationale: Excessive permission for tkprof leaves information within, unprotected.

15.5.100 Unlimited Tablespace Quota

Description: Ensures database users are allocated a limited tablespace quota

Severity: Warning

Rationale: Granting unlimited tablespace quotas can cause the filling up of the allocated disk space. This can lead to an unresponsive database.

15.5.101 Use Of Automatic Log Archival Features

Description: Ensures that archiving of redo logs is done automatically and prevents suspension of instance operations when redo logs fill. Only applicable if database is in archivelog mode

Severity: Critical

Rationale: Setting the LOG_ARCHIVE_START initialization parameter to TRUE ensures that the archiving of redo logs is done automatically and prevents suspension of instance operations when redo logs fill. This feature is only applicable if the database is in archivelog mode.

15.5.102 Use Of Sql92 Security Features

Description: Ensures use of SQL92 security features

Severity: Warning

Rationale: If SQL92 security features are not enabled, a user might be able to execute an UPDATE or DELETE statement using a WHERE clause without having select privilege on a table.

15.5.103 Use Of Windows Nt Domain Prefix

Description: Ensures externally identified users specify the domain while connecting

Severity: Critical

Rationale: This setting is only applicable to Windows systems. If externally identified accounts are required, setting OSAUTH_PREFIX_DOMAIN to TRUE in the registry forces the account to specify the domain. This prevents spoofing of user access from an alternate domain or local system.

15.5.104 Utility File Directory Initialization Parameter Setting In Oracle9I Release 1 And Later

Description: Ensure that the UTL_FILE_DIR initialization parameter is not used in Oracle9i Release 1 and later

Severity: Critical

Rationale: Specifies the directories which UTL_FILE package can access. Having the parameter set to asterisk (*), period (.), or to sensitive directories could expose them to all users having execute privilege on UTL_FILE package.

15.5.105 Webcache Initialization File Owner

Description: Ensures Webcache initialization file (webcache.xml) is owned by Oracle software owner

Severity: Warning

Rationale: Webcache stores sensitive information in the initialization file (webcache.xml). A publicly accessible Webcache initialization file can be used to extract sensitive data like the administrator password hash.

15.5.106 Webcache Initialization File Permission

Description: Ensures the Webcache initialization file (webcache.xml) permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: Webcache stores sensitive information in the initialization file (webcache.xml). A publicly accessible Webcache initialization file can be used to extract sensitive data like the administrator password hash.

15.5.107 Webcache Initialization File Permission(Windows)

Description: Ensures the Webcache initialization file (webcache.xml) permissions are limited to the Oracle software set and DBA group

Severity: Warning

Rationale: Webcache stores sensitive information in the initialization file (webcache.xml). A publicly accessible Webcache initialization file can be used to extract sensitive data like the administrator password hash.

15.5.108 Windows Tools Permission

Description: Ensures Oracle service does not have permissions on windows tools

Severity: Warning

Rationale: Granting Oracle service the permissions of windows tools may cause serious securty issues.

15.5.109 Tcp.Excludeded_Nodes

Description: Ensures that tcp.excludeded_nodes parameter is set.

Severity: Warning

Rationale: Not setting valid node check can potentially allow anyone to connect to the sever, including a malicious user.

15.5.110 Tcp.Invited_Nodes

Description: Ensures that tcp.invited_nodes parameter is set.

Severity: Warning

Rationale: Not setting valid node check can potentially allow anyone to connect to the sever, including a malicious user.

15.6 Patchable Configuration For Oracle Database

The compliance rules for the Patchable Configuration For Oracle Database standard follow.

15.6.1 Patchability

Description: Ensure the Oracle Database target has a patchable configuration

Severity: Warning

Rationale: Unpatchable Oracle Database target could not be patched by using the provided EM Patching feature

15.7 Storage Best Practices For Oracle Database

The compliance rules for the Storage Best Practices For Oracle Database standard follow.

15.7.1 Default Permanent Tablespace Set To A System Tablespace

Description: Checks if the DEFAULT_PERMANENT_TABLESPACE database property is set to a system tablespace

Severity: Warning

Rationale: If not specified explicitly, DEFAULT_PERMANENT_TABLESPACE is defaulted to the SYSTEM tablespace. This is not the recommended setting. With this setting, any user that is not explicitly assigned a tablespace uses the system tablespace. Doing so may result in performance degradation for the database. This is also a security issue. Non-system users may store data and consume all available space in the system tablespace, thus causing the database to stop working.

15.7.2 Default Temporary Tablespace Set To A System Tablespace

Description: Checks if the DEFAULT_TEMP_TABLESPACE database property is set to a system tablespace

Severity: Warning

Rationale: If not specified explicitly, DEFAULT_TEMP_TABLESPACE would default to SYSTEM tablespace and this is not a recommended setting. With this setting, any user that is not explicitly assigned a temporary tablespace uses the system tablespace as their temporary tablespace. System tablespaces should not be used to store temporary data. This is also a security issue. Non-system users may store data and consume all available space in the system tablespace, thus causing the database to stop working.

15.7.3 Dictionary Managed Tablespaces

Description: Checks for dictionary managed tablespaces

Severity: Minor Warning

Rationale: These tablespaces are dictionary managed. Oracle recommends using locally managed tablespaces, with AUTO segment-space management, to enhance performance and ease of space management.

15.7.4 Insufficient Number Of Redo Logs

Description: Checks for use of less than three redo logs

Severity: Warning

Rationale: The online redo log files are used to record changes in the database. When archiving is enabled, these online redo logs need to be archived before they can be reused. Every database requires at least two online redo log groups to be up and running. When the size and number of online redo logs are inadequate, LGWR will wait for ARCH to complete its writing to the archived log destination, before it overwrites that log. This can cause severe performance slowdowns during peak activity periods.

15.7.5 Insufficient Redo Log Size

Description: Checks for redo log files less than 1 Mb

Severity: Critical

Rationale: Small redo logs cause system checkpoints to continuously put a high load on the buffer cache and I/O system.

15.7.6 Non-System Data Segments In System Tablespaces

Description: Checks for data segments owned by non-system users located in tablespaces SYSTEM, SYSAUX and SYSEXT.

Severity: Minor Warning

Rationale: These segments belonging to non-system users are stored in system tablespaces SYSTEM or SYSAUX or SYSEXT. This violation makes it more difficult to manage these data segments and may result in performance degradation in the system tablespace. This is also a security issue. If non-system users are storing data in a system tablespace it is possible that all available space in the system tablespace may be consumed, thus causing the database to stop working.

15.7.7 Non-System Users With System Tablespace As Default Tablespace

Description: Checks for non-system users using SYSTEM or SYSAUX as the default tablespace

Severity: Minor Warning

Rationale: These non-system users use a system tablespace as the default tablespace. This violation will result in non-system data segments being added to the system tablespace, making it more difficult to manage these data segments and possibly resulting in performance degradation in the system tablespace. This is also a security issue. All Available space in the system tablespace may beconsumed, thus causing the database to stop working.

15.7.8 Non-Uniform Default Extent Size For Tablespaces

Description: Checks for dictionary managed or migrated locally managed tablespaces with non-uniform default extent size

Severity: Minor Warning

Rationale: Dictionary managed or migrated locally managed tablespaces using non-uniform default extent sizes have been found. This means that the extents in a single tablespace will vary insize leading to fragmentation, inefficient space usage and performance degradation.

15.7.9 Rollback In System Tablespace

Description: Checks for rollback segments in SYSTEM tablespace

Severity: Minor Warning

Rationale: The SYSTEM tablespace should be reserved only for the Oracle data dictionary and its associated objects. It should NOT be used to store any other types of objects such as user tables, user indexes, user views, rollback segments, undo segments or temporary segments.

15.7.10 Tablespace Not Using Automatic Segment-Space Management

Description: Checks for locally managed tablespaces that are using MANUAL segment space management

Severity: Minor Warning

Rationale: Automatic segment-space management is a simpler and more efficient way of managing space within a segment. It completely eliminates any need to specify and tune the PCTUSED, FREELISTS and FREELIST GROUPS storage parameters for schema objects created in the tablespace. In a RAC environment there is the additional benefit of avoiding the hard partitioning of space inherent with using free list groups.

15.7.11 Tablespaces Containing Rollback And Data Segments

Description: Checks for tablespaces containing both rollback and data segments

Severity: Minor Warning

Rationale: These tablespaces contain both rollback and data segments. Mixing segment types in this way makes it more difficult to manage space and may degrade performance in the tablespace. Use of a dedicated tablespace for rollback segments enhances availability and performance.

15.7.12 Users With Permanent Tablespace As Temporary Tablespace

Description: Checks for users using a permanent tablespace as the temporary tablespace

Severity: Minor Warning

Rationale: These users use a permanent tablespace as the temporary tablespace. Using temporary tablespaces allows space management for sort operations to be more efficient. Using a permanent tablespace for these operations may result in performance degradation, especially for Real Application Clusters. There is an additional security concern. This makes it possible for users to use all available space in the system tablespace, causing the database to stop working.

16

Oracle WebLogic Cluster Compliance Standards

These are the compliance rules for the Oracle WebLogic Cluster compliance standards

16.1 Weblogic Cluster Configuration Compliance

The compliance rules for the Weblogic Cluster Configuration Compliance standard follow.

16.1.1 Session Lazy Deserialization Enabled

Description: The compliance standard rule verifies whether SessionLazyDeserializationEnabled attribute is enabled or not for the server running on exalogic.

Severity: Critical

Rationale: Enabling this attribute, improves Session replication performance and CPU utilization of the server, which avoids performing extra work on every session update, that is only necessary when a server fails.

17

Oracle WebLogic Domain Compliance Standards

These are the compliance rules for the Oracle WebLogic Domain compliance standards.

Note:

See My Oracle Support for additional information regarding the future of the deprecated standards.

17.1 All WLS V10 Rules (Deprecated)

The compliance rules for the All Wls V10 Rules standard follow.

17.1.1 Administration Server Is Hosting Applications Other Than Oracle System Applications

Description: Your Administration Server is hosting applications other than Oracle system applications. Oracle recommends hosting these applications only on the managed servers within your domain. The only applications that should be deployed to your Administration Server are Oracle applications (for example, the Oracle WebLogic Server Administration Console and Oracle agents).

Severity: Warning

17.1.2 Administration Console Hangs During Restart Of A Remote Managed Server

Description: Cannot display the JNDI tree on the Oracle WebLogic Server console on a managed server. It seems that the problem is caused by an empty <jndi-name> tag, which was accidentally added in the datasource configuration file.<jdbc-data-source-params> <jndi-name>dsGestionRepresentations</jndi-name> <jndi-name></jndi-name><global-transactions-protocol>TwoPhaseCommit</global-transactions-protocol></jdbc-data-source-params>Will see a StackOverflowError in the logs as a symptom of this problem.

Severity: Critical

Rationale: Server Outage

17.1.3 Administration Console Hangs During Restart Of A Remote Managed Server

Description: When the Administration Console is used to stop and restart a remote managed server, the Administration Console hangs until the remote managed server has been fully started.The remote managed servers are started by the Node Manager.

If there is no response from a remote managed server at startup, the Administration Console hangs.

Severity: Warning

Rationale: Administration

17.1.4 Administration Console Hangs During Restart Of A Remote Managed Server. (Upgrade)

Description: When the Administration Console is used to stop and restart a remote managed server, the Administration Console hangs until the remote managed server has been fully started.The remote managed servers are started by the Node Manager. If there is no response from a remote managed server at startup, the Administration Console hangs.This problem, described in Oracle Bug 8158504, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.1.5 Administration Console Hangs During Restart Of A Remote Managed Server. (Upgrade)

Description: The JNDI tree on the Oracle WebLogic Server Administration Console cannot be displayed for a managed server. It seems that the problem is caused by an empty <jndi-name> tag, which was accidentally added in the DataSource configuration file.<jdbc-data-source-params> <jndi-name>dsGestionRepresentations</jndi-name> <jndi-name></jndi-name><global-transactions-protocol>TwoPhaseCommit</global-transactions-protocol></jdbc-data-source-params>This problem, described in 8164017, has been fixed in Oracle WebLogic Server 10.3 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Server Outage

17.1.6 An Org.Hibernate.Lazyinitializationexception Occurs For Calls Over Iiop (Wls V10.0)

Description: When using the -Dweblogic.iiop.useJavaSerialization flag in a call over IIOP, an org.hibernate.LazyInitializationException can occur.

Severity: Critical

Rationale: Server Outage

17.1.7 An Org.Hibernate.Lazyinitializationexception Occurs For Calls Over Iiop (Wls V10.0, Upgrade)

Description: When using the -Dweblogic.iiop.useJavaSerialization flag in a call over IIOP, an org.hibernate.LazyInitializationException can occur.This problem, described in Oracle Bug 8145565, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Server Outage

17.1.8 Annotation Does Not Work With Unchecked Exceptions

Description: For Oracle WebLogic Server 10.0 with EJB3.0, an ApplicationException occurs. Annotation does not work with unchecked exceptions.

Severity: Critical

Rationale: Server Outage

17.1.9 Annotation Does Not Work With Unchecked Exceptions (Wls V10.0, Upgrade)

Description: For Oracle WebLogic Server 10.0 with EJB3.0, an ApplicationException occurs. Annotation does not work with unchecked exceptions.This problem, described in Oracle Bug 8179501, has been fixed in Oracle WebLogic Server 10.3 Maintenance Pack 1

Severity: Minor Warning

Rationale: Server Outage

17.1.10 Arrayindexoutofboundsexception Occurs In Jspencoder Class When Compiling Jsp Files

Description: The following ArrayIndexOutOfBoundsException is thrown by the JspEncoder class when compiling certain JSP files:java.lang.ArrayIndexOutOfBoundsException: 0 at javelin.jsp.JspEncoder $JspxEncoder.guessEncodingFamily(JspEncoder.java:304) at workshop.util.encoding.EncodingManager._detectEncoding(EncodingManager.java: 174) at workshop.util.encoding.EncodingManager.findIEncodingForReader(EncodingManage r.java:104)

Severity: Warning

Rationale: Performance

17.1.11 Bea07-175.00 - Ssl Clients May Miss Possible Cipher Suites Resulting In Use Of Null Cipher (Wls V10)

Description: In some circumstances, SSL clients that run outside the server environment may not find all possible ciphers with which to construct the list of potential SSL cipher suites resulting in use of the default null cipher (no encryption).This advisory corrects this issue by supplying jars and instructions to ensure all cipher suites are found.

Severity: Critical

Rationale: Server Outage

17.1.12 Bea07-176.00 - Server May Select Null Cipher Suite For Ssl Communication With Ssl Clients (Wls V10.0.0)

Description: An attacker could obtain and exploit information that is not encrypted when a null cipher suite is in use. Under certain circumstances, when a client does not offer support for any of the cipher suites available in the server, then the server may select a cipher suite that uses a null cipher; this may result in SSL communication that is not encrypted.This advisory corrects this issue by logging a message when null

cipher is in use and also provides administrators the ability to disable the use of null ciphers during SSL communications with SSL clients.

Severity: Critical

Rationale: Server Outage

17.1.13 Bea07-177.00 - Multiple Security Vulnerabilities In The Java Runtime Environment

Description: Contact Oracle Support or visit support.oracle.com for the following information:- A JavaDoc defect may lead to the generation of HTML documentation pages with potential cross-site scripting (XSS) vulnerability.- A buffer overflow vulnerability in the JRE image parsing code may allow an untrusted applet or application to elevate its privileges.- A vulnerability in the JRE font parsing code may allow an untrusted applet to elevate its privileges.- The Java XML Digital Signature implementation in JDK and JRE 6 does not securely process XSLT stylesheets in XSLT Transforms in XML Signatures.- A JRE Applet Class Loader security vulnerability may allow an untrusted applet that is loaded from a remote system to circumvent network access.

Severity: Critical

Rationale: Administration

17.1.14 Bea07-178.00 - Java Secure Socket Extension Does Not Correctly Process Ssl/Tls Handshake

Description: The Java Secure Socket Extension (JSSE) that is included in various releases of the Java Runtime Environment does not correctly process SSL/TLS handshake requests. This vulnerability may be exploited to create a Denial of Service (DoS) condition to the system as a whole on a server that listens for SSL/TLS connections using JSSE for SSL/TLS support. For more information, please contact Oracle Support or visit support.oracle.com.This advisory corrects this issue by supplying patched versions of JRockit.

Severity: Critical

Rationale: Administration

17.1.15 Bea08-191.00 - Tampering Html Request Headers Could Lead To An Elevation Of Privileges (Wls V10.0)

Description: An attacker can spoof certain information in a request header that can lead to possibly getting access to application servlets that rely on this information for authentication.This advisory corrects this issue by ensuring that the header information is properly handled before passing it to the servlet.

Severity: Critical

Rationale: Administration

17.1.16 Bea08-193.00 - Non-Authorized User May Be Able To Receive Messages From A Secured Jms (Wls V10)

Description: WebLogic security policies can be configured to restrict the access to a JMS destination. If an application user does not have the "receive" permission to a JMS destination (queue/topic), an attempt to receive messages from that destination by the

application should fail with security errors. By exploiting this vulnerability, an unauthorized user may be able to receive messages from a standalone (physical) JMS Topic destination or a member of a secured Distributed Topic member destination.This advisory resolves this issue by checking permissions before allowing a subscriber to use a durable subscription.

Severity: Critical

Rationale: Administration

17.1.17 Bea08-194.00 - A Non-Authorized User May Be Able To Send Messages To A Protected Queue (Wls V10)

Description: The distributed queue feature in Oracle WebLogic Server JMS provides higher availability in a clustered environment. If a JMS client sends a message to a distributed queue and encounters a problem with one member of that distributed queue (the member is down, the member exceeds its quota, access denied, etc), internally the JMS subsystem will retry another member of the same distributed destination. In certain configurations, an unauthorized user is able to send messages to a secure distributed queue.This advisory corrects the problem and ensures that the correct user identity is maintained.

Severity: Critical

Rationale: Administration

17.1.18 Bea08-195.00 - Cross-Site Scripting Vulnerability In Console'S Unexpected Exception Page (Wls V10)

Description: Cross-Site Scripting (XSS) vulnerabilityFor more information, see:http://download.oracle.com/docs/cd/E13222_01/wls/docs81/servlet/progtasks.html#160803Background: Cross-Site Scripting (XSS) vulnerabilities are well documented in the industry. An XSS vulnerability requires three parties:Installers, updates, patches and more information are available at support.oracle.com.

Severity: Critical

Rationale: Administration

17.1.19 Bea08-196.00 - A Session Fixation Exploit Could Result In Elevated Privileges. (Wls V10.0)

Description: In order to exploit this vulnerability, an attacker must have access to the server's console login page and have a non-administrator user account on that server. A session fixation vulnerability exists which can result in elevation of the attacker's privileges. For more information about Session Fixation attacks, see:http://en.wikipedia.org/wiki/Session_fixationThis advisory corrects this issue by always regenerating an auth cookie on login.

Severity: Critical

Rationale: Administration

17.1.20 Bea08-197.00 - Account Lockout Can Be Bypassed, Exposing The Account To Brute-Force Attack

Description: In order to avoid brute-force credential attacks, Oracle WebLogic Server has a mechanism that locks the corresponding user account after a certain number of

invalid login attempts. By default, the account is locked after 5 invalid login attempts and remains locked for 30 minutes.Even after a user has been locked out, logon requests to certain carefully constructed URLs can still give hints as to whether the password is correct or not. This allows a sophisticated attacker to successfully run a brute-force password attack, a dictionary attack, or other similar attacks.The patch associated with this advisory corrects the problem. All sites that use servlets are vulnerable to this problem.

Severity: Critical

Rationale: Administration

17.1.21 Bea08-199.00 - A Carefully Constructed Url May Cause Sun, Iis, Or Apache Webserver To Crash. (Wls V10)

Description: An attacker can use a carefully constructed URL to cause BEA's proxy plugin to crash the Sun, IIS or Apache web server process. On re-start, this may cause in-flight requests to be lost. This can cause a temporary denial of service. This attack can be exploited remotely, and the attacker does not need any authentication.This advisory resolves the issue in the plugin by correctly handling URLs.

Severity: Critical

Rationale: Administration

17.1.22 Bea08-201.00 - Multiple Security Vulnerabilities In The Java Runtime Environment

Description: This is a combined security advisory. These vulnerabilities are fixed in JRockit R27.5.0. Installers, updates, patches and more information are available at support.oracle.com.

Severity: Critical

Rationale: Administration

17.1.23 Bea08-80.04 - Patches Available To Prevent Multiple Cross-Site Scripting Vulnerabilities. (Wls V10)

Description: Cross-Site Scripting (XSS) vulnerabilityFor more information, see:http://download.oracle.com/docs/cd/E13222_01/wls/docs81/servlet/progtasks.html#160803Caution About Existing Samples:Our samples are intended to provide a simple tutorial regarding a few specific features. They are not comprehensive guides to best practices. Many of them omit the use of the Utils.encodeXSS() method or other XSS preventative techniques in needed places and are hence vulnerable to XSS attacks.

Severity: Critical

Rationale: Administration

17.1.24 Blocked Threads Occur In Jspfactory.Getdefaultfactory() Method

Description: While evaluating each EL Expression in JSP, blocked threads occur in a static synchronized method, JspFactory.getDefaultFactory(), resulting in performance degradation.A sample thread dump below shows a blocked thread occurring in the getDefaultFactory() method."[ACTIVE] ExecuteThread: '116' for queue: 'weblogic.kernel.Default (self-tuning)'" daemon prio=6 tid=0x5ff3e870 nid=0xa90

waiting for monitor entry [0x67c8d000..0x67c8fd1c] at javax.servlet.jsp.JspFactory.getDefaultFactory(JspFactory.java:87) - waiting to lock <0x0645ab30> (a java.lang.Class) at weblogic.servlet.jsp.ELHelper.getExpressionFactory(ELHelper.java:114) ...

Severity: Minor Warning

Rationale: Development

17.1.25 Blocked Threads Occur In Jspfactory.Getdefaultfactory() Method (Upgrade)

Description: While evaluating each EL Expression in JSP, blocked threads occur in a static synchronized method, JspFactory.getDefaultFactory(), resulting in performance degradation.A sample thread dump below shows a blocked thread occurring in the getDefaultFactory() method."[ACTIVE] ExecuteThread: '116' for queue: 'weblogic.kernel.Default (self-tuning)'" daemon prio=6 tid=0x5ff3e870 nid=0xa90 waiting for monitor entry [0x67c8d000..0x67c8fd1c] at javax.servlet.jsp.JspFactory.getDefaultFactory(JspFactory.java:87) - waiting to lock <0x0645ab30> (a java.lang.Class)...This problem, described in Oracle Bug 8174471, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Development

17.1.26 Boxing Conversion Of Small Integer Values Incorrect In Oracle Jrockit R27.2.X And R27.3.X

Description: The following Java class should produce TRUE for Integer values within the range(-128...+127). However, with Oracle JRockit releases R27.2.X and R27.3.X, this may return FALSE.public class Test { public static void main(String[] args) { Integer i1 = 4, i2 = 4; System.out.println(i1 == i2); }}

Severity: Minor Warning

Rationale: Development

17.1.27 Cve-2008-1006 - Multiple Security Vulnerabilities In Jrockit

Description: Advisory CVE-2009-1006 refers to all the vulnerability fixes that have been made in JRockit for addressing the applicable issues. The applicable advisories include:CVE 2008-5347CVE 2008-5348CVE 2008-5349CVE 2008-5350CVE 2008-5351CVE 2008-5352CVE 2008-5353CVE 2008-5354CVE 2008-5356CVE 2008-5360xFor more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.1.28 Cve-2008-2578 - Information Disclosure Vulnerability In The Weblogic Console Or Server Log

Description: Information Disclosure vulnerability in the WebLogic console or server log.

Severity: Critical

Rationale: Administration

17.1.29 Cve-2008-2579 - Information Disclosure Vulnerability In Weblogic Plug-Ins For Web Servers (Wls V10)

Description: Information disclosure vulnerability in WebLogic Server plug-ins for Apache, Sun, and IIS Web servers.

Severity: Critical

Rationale: Administration

17.1.30 Cve-2008-2580 - Information Disclosure In Jsp Pages (Wls V10.0)

Description: Information disclosure in JSP pages.

Severity: Critical

Rationale: Administration

17.1.31 Cve-2008-2581 - Elevation Of Privilege Vulnerabilities In The Uddi Explorer (Wls V10)

Description: Elevation of privilege vulnerabilities in the UDDI Explorer.

Severity: Critical

Rationale: Administration

17.1.32 Cve-2008-2582 - Denial-Of-Service Vulnerability In Weblogic Server

Description: Denial-of-Service vulnerability in WebLogic Server.

Severity: Critical

Rationale: Server Outage

17.1.33 Cve-2008-3103 - Security Vulnerability In Java Management Extensions (Jmx)

Description: A vulnerability in the Java Management Extensions (JMX) management agent included in the Java Runtime Environment (JRE) may allow a JMX client running on a remote host to perform unauthorized operations on a system running JMX with local monitoring enabled.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.1.34 Cve-2008-3104 - Security Vulnerabilities In Java Runtime Environment Allows Same Origin

Description: Security vulnerabilities in the Java Runtime Environment may allow an untrusted applet that is loaded from a remote system to circumvent network access restrictions and establish socket connections to certain services running on machines other than the one that the applet was downloaded from. This may allow the untrusted remote applet the ability to exploit any security vulnerabilities existing in the services it has connected to.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.1.35 Cve-2008-3105 - Security Vulnerability In The Java Runtime Environment Related Xml Data

Description: A vulnerability in the Java Runtime Environment related to the processing of XML data may allow unauthorized access to certain URL resources (such as some files and web pages) or a Denial of Service (DoS) condition to be created on the system running the JRE.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.1.36 Cve-2008-3106 - Security Vulnerability In The Java Runtime Environment Related To Xlm Data

Description: A vulnerability in the Java Runtime Environment with processing XML data may allow an untrusted applet or application that is downloaded from a website unauthorized access to certain URL resources (such as some files and web pages).For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.1.37 Cve-2008-3108 - A Security Vulnerability With The Processing Of Fonts In The Java Runtime

Description: A buffer overflow security vulnerability with the processing of fonts in the Java Runtime Environment (JRE) may allow an untrusted applet or application to elevate its privileges. For example, an untrusted applet may grant itself permissions to read and write local files or execute local applications that are accessible to the user running the untrusted applet.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.1.38 Cve-2008-3109 - Security Vulnerability In The Java Runtime Environment Scripting Language

Description: A vulnerability in the Java Runtime Environment relating to scripting language support may allow an untrusted applet or application to elevate its privileges. For example, an untrusted applet may grant itself permissions to read and write local files or execute local applications that are accessible to the user running the untrusted applet.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.1.39 Cve-2008-3110 - Security Vulnerability In The Java Runtime Environment Scripting Language

Description: A vulnerability in the Java Runtime Environment relating to scripting language support may allow an untrusted applet to access information from another applet.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.1.40 Cve-2008-3257 - Security Vulnerability In Weblogic Plug-In For Apache (Wls V10)

Description: Recently, an exploit has been made public which may impact the availability, confidentiality, or integrity of WebLogic Server applications that use the Apache web server configured with the WebLogic plug-in for Apache. This vulnerability may be remotely exploitable without authentication (that is, it may be exploited over a network without the need for a username and password).

Severity: Critical

Rationale: Server Outage

17.1.41 Cve-2008-4008 - Security Vulnerability In Weblogic Plug-In For Apache

Description: This vulnerability may impact the availability, confidentiality, or integrity of WebLogic Server applications which use the Apache web server configured with the WebLogic plug-in for Apache. This vulnerability may be remotely exploitable without authentication, that is, it may be exploited over a network without the need for a username and password.

Severity: Critical

Rationale: Administration

17.1.42 Cve-2008-4010 - Elevation Of Privilege Vulnerability In Some Netui Tags (Wls V10)

Description: This vulnerability in some NetUI tags may allow an attacker to read unauthorized data. This may be exploited over a network.

Severity: Critical

Rationale: Administration

17.1.43 Cve-2008-4011 - Elevation Of Privileges For Some Applications (Wls V10.0)

Description: Under certain conditions, some applications in admin state may be made available to non admin users.

Severity: Critical

Rationale: Administration

17.1.44 Cve-2008-4013 - Protected Web Apps May Be Displayed Under Certain Conditions. (Wls V10)

Description: If you upgrade from Oracle WebLogic Server 8.1SP3 to a higher version and use auth-method as CLIENT-CERT, some web apps which were protected in Oracle WebLogic Server 8.1SP3 may be made available to an invalid user.

Severity: Critical

Rationale: Administration

17.1.45 Cve-2008-5457 - Security Vulnerability In Wls Plug-Ins For Apache, Sun, And Iis Web Server (Wls V10)

Description: This vulnerability may impact the availability, confidentiality or integrity of WebLogic Server applications, which use the Apache, Sun, or IIS web server configured with the WebLogic plug-in for Apache, Sun, or IIS, respectively. This vulnerability may be remotely exploitable without authentication, that is, it may be exploited over a network without the need for a username and password.

Severity: Critical

Rationale: Administration

17.1.46 Cve-2008-5460 - Information Disclosure Vulnerability In Jsp And Servlets (Wls V10)

Description: Certain circumstances may cause some information disclosure in WebLogic Server JSPs and servlets.

Severity: Critical

Rationale: Subsystem Outage

17.1.47 Cve-2008-5461 - Elevation Of Privilege Vulnerability In Oracle Weblogic Console

Description: This vulnerability in Oracle WebLogic Console may allow information disclosure and elevation of privileges. This may be exploited over a network.

Severity: Critical

Rationale: Subsystem Outage

17.1.48 Cve-2008-5462 - Elevation Of Privilege Vulnerability In Weblogic Portal (Wls V10)

Description: This vulnerability in WebLogic Portal may allow elevation of privileges. This may be exploited over a network.

Severity: Critical

Rationale: Administration

17.1.49 Cve-2009-0217 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle JRockit R27.6.3 JRE/JDK 1.6.0_11. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.1.50 Cve-2009-0217 - Critical Patch Update Notice (Wls V10.0)

Description: Oracle has released Critical Patch Updates for July 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 10.0. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Server Outage

17.1.51 Cve-2009-1002 - Elevation Of Privilege Vulnerability In Weblogic Server (Wls V10)

Description: This vulnerability in WebLogic Server may allow elevation of privileges. This may be exploited over a network.

Severity: Critical

Rationale: Administration

17.1.52 Cve-2009-1003 - Source Code Access Vulnerability In Web Pages, Weblogic Server (Wls V10)

Description: This vulnerability in WebLogic Server may allow access to source code of web pages. This may be exploited over a network.

Severity: Critical

Rationale: Administration

17.1.53 Cve-2009-1012 - Security Vulnerability In Weblogic Plug-In For Apache Web Server

Description: This vulnerability may impact the availability, confidentiality, or integrity of WebLogic Server applications, which use the Apache, Sun, or IIS web server configured with the WebLogic plug-in for Apache, Sun, or IIS servers, respectively. This vulnerability may be remotely exploitable without authentication. That is. it may be exploited over a network without the need for a username and password.

Severity: Critical

Rationale: Administration

17.1.54 Cve-2009-1016 - Security Vulnerability In Oracle Weblogic Server Plug-Ins For Apache, Sun, And Iis Servers

Description: This vulnerability may impact the availability, confidentiality, or integrity of Oracle WebLogic Server applications, which use the Apache, Sun, or IIS web server configured with the WebLogic Server plug-ins for Apache, Sun, or IIS servers, respectively.

Severity: Critical

Rationale: Administration

17.1.55 Cve-2009-1094 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for July 2009 that provide corrective action for potential security vulnerabilities for Oracle JRockit R27.6.3 and earlier JRE and JDK 6, R27.6.3 and earlier JRE and JDK 5.0, R27.6.3 and earlier SDK and JRE 1.4.2. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.1.56 Cve-2009-1974 - Critical Patch Update Notice (Wls V10.0)

Description: Oracle has released Critical Patch Updates for July 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 10.0. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Server Outage

17.1.57 Cve-2009-2002 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Portal 10.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.1.58 Cve-2009-2625 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle JRockit 1.5.0_19 and 1.6.0_14.Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.1.59 Cve-2009-3396 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.0, 9.1, and 9.2. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Server Outage

17.1.60 Cve-2009-3396 - Critical Patch Update Notice (Wls V10.0)

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 10.0. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Server Outage

17.1.61 Cve-2009-3403 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle JRockit 1.6.0_14, 1.5.0_19 and 1.4.2_21. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.1.62 Cve-2009-3555 - Critical Patch Update Notice (Wls V10.0)

Description: Oracle has released a Critical Patch Update that provides corrective action for a potential security vulnerability for Oracle WebLogic Server 10.0. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Development

17.1.63 Cve-2010-0068 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.1.64 Cve-2010-0068 - Critical Patch Update Notice (Wls V10.0)

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 10.0. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Development

17.1.65 Cve-2010-0069 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.1.66 Cve-2010-0069 - Critical Patch Update Notice (Wls V10.0)

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 10.0. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Development

17.1.67 Cve-2010-0073 - Critical Patch Update Notice (Wls V10.0)

Description: Oracle has released a Critical Patch Update that provides corrective action for a potential security vulnerability for Oracle WebLogic Server 10.0. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Development

17.1.68 Cve-2010-0074 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.1.69 Cve-2010-0074 - Critical Patch Update Notice (Wls V10.0)

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 10.0. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Development

17.1.70 Cve-2010-0078 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.1.71 Cve-2010-0078 - Critical Patch Update Notice (Wls V10.0)

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 10.0. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Development

17.1.72 Cve-2010-0079 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle JRockit 1.6.0_14, 1.5.0_19 and 1.4.2_21. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.1.73 Cve-2010-0849 - Critical Patch Update Notice

Description: Oracle has released a Critical Patch Update that provides corrective action for a potential security vulnerability for Oracle JRockit R27.6.6: JRE/JDK 1.4.2, 5 and 6; R28.0.0, JRE/JDK 5 and 6. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.1.74 Cve-2010-2375 - Critical Patch Update Notice (Wls V10.0)

Description: Oracle has released a Critical Patch Update that provides corrective action for a potential security vulnerability for Oracle WebLogic Server 10.0. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Development

17.1.75 Cacerts Do Not Work With Demotrust.Jks And Demoidentity.Jks

Description: Bad Certificate Error is thrown during NodeManager startup.Workaround or Apply patch: 1. Use JDK 1.6.0_12 or lower. 2. Copy cacerts from WL_HOME/server/lib directory to JDK_HOME/jre/lib/security/ Installers, updates, patches and more information are available at support.oracle.com.

Severity: Warning

Rationale: Not Complying with Specifications

17.1.76 Cacerts Do Not Work With Demotrust.Jks And Demoidentity.Jks (Wls V10.0.0 And 10.0.1, Upgrade)

Description: Bad Certificate Error is thrown during NodeManager startup.Example from the Admin Server:####<Apr 9, 2009 12:55:33 PM EDT> <Debug> <SecuritySSL> <xxxxx-us><AdminServer> <[ACTIVE] ExecuteThread: '2' for queue:'weblogic.kernel.Default (self-tuning)'> <<Oracle WebLogic Server Kernel>> <> <> <1239296133359>...Workaround or Apply patch: - - - - - - - - - - - - - 1. Use JDK 1.6.0_12 or lower. 2. Copy cacerts from WL_HOME/server/lib directory to JDK_HOME/jre/lib/security/This problem, described in 8422724, has been fixed in Oracle WebLogic Server 10.3 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.1.77 Cacerts Do Not Work With Demotrust.Jks And Demoidentity.Jks (Wls V10.0.2, Upgrade)

Description: Bad Certificate Error is thrown during NodeManager startup.Example from the Admin Server:####<Apr 9, 2009 12:55:33 PM EDT> <Debug> <SecuritySSL> <xxxxx-us><AdminServer> <[ACTIVE] ExecuteThread: '2' for queue:'weblogic.kernel.Default (self-tuning)'> <<Oracle WebLogic Server Kernel>> <> <> <1239296133359><BEA-000000> <Failed to load server trusted CAs...Workaround or Apply patch: - - - - - - - - - - - - - 1. Use JDK 1.6.0_12 or lower. 2. Copy cacerts from WL_HOME/server/lib directory to JDK_HOME/jre/lib/security/This problem,

described in 8896127, has been fixed in Oracle WebLogic Server 10.3 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.1.78 Callbacks Do Not Work With Bumpy Case Packages

Description: Web Services that define a Callback interface with a mixed-case package name will fail to compile with JWSC.

Severity: Minor Warning

Rationale: Development

17.1.79 Calls To Isconnected Method On Ssllayeredsocket Always Result In Socket Not Connected

Description: Calls to isConnected on SSLLayeredSocket result in a "socket not connected" indication.

Severity: Warning

Rationale: Non-User Viewable Errors

17.1.80 Calls To Isconnected Method On Ssllayeredsocket Always Result In Socket Not Connected (Upgrade)

Description: Calls to isConnected on SSLLayeredSocket result in a "socket not connected" indication.This problem, described in Oracle Bug 8187246, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Non-User Viewable Errors

17.1.81 Cannot Deploy Persistence Unit With Hibernate As Provider

Description: When trying to deploy an application, Hibernate is throwing an exception "it can't use jboss-archive-browser into a compressed archive". Oracle recommends upgrading the jboss-archive-browsing.jar to solve the problem.

Severity: Minor Warning

Rationale: Development

17.1.82 Cannot Locate Bundle For Class Weblogic.I18N.Logging.Loggingtextlocalizer

Description: In the Administration Console, if you change the log level for stdout from "Notify" (default) to "Trace," and then change the log level back to "Notify," the following exception occurs during activation:<AdminServer> <[STANDBY] ExecuteThread: '5' for queue:'weblogic.kernel.Default (self-tuning)'> <<WLS Kernel>> <> <> <1186585039843><BEA-141190> <The commit phase of the configuration update failed with an exception:java.util.MissingResourceException: Can't locate bundle for class 'weblogic.i18n.logging.LoggingTextLocalizer' at weblogic.i18ntools.L10nLookup.getLocalizer(L10nLookup.java:392) ...As a workaround, you can manually edit the config.xml file.

Severity: Warning

Rationale: User Viewable Errors

17.1.83 Cannot Locate Bundle For Class Weblogic.I18N.Logging.Loggingtextlocalizer (Upgrade)

Description: In the Administration Console, if you change the log level for stdout from "Notify" (default) to "Trace," and then change the log level back to "Notify" you may see "[STANDBY] ... The commit phase of the configuration update failed with an exception:java.util.MissingResourceException: Can't locate bundle for class 'weblogic.i18n.logging.LoggingTextLocalizer' at weblogic.i18ntools.L10nLookup.getLocalizer(L10nLookup.java:392) ...As a workaround, you can manually edit the config.xml file. This problem, described in Oracle Bug 8167473, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: User Viewable Errors

17.1.84 Cannot Set Weblogicpluginenabled Attribute Of Clustermbean From Admin Console

Description: In the Oracle WebLogic Server Administration Console, it is not possible to set the WeblogicPluginEnabled attribute of ClusterMBean.

Severity: Minor Warning

Rationale: Administration

17.1.85 Cannot Specify The Socket Timeout For Ssl Connections Using T3S

Description: Cannot specify the socket connect timeout while creating a new SSL socket. A specified timeout can provide a faster bailout if the remote server is not available, rather than relying on the default operating system timeout value.

Severity: Warning

Rationale: Administration

17.1.86 Cannot Specify The Socket Timeout For Ssl Connections Using T3S (Upgrade)

Description: Cannot specify the socket connect timeout while creating a new SSL socket. A specified timeout can provide a faster bailout if the remote server is not available, rather than relying on the default operating system timeout value.This problem, described in Oracle Bug 8192393, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.1.87 Cannot View Request Uri Of Threads With Use81-Style-Execute-Queues

Description: When the <use81-style-execute-queues> element is set to true in config.xml, the HTTP URI request is not displayed properly on the Server - Monitoring - Threads page of the Administration Console.When you configure Oracle WebLogic Server to use the 8.1 style execute queues such as:<server> <name>AdminServer</name> <use81-style-execute-queues>true</use81-style-execute-queues> <listen-address/></server>When you monitor the threads in the

console, the current request does not show the HTTP URI, but something like:weblogic.work.ExecuteRequestAdapter@124a4bc

Severity: Warning

Rationale: Administration

17.1.88 Cannot View Request Uri Of Threads With Use81-Style-Execute-Queues. (Upgrade)

Description: When the <use81-style-execute-queues> element is set to true in config.xml, the HTTP URI request is not displayed properly on the Server>Monitoring>Threads page of the Administration Console.If Oracle WebLogic Server is configured to use the 8.1-style execute queues such as -<server> <name>AdminServer</name> <use81-style-execute-queues>true</use81-style-execute-queues> <listen-address/></server>- the current request does not show the HTTP URI when monitoring the threads in the console. Instead, a string such as the following is seen:weblogic.work.ExecuteRequestAdapter@124a4bcThis problem, described in Oracle Bug 8160163, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.1.89 Chainentityresolver Exception While Calling A Webservice (Wls V10.0)

Description: While invoking a Web Services Application based on Apache AXIS version 1.3, the following exception is logged:[[ACTIVE] ExecuteThread: '0' for queue:'weblogic.kernel.Default (self-tuning)'] DEBUG [TXID:]org.apache.axis.utils.XMLUtils - Failed to set EntityResolver on DocumentBuilderjava.lang.NullPointerException at weblogic.xml.jaxp.ChainingEntityResolver.popEntityResolver(ChainingEntityResolver.java:61) at weblogic.xml.jaxp.RegistryDocumentBuilder.setEntityResolver(RegistryDocumentBuilder.java:169) ...

Severity: Minor Warning

Rationale: User Viewable Errors

17.1.90 Changes In Dst Definitions Cause Issues With Basic Date Handling In Oracle Jrockit Jdk

Description: The recent change to the definition of US timezones to remove Daylight Savings Time (DST) awareness has broken basic functionality in date handling in multiple vendor JVMs, including Oracle JRockit 1.5.0_08. This issue only affects sites using three-letter abbreviations of DST times zones denotations, which have been deprecated, and any affected JVM.The DateFormat parser uses the contents of String zoneStrings[][] in class DateFormatSymbols to identify the timezone based on the zone value in the input date string.The bug will only have an impact if and only if the application is using the deprecated denotation of three-letter abbreviations for US timezones (for example, EST, MST, or HST).

Severity: Warning

Rationale: Not Complying with Specifications

17.1.91 Changes In Dst Definitions Cause Issues With Basic Date Handling In Oracle Jrockit Jdk

Description: The recent change to the definition of US timezones to remove Daylight Savings Time (DST) awareness has broken basic functionality in date handling in multiple vendor JVMs, including Oracle JRockit 1.4.2_12. This issue affects sites using the three letter abbreviations for the deprecated DST timezone denotations, when using any affected JVM.The DateFormat parser uses the contents of String zoneStrings[][] in class DateFormatSymbols to identify the timezone based on the zone value in the input date string. For example, the zoneStrings[][] array defines "EST" before "America/New_York" and so sets the timezone for the parser to the EST zone, which is now unaware of DST.

Severity: Warning

Rationale: Not Complying with Specifications

17.1.92 Character Encoding Discrepencies Between Environments

Description: When using UTF-8 encoding and retrieving the data through a JSP from the database in production, you may get incorrect values or characters.Resolution: 1.Use -Dfile.encoding options in JVM arguments.2.Use pageEncoding in JSP page directive:<%@ page contentType="text/html; charset=UTF-8" pageEncoding="UTF-8" %>3.Use charset in HTML Meta tag:<meta http-equiv="content-type" content="text/html; charset=UTF-8" />4.jsp-config directive in the deployment descriptor:<jsp-config><jsp-property-group><url-pattern>*.jsp</url-pattern><page-encoding>UTF-8</page-encoding></jsp-property-group></jsp-config>

Severity: Minor Warning

Rationale: Subsystem Outage

17.1.93 Charset Attribute Of Deployed Html Does Not Work

Description: The servlet container appends charset=ISO-8859-1 to the HTTP Header contentType in the response for non-JSP pages with any charset contents. This results in improper display of multibyte characters.

Severity: Warning

Rationale: User Viewable Errors

17.1.94 Charset Attribute Of Deployed Html Does Not Work (Upgrade)

Description: The servlet container appends charset=ISO-8859-1 to the HTTP Header contentType in the response for non-JSP pages with any charset contents. This results in improper display of multibyte characters.This problem, described in Oracle Bug 8122750, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 1.

Severity: Minor Warning

Rationale: User Viewable Errors

17.1.95 Classcastexception Involving Custom Jndi Object And Cluster Synchronization (Wls V10.0)

Description: When you create a custom object and bind the object to the JNDI tree of a managed server of a two node cluster, the server log in the managed server will contain a ClassCastException.

Severity: Warning

Rationale: Performance

17.1.96 Classcastexception Involving Custom Jndi Object And Cluster Synchronization (Wls V10.0, Upgrade)

Description: When you create a custom object and bind the object to the JNDI tree of a managed server of a two node cluster, you encounter the following issue.After the custom object is bound, the server log in the managed server shows a ClassCastException.This problem, described in Oracle Bug 8141074, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Performance

17.1.97 Cluster Has No Frontendhost Server Specified

Description: A cluster has the Oracle WebLogic Plugin enabled, but the FrontEndHost server setting has not been specified. Oracle WebLogic Server uses this setting to specify the host for HTTP responses. If no FrontEndHost server has been specified, Oracle WebLogic Server uses the hostname of the server that processed the request.

Severity: Warning

Rationale: Non-User Viewable Errors

17.1.98 Compaction(S) Aborted Due To Counters Do Not Reset Between Each Garbage Collection

Description: Compaction of objects is the process of moving objects closer to each other in the heap, thus reducing the fragmentation and making object allocation easier for the JVM. Oracle JRockit compacts a part of the heap at each garbage collection (or old collection, if the garbage collector is generational).It has been observed in Oracle JRockit releases R27.3.1 and R27.4.0 that the compaction is being aborted when it should not be aborted due to the counter not being set to 0 between Garbage Collections.In some cases, the counter will continue to increase until it grows too large, leading to an aborted compaction. Since it is not set to 0, all the following Garbage Collections will be aborted as well.

Severity: Warning

Rationale: Performance

17.1.99 Connection Pool Performance May Be Degraded Due To The Test Settings That Are Specified

Description: A connection pool has been set up to perform all of the following tests:* TestOnCreate* TestOnReserve* TestOnReleaseAs a result of enabling all three of these

settings, the connection will be tested when it is retrieved from the pool and then again when it is put back into the pool. This can lead to performance issues in JDBC access code.

Severity: Minor Warning

Rationale: Performance

17.1.100 Console Shows Wrong Config Values If Production Mode Is Enabled/Disabled From Command Line

Description: When Production Mode is enabled or disabled with the command line option "-Dweblogic.ProductionModeEnabled=[true

Severity: false]" but the setting does not agree with the config.xml "ProductionMode" setting, the Adminstration Console may show incorrect values for some configuration options. This can occur for any configuration options for which the default values for production mode differ from the default values for development mode.Note: Command line overrides are not persisted in config.xml. The Administration Console shows the configuration attribute values and defaults that correspond to the persisted version in the config.xml file.

Rationale: Warning

17.1.101 Consumers Not Recreated After Server Is Rebooted

Description: When a Message Driven Bean (MDB) is deployed on a multiserver domain and is listening on a distributed queue, and the MDB is configured to connect to all of the distributed queue members. However, if a remote distributed queue member server is restarted, the deployed MDB server does not reconnect with the remote distributed queue member server.

Severity: Warning

Rationale: Subsystem Outage

17.1.102 Crashes In Conjunction With A Native Library

Description: If you are using Oracle JRockit in conjunction with a native library that relies on OS signals you may experience crashes due to a signal handling conflict between Oracle JRockit and the native library.Dump stack matches known issue:Thread Stack Trace: at pthread_kill+62()@0xb75c00ee at ptSendSignal +34()@0xb71aedc6 at trapiConvertToDeferredSigsegv+199()@0xb719d207 at trapiSigSegvHandler+40()@0xb719d23c at xehInterpretSavedSigaction +219(amqxerrx.c)@0xb72f276b at xehExceptionHandler+543()@0xb72f2b3f at __libc_sigaction+272()@0xb75c2f80Oracle Engineering found this conflict using IBM's MQSeries native drivers, and it may be present in other libraries that rely on native code.

Severity: Critical

Rationale: Server Outage

17.1.103 Datasource Test Frequency In Seconds Does Not Work After A Shutdown And Restart. (Upgrade)

Description: The shutdown of a pool also kills its asynchronous connection testing process. When the pool is restarted, the asynchronous testing job does not restart, and the DataSource cannot detect database failures by test frequency until Oracle

WebLogic Server is rebooted. This issue no longer occurs, as asynchronous testing is always restarted when the pool is restarted.This problem, described in Oracle Bug 8195854, has been fixed in Oracle WebLogic Server 10.3.

Severity: Minor Warning

Rationale: Administration

17.1.104 Datasource Test Frequency Seconds Does Not Work After Doing Shutdown And Start

Description: The shutdown of a pool also kills its asynchronous connection testing process. When the pool is restarted, the asynchronous testing job does not restart, and the DataSource cannot detect database failures by test frequency until Oracle WebLogic Server is rebooted. This issue no longer happens, as asynchronous testing is always restarted when the pool is restarted.

Severity: Minor Warning

Rationale: Administration

17.1.105 Deactivate Synchronization During The Registration Of Managed Servers And Reconnect

Description: Starting up a large cluster can be very slow, because establishing the JMX connection can be a fairly heavy operation.

Severity: Warning

Rationale: Administration

17.1.106 Deactivate Synchronization During The Registration Of Managed Servers And Reconnect (Upgrade)

Description: Starting up a large cluster can be very slow, because establishing the JMX connection can be a fairly heavy operation.This problem, described in Oracle Bug 8138357, has been fixed in Oracle WebLogic Server 10.3.

Severity: Minor Warning

Rationale: Administration

17.1.107 Deadlock In Feconnection.Close And Feconnectionruntimedelegate.Getsessionscurren (Wls V10)

Description: A deadlock occurs in FEConnection and FEConnectionRuntimeDelegate class when sending a message to JMS Server using a thin client.The following is the thread stack from the deadlock:"[STANDBY] ExecuteThread: '5' for queue: 'weblogic.kernel.Default(self-tuning)'": at weblogic.management.runtime.RuntimeMBeanDelegate.unregisterChildren(RuntimeMBeanDelegate.java:336) - waiting to lock <0x03ae0028> (a weblogic.jms.frontend.FEConnectionRuntimeDelegate) ...

Severity: Warning

Rationale: Administration

17.1.108 Deadlock In Weblogic.Jms.Client.Wlconnectionimpl.Processreconnecttimer

Description: When using Oracle WebLogic Server 10.0 and JMS operations, a deadlock occurs when trying to reconnect with an Oracle WebLogic Server 8.1 SP5 server that has gone down.Found one Java-level deadlock:'weblogic.timers.TimerThread': waiting to lock monitor 0x00000001012cdbe0 (object 0xffffffff23111248, a java.lang.Object), which is held by '[ACTIVE] ExecuteThread: '36' for queue: 'weblogic.kernel.Default (self-tuning)'"[ACTIVE] ExecuteThread: '36' for queue: 'weblogic.kernel.Default (self-tuning)": waiting to lock monitor 0x00000001002d26f8 (object 0xffffffff13ca1368, a weblogic.timers.internal.TimerThread), which is held by 'weblogic.timers.TimerThread'

Severity: Critical

Rationale: Subsystem Outage

17.1.109 Deadlock In Weblogic.Jms.Client.Wlconnectionimpl.Processreconnecttimer (Upgrade)

Description: When using Oracle WebLogic Server 10.0 and JMS operations, a deadlock occurs when trying to reconnect with an Oracle WebLogic Server 8.1 SP5 server that has gone down. For example:Found one Java-level deadlock:'weblogic.timers.TimerThread': waiting to lock monitor 0x00000001012cdbe0 (object 0xffffffff23111248, a java.lang.Object), which is held by '[ACTIVE] ExecuteThread: '36' for queue: 'weblogic.kernel.Default (self-tuning)'"[ACTIVE] ExecuteThread: '36' for queue: 'weblogic.kernel.Default (self-tuning)": waiting to lock monitor 0x00000001002d26f8 (object 0xffffffff13ca1368, a weblogic.timers.internal.TimerThread), which is held by 'weblogic.timers.TimerThread'This problem, described in Oracle Bug 8135972, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Subsystem Outage

17.1.110 Deadlock Occurs In Oracle Weblogic Server (Wls V10.0)

Description: Java level deadlock between weblogic.deployment.jms.JMSSessionPoolTester and weblogic.deployment.jms.JMSSessionPool reveal in Oracle WebLogic Server Thread dump.

Severity: Critical

Rationale: Server Outage

17.1.111 Deadlock Occurs In Oracle Weblogic Server (Wls V10.0, Upgrade)

Description: Java level deadlock between weblogic.deployment.jms.JMSSessionPoolTester and weblogic.deployment.jms.JMSSessionPool reveal in Oracle WebLogic Server Thread dump.

Severity: Minor Warning

Rationale: Server Outage

17.1.112 Delay Can Occur When A Transaction Commits Using Usertransaction With Jms

Description: A delay can occur when a transaction commits using UserTransaction with JMS when the system is under load. When this happens, Oracle WebLogic Server may throw a java.rmi.server.ServerNotActiveException at getClientEndPoint() in the ServerHelper class. This can cause a stop startCommit() process in the SubCoordinatorImpl class, and the commit is delayed until after the JTA timeout value.

Severity: Warning

Rationale: Performance

17.1.113 Deleting Modified Workspace Copy Of Library Module .Jsp Doesn'T Revert To Library Version

Description: If a .jsp (for instance, a framework skeleton .jsp) is copied into the workspace, modified, then deleted, the .jsp does not revert to the library version of the .jsp, and the modifications are not removed.For example, if you:1) Copy a library module version of a .jsp to the workspace.2) Modify the .jsp.3) Publish and view a desktop using that .jsp.4) Delete the .jsp.5) Republish and view the desktop again. Changes made to copy are still visible.6) Run Project -> clean.7) Republish and view the desktop again. The changes made to the copy are still visible.

Severity: Minor Warning

Rationale: Administration

17.1.114 Diagnostic Image File Growing Rapidly. (Wls V10.0)

Description: When JDBC profiling is enabled, it periodically dumps profiling information into the diagnostic store. Enabling it for an extended time can cause the diagnostic store to grow.

Severity: Warning

Rationale: Performance

17.1.115 Dweblogic.Management.Nologsystemproperties=True Has No Effect

Description: In Oracle WebLogic Server 8.1 Maintenance Pack 5, it was possible to disable the writing of system properties to the Oracle WebLogic Server log file by using the -Dweblogic.management.noLogSystemProperties=true parameter.However, after upgrading to Oracle WebLogic Server 9.x, this setting no longer has any effect.

Severity: Minor Warning

Rationale: Performance

17.1.116 Dynamic Wsdl Host Address Incorrect When Deployed In A Cluster

Description: An incorrect dynamic Web Service Definition Language (WSDL) location address is generated when a Web service is deployed on a cluster with multiple front-end hosts and ports. A new property, weblogic.wsee.useRequestHost, has been introduced in Oracle WebLogic Server 9.2.1 that allows generation of the WSDL location address either from the host header or by following the topology design.

Severity: Minor Warning

Rationale: Administration

17.1.117 Ejb 3.0 Resource Injection Exception In Interceptor

Description: When trying to inject an EJB resource into an interceptor using annotation, you may receive a runtime error:@EJB private LocalEjb localEjb;The exception received is the following:Runtime exception : javax.ejb.EJBException: nested exception is:java.lang.InstantiationException: [EJB:011128]Error creating an instance of the EJB 'TestFacadeImpl':com.bea.core.repackaged.springframework.beans.factory.BeanCreationException:Error creating bean with name'com.company.vdds.server.facade.TestInterceptor_42to9f_Impl': Initialization of bean failed; nested exception is java.lang.UnsupportedOperationException:Cannot inject value of class 'class $Proxy258' into privatecom.company.vdds.server.facade.LocalEjbcom.company.vdds.server.facade.TestInterceptor.localEjb

Severity: Minor Warning

Rationale: Development

17.1.118 Ejb 3.0 Resource Injection Exception In Interceptor (Upgrade)

Description: When trying to inject an EJB resource into an interceptor using annotation, you may receive a runtime error:@EJB private LocalEjb localEjb;The exception received is the following:Runtime exception : javax.ejb.EJBException: nested exception is:java.lang.InstantiationException: [EJB:011128]Error creating an instance of the EJB 'TestFacadeImpl':com.bea.core.repackaged.springframework.beans.factory.BeanCreationException:Error creating bean with name...This problem, described in Oracle Bug 8116768, has been fixed in Oracle WebLogic Server 10.3

Severity: Minor Warning

Rationale: Development

17.1.119 Ejbhomequery Causes Nullpointerexception In Cachekey

Description: ejbHomeQuery causes NullPointerException in the EJB container.

Severity: Minor Warning

Rationale: Administration

17.1.120 Ejbhomequery Causes Nullpointerexception In Cachekey (Upgrade)

Description: ejbHomeQuery causes NullPointerException in the EJB container.This problem, described in Oracle Bug 8115318, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3.

Severity: Minor Warning

Rationale: Administration

17.1.121 End-Of-Support Announcement For Microsoft Windows 2000 Server

Description: As of June 30, 2005, Microsoft has announced the end of mainstream support for the following platforms:* Windows 2000 Server* Advanced Server*

Datacenter ServerOracle will continue supporting Oracle applications (for example Oracle JRockit on these platforms) at least through December 2006. A final notice of the end of support for Oracle JRockit on Windows 2000 will appear at least 12 months before the actual end of support.Note: Support for any Windows-specific issues must addressed by Microsoft via their extended support services.

Severity: Warning

Rationale: Not Complying with Specifications

17.1.122 End-Of-Support Announcement For Red Hat Enterprise Linux 2.1

Description: Oracle stopped supporting Red Hat Linux 2.1 on April 30, 2006.

Severity: Warning

Rationale: Not Complying with Specifications

17.1.123 Enhancement To Disable Passivation/Activation During Sfsb Replication In Cluster

Description: Enhancement to add deployment descriptor to turn off passivation/ activation during replication of Stateful Session Bean (SFSB) in cluster.A new flag <passivate-during-replication> is added to weblogic-ejb-jar.xml. This flag is part of <stateful-session-descriptor> as below:<!ELEMENT stateful-session-clustering (home-is-clusterable?, home-load-algorithm?, home-call-router-class-name?, use-serverside-stubs?, replication-type?, passivate-during-replication?)>Set the flag to 'false' to avoid passivation/activation during SFSB replication. The default value for the flag is 'true'.

Severity: Minor Warning

Rationale: Administration

17.1.124 Entity Bean Creation With Primary Key Of Sequence Generator Int Type Fails In A Global Tx

Description: When a new Entity bean has been created with a primary key ID of sequence generator int type, attempts to persist this bean as part of a global transaction will fail with a javax.ejb.EJBException if a nontransactional datasource is used.No issues will be encountered if the annotation is removed from the Primary Key value, or if the uid-string generator is used and the field type changed to String.

Severity: Minor Warning

Rationale: User Viewable Errors

17.1.125 Errors When Using Cached Remote Home Of New Redeployed Stateless Ejbs

Description: The issue exists in the following situation:Two domains.On domain1, business services implemented as Stateless EJBs are deployed.On domain2, other business services using those of domain1 are implemented.Business services on domain2 put Remote Home EJB object from domain1 into cache, so that domain2 does not have to lookup home objects needlessly.Unfortunately, when redeploying business services on domain1, services on domain2 do not work on the first call. They do work on the second call.

Severity: Warning

Rationale: Performance

17.1.126 Errors When Using Cached Remote Home Of New Redeployed Stateless Ejbs (Upgrade)

Description: The issue exists in the following situation:Two domains:On domain1, business services implemented as Stateless EJBs are deployed.On domain2, other business services using those of domain1 are implemented.Business services on domain2 put Remote Home EJB object from domain1 into cache, so that domain2 does not look up home objects needlessly.However, when redeploying business services on domain1, services on domain2 do not work on the first call. They do work on the second call.This problem, described in Oracle Bug 8156181, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Performance

17.1.127 Exceptions Occur When Viewing Persistence Units In Oracle Weblogic Server Administration Console.

Description: Exceptions occur in the Oracle WebLogic Server 10.0.x Administration Console when viewing persistence units in any application. After this occurs, no persistence units are displayed in the console.The following exception is thrown:<Error> <Console> <BEA-240003> <Console encountered the following error java.lang.NullPointerExceptionAt weblogic.deploy.api.spi.config.DeploymentConfigurationImpl.getRootTag(DeploymentConfigurationImpl.java:1285)at weblogic.deploy.api.spi.config.BasicDConfigBeanRoot.getDConfigBean(BasicDConfigBeanRoot.java:131)

Severity: Minor Warning

Rationale: Administration

17.1.128 Excessive Logging Of Ejb Exceptions

Description: Per the EJB specification, any business exception thrown from business methods needs to be handled at the client end. That is, the business exception propagates to the client end without any intervention from the server.However, when implementing a Web service using an EJB, with a business exception thrown from the exposed methods, the business exception thrown is propagated to the client; but an exception stack trace is also getting generated in the server log.This results in unneccessary growth of server logs.NOTE: The following flag suppresses the error message from the logs:-Dweblogic.wsee.component.exception=false

Severity: Minor Warning

Rationale: Administration

17.1.129 Excessive Logging Of Ejb Exceptions (Upgrade)

Description: Per the EJB specification, any business exception thrown from business methods needs to be handled at the client end (that is, the business exception propagates to the client end without any intervention from the server).However, when implementing a Web service using an EJB, with a business exception thrown from the exposed methods, the business exception thrown is propagated to the client; but, an exception stack trace is also getting generated in the server log.This results in unneccessary growth of server logs.NOTE: The following flag suppresses the error

message from the logs:-Dweblogic.wsee.component.exception=falseThis problem, described in Oracle Bug 8182695, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.1.130 Failure In A Class Preprocessing Recursive Calls In Oracle Jrockit R27.X

Description: In Oracle JRockit R27.1, the class bytes preprocessing facility was changed to allow for recursive preprocessing. This meant that a class preprocessor instance that was currently doing class preprocessing and through this caused a new class to be loaded would be recursively called with the new class bytes. This caused failures in some existing preprocessor implementations that relied on the old behavior of JRockit R27.1. In Oracle JRockit R27.5, this has been reverted. A thread doing class preprocessing will now silently refuse to preprocess any types created by executing the preprocessor itself.For example, in Oracle SOA Manager (ALSM), the error "Nanoagents not loading" occurs when used with Oracle JRockit R27.3.1.

Severity: Warning

Rationale: Subsystem Outage

17.1.131 For Oracle Weblogic Server 10.0, Single Sign On (Sso) Fails With Sun Jdk Less Than 1.5.0_8

Description: For Oracle WebLogic Server 10.0 with a Sun JDK version less than 1.5.0_08, if you use the JDK "ktab" command to generate a "keytab" file, the Single Sign On (SSO) fails with an "unsupported algorithm" exception.

Severity: Minor Warning

Rationale: Development

17.1.132 Foreign Jndi Link Causes Server Jndi Tree To Be Incorrectly Displayed In Administration Console. (Upgrade)

Description: If a configuration contains foreign JNDI links, the Oracle WebLogic Server Administration Console fails to display the JNDI tree. There are no exceptions, and the Console displays a blank page. This makes it impossible to browse the JNDI tree for debugging purposes or to administer the JNDI security policies.This problem, described in Oracle Bug 8096067, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.1.133 Foreign Jndi Link Causes The Server Jndi Tree To Be Incorrectly Displayed In Administration Console

Description: If a configuration contains foreign JNDI links, the Oracle WebLogic Server Administration Console fails to display the JNDI tree. There are no exceptions, and the Console displays a blank page. This makes it impossible to browse the JNDI tree for debugging purposes or to administrate the JNDI security policies.

Severity: Minor Warning

Rationale: Administration

17.1.134 Foreign-Connection-Factory Credentials Are Not Taken To Account If Provider-Url Specified

Description: JMS proxy using local foreign JMS server configuration with credentials given is not able to connect to the remote system.

Severity: Warning

Rationale: Subsystem Outage

17.1.135 Getting 'Nullpointerexception' When Running The Servlet As A Beehive Control

Description: When you insert the control manually, you get a 'nullPointerException' when running the servlet.In Oracle Workshop for WebLogic 10.0 there is no direct procedure to call a control from a Java class, but there are the workarounds available. See the Remedy section.

Severity: Minor Warning

Rationale: Development

17.1.136 Getting Unsatisfiedlinkerror: No Wlenv In Java.Library.Path On Linux

Description: Oracle WebLogic Server 10 on Linux and using CGIServlet is getting following error:<HTTP> <BEA-101017> <[weblogic.servlet.internal.WebAppServletContext@1026c8d - appName: 'itcon_app', name: 'itcon_app', context-path: ''] Root cause of ServletException.java.lang.UnsatisfiedLinkError: no wlenv in java.library.pathat java.lang.ClassLoader.loadLibrary(Ljava.lang.Class;Ljava.lang.String;Z)V (Unknown Source)at java.lang.Runtime.loadLibrary0(Runtime.java:822)at java.lang.System.loadLibrary(Ljava.lang.String;)V(UnknownSource)at weblogic.servlet.Env.<clinit>(Env.java:16)at weblogic.servlet.CGIServlet.init(CGIServlet.java:72)Truncated. see log file for complete stacktrace

Severity: Minor Warning

Rationale: Administration

17.1.137 Global Multicast Address Has Cluster Jndi Replication Issues

Description: Using global multicast addresses between 230.0.0.1 and 239.192.0.0 causes cluster issues. For example, the JMS destination may not replicate to all members of the cluster although the JNDINameReplicated attribute is set to "true."

Severity: Warning

Rationale: Administration

17.1.138 Group Circular Reference In External Authenticator Causes Ldap To Hang

Description: By default, Oracle WebLogic Server does not check for Group circularity for any externally configured LDAP Authenticators (iPlanet, Active Directory, Novell, Open LDAP, etc.).Circular reference:Group A is a member of Group BGroup B is a member of Group AWhen a group circularity exists in the backend LDAP, so many

LDAP connections are created (due to the backend LDAP group having itself as a member), that a server crash can result.

Severity: Minor Warning

Rationale: Subsystem Outage

17.1.139 Http Head Request For Web Service Wsdl Failed With Http 404 Error

Description: When using HTTP HEAD requests against http://<host>:<port>/WebApp/WebService?WSDL (to determine if service is available), it returns HTTP 404 error in Oracle WebLogic Server 10.0.The Web service can be verified as available via telnet GET or by accessing the Web Services Definition Language (WSDL) in a browser.

Severity: Minor Warning

Rationale: Development

17.1.140 Http Head Request For Web Service Wsdl Failed With Http 404 Error (Upgrade)

Description: When using HTTP HEAD requests against http://<host>:<port>/WebApp/WebService?WSDL (to determine if service is available), it returns HTTP 404 error in Oracle WebLogic Server 10.0.The Web service is verified to be available via telnet GET or by accessing the Web Service Definition Language (WSDL) in a browser.This problem, described in Oracle Bug 8160606, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Development

17.1.141 Http Head Request Throws Servletexception (Wls V10)

Description: If a servlet calls RequestDispatcher.forward(), the following exception is thrown for HEAD request:javax.servlet.ServletException: Original response not available

Severity: Warning

Rationale: Administration

17.1.142 Http Head Request Throws Servletexception (Wls V10, Upgrade)

Description: If a servlet calls RequestDispatcher.forward(), the following exception is thrown for HEAD request:javax.servlet.ServletException: Original response not availableThis problem, described in Oracle Bug 8103455, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Administration

17.1.143 Http Post Method Can Be Tuned Via Maxpostsize To Harden Security

Description: A denial-of-service attack is a malicious attempt to overload a server by sending more requests than it can handle, preventing access to a service. Attackers may overload the server by sending huge amounts of data in an HTTP POST method. The client can get an HTTP error code 413 (Request Entity Too Large) or the connection may be broken.Prevent this type of attack by setting the MaxPostSize parameter. This limits the number of bytes of data that can be received in a POST from

a single request. (By default, the value for MaxPostSize is -1, i.e. unlimited.) If an attacker sends an HTTP POST that exceeds the limit you specify, it triggers a MaxPostSizeExceeded exception and the server logs a "POST size exceeded the parameter MaxPostSize" message.

Severity: Critical

Rationale: Server Outage

17.1.144 Handlerpipe In Jax-Ws 2.0.1 Ri Bundled With Oracle Weblogic Server 10.0 Is Not Thread Safe

Description: HandlerPipe in JAX-WS 2.0.1 is not thread safe in Oracle WebLogic Server 10.0. A NullPointerException occurs when the JAX-WS handler is used. Below is an example of the exception stack trace:java.lang.NullPointerException at com.sun.xml.ws.handler.HandlerPipe.isHandleFalse(HandlerPipe.java:181) at com.sun.xml.ws.handler.HandlerPipe.process(HandlerPipe.java:109) at com.sun.xml.ws.handler.HandlerPipe.process(HandlerPipe.java:107) at weblogic.wsee.jaxws.MonitoringPipe.process(MonitoringPipe.java:98)

Severity: Warning

Rationale: Administration

17.1.145 Hibernate And Ehcache Cache Locking Problem With Multiple Managed Servers On Same Server

Description: When Hibernate and ehcache are used with Oracle WebLogic Server, the ehcache component writes cached objects to the file system defined by the property java.io.tmpDir. This, in itself, is not an issue. However, when there are two or more managed servers running on each physical server, these managed servers write to the same directory in the file system using the same file names. Consequently, the servers are sharing resources that require explicit locks in order to modify the files, which can result in a deadlock condition.

Severity: Critical

Rationale: Administration

17.1.146 Httpproxyservlet Keeps Reading Response From Backend After Client Closes Connection (Upgrade)

Description: When using HttpProxyServlet in Oracle WebLogic Server as the Reversed Proxy Server (RPS), the socket is to be closed when the browser is closed or navigated to some other site. However, the connection is found to be kept alive, and it keeps reading from the socket. And it will take a long time to respond to a new request. Finally, it results in the server hanging.thread dumps:"ExecuteThread: '48' for queue: 'weblogic.kernel.Default'" daemon prio=5 tid=0x24d488c0 nid=0xa80 runnable [26cef000..26cefdb0] at java.net.SocketInputStream.socketRead0(Native Method)...Oracle Bug 8118037 has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Administration

17.1.147 Httpservletrequest.Getremoteuser() Returns Null

Description: The request.getRemoteUser() call returns null.Workaround: Use request.getHeader('REMOTE_USER') to get the remote user.

Severity: Minor Warning

Rationale: Development

17.1.148 Httpservletrequest.Getremoteuser() Returns Null (Upgrade)

Description: The request.getRemoteUser() call returns null.Workaround: Use request.getHeader('REMOTE_USER') to get the remote user.This problem, described in Oracle Bug 8147527, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Development

17.1.149 Ibm Jdk 64 Bit Is Not Supported By All Versions Of Oracle Weblogic Server

Description: IBM JDK 64 bit is not supported for all versions of Oracle WebLogic Server. Oracle will provide support to the best of its ability. You may be advised to revert to a supported JVM configuration if you encounter an Oracle issue that appears to be JVM-related.

Severity: Warning

Rationale: Administration

17.1.150 Ipv6 Dual Stack Is Unsupported

Description: Dual stack is NOT supported. As a result, when dual stack is configured and an Oracle WebLogic Server domain is started on the machine, Oracle WebLogic Server seems to be listening only to IPv4 address and not to the IPv6 address.Now Oracle WebLogic Server supports IPv6 address.

Severity: Warning

Rationale: Administration

17.1.151 Ipv6 Dual Stack Is Unsupported (Upgrade)

Description: Dual stack is not supported. As a result, when dual stack is configured and an Oracle WebLogic Server domain is started on the machine, Oracle WebLogic Server seems to be listening only to IPv4 address and not to the IPv6 address.Now Oracle WebLogic Server supports IPv6 address.This problem, described in Oracle Bug 8153228, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.1.152 If The Ssl Option Is Changed Through Administration Console, Url Always Reverts To Port 7001

Description: If you use the Administration Console to enable/disable the SSL option for a server, and the server is accessed through a proxy server, when the changes are

activated, the accessed URL is hard-coded and redirects to port 7001.If you access the Administration Console through a proxy server, the connection to the Administration Server will be lost. This is because the URL is redirected to port 7001, which does not access the Console from the client side.

Severity: Minor Warning

Rationale: Administration

17.1.153 If Weblogic_Patch.Jar Is After Weblogic.Jar The Installed Patches Have No Effect

Description: Some customers write their own startup and environment scripts. Sometimes they invert the CLASSPATH order. When this occurs, patches applied with BSU are not active even if Oracle Enterprise Manager detects them. The weblogic_patch.jar must always come before weblogic_sp.jar and weblogic.jar in the classpath.

Severity: Critical

Rationale: Administration

17.1.154 Incorrect <Info> Message In Logs: Java.Net.Protocolexception: Http Tunneling Is Disabled

Description: Under the following conditions, you may observe the following message written to the server logs continuously every few seconds. This happens when a certain sequence is used when starting the Oracle WebLogic Server Administration Server and Managed Servers.This can occur under the following conditions:1. The Administration Server listen-address is set to something other than "localhost."2. TunnelingEnabled is set to "false" (default setting).Example error message:HTTPClntLogin: Login rejected with code: 'Failed', reason: java.net.ProtocolException: HTTP tunneling is disabled at weblogic.rjvm.http.HTTPServerJVMConnection.acceptJVMConnection(HTTPServerJVMConnection.java:88) ...

Severity: Minor Warning

Rationale: Administration

17.1.155 Increased Garbage Collection Time In Oracle Jrockit R27.1.X And R27.2.X

Description: In rare cases, external compaction can cause very long pause times when attempting to move a large object from the highest heap parts, if the heap is fragmented.

Severity: Warning

Rationale: Performance

17.1.156 Jax-Ws Bundled With Wls Complains Wsdl Is Not A Valid Service At Runtime

Description: When invoking a Web service using JAX-WS stack at runtime, the following exception is thrown by the client:javax.xml.ws.WebServiceException: {http://host.domain/schemas/envelope/v3_0}GetProfileService is not a valid service. Valid services are: at com.sun.xml.ws.client.WSServiceDelegate.parseWSDL(WSServiceDelegate.java:210) at com.sun.xml.ws.client.WSServiceDelegate.<init>(WSServiceDelegate.java:165) at com.sun.xml.ws.spi.ProviderImpl.createServiceDelegate(ProviderImpl.java:49) at

weblogic.wsee.jaxws.spi.WLSProvider.createServiceDelegate(WLSProvider.java:18) at javax.xml.ws.Service.<init>(Service.java:57)The reason for this is that JAX-WS stack failed to read relative paths in XSDs while parsing WSDLs packaged as JARs.

Severity: Warning

Rationale: Development

17.1.157 Jax-Ws Bundled With Wls Complains Wsdl Is Not A Valid Service At Runtime (Upgrade)

Description: When invoking a Web service using JAX-WS stack at runtime, the following exception is thrown by the client:javax.xml.ws.WebServiceException: {http://host.domain/schemas/envelope/v3_0}GetProfileService is not a valid service. Valid services are: at com.sun.xml.ws.client.WSServiceDelegate.parseWSDL(WSServiceDelegate.java:210)The reason for this error is that JAX-WS stack failed to read relative paths in XSDs while parsing WSDLs packaged as JARs. This problem, described in Oracle Bug 8194951, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Development

17.1.158 Jaxb-Compiler-Generated Client Throws Nullpointerexception

Description: When the Web Services Definition Language (WSDL) elements are qualified without default namespace, the JAXB-compiler-generated client class is throwing a NullPointerException, with client exception as below:Exception in thread 'Main Thread' java.lang.NullPointerException at com.sun.xml.ws.model.wsdl.WSDLBoundPortTypeImpl.freeze(WSDLBoundPortTypeImpl.java:203) at com.sun.xml.ws.model.wsdl.WSDLModelImpl.freeze(WSDLModelImpl.java:221) ...Note: The same thing is working fine when all elements with namespace (default explicitly) are qualified.

Severity: Warning

Rationale: Development

17.1.159 Jaxb-Compiler-Generated Client Throws Nullpointerexception (Upgrade)

Description: When Web Services Definition Language (WSDL) elements are qualified without default namespace, the JAXB-compiler-generated client class throws a NullPointerException, beginning with the lines below:Exception in thread 'Main Thread' java.lang.NullPointerException at com.sun.xml.ws.model.wsdl.WSDLBoundPortTypeImpl.freeze(WSDLBoundPortTypeImpl.java:203) ...Note: This error does not occur when all elements with namespaces (default explicitly) are qualified.This problem, described in Oracle Bug 8192605, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Development

17.1.160 Jdbc Pool Check For Hanging Connections Can Suspend A Good Pool

Description: When an application attempts to retrieve a connection from the JDBC pool, and the connections appear to be hanging, the system checks if the maximum

"Seconds to Trust an Idle Pool Connection" has been exceeded. The return value for the test method should indicate whether a real test was done, and whether it passed. However, the test method return values are inconsistent. In addition, the code responsible for tabulating test durations does not distinguish between actual tests and non-tests, so the non-tests biased the average "test time" as faster than a real test. This can cause some actual tests to appear to hang.

Severity: Minor Warning

Rationale: Administration

17.1.161 Jdbc Pool Check For Hanging Connections Can Suspend A Good Pool. (Upgrade)

Description: When an application attempts to retrieve a connection from the JDBC pool, the implementation checks if the maximum "Seconds to Trust an Idle Pool Connection" has been exceeded, and the connections appear to be hanging. The return value for the test method is supposed to indicate whether a real test was done or not, and whether it passed or not. However, the test method return values are inconsistent. Furthermore, the code responsible for tabulating test durations does not distinguish between actual tests and non-tests, so the non-tests biased the average "test time" as faster than a real test. This can cause actual tests to appear to hang.This problem, described in Oracle Bug 8174835, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.1.162 Jms Saf Client Does Not Fail Over To Other Cluster Members When Primary Member Goes Down

Description: The JMS SAF Client does not fail over to other cluster members when the primary member goes down. The following exception occurs on closing and creating a new SAF client context, as the messages are redirected to the other members:<Jun 19, 2008 7:23:26 PM PDT> <Error> <Kernel> <BEA-000802> <ExecuteRequest failed java.lang.IllegalArgumentException: TimerManager is in STOPPED state.java.lang.IllegalArgumentException: TimerManager is in STOPPED state at weblogic.timers.internal.TimerManagerImpl.schedule(TimerManagerImpl.java: 392) ...>

Severity: Minor Warning

Rationale: User Viewable Errors

17.1.163 Jms Client Hangs Occasionally

Description: JMS client occasionally hangs on a belated connection close if the auto-reconnect logic has already been activated for the connection.

Severity: Warning

Rationale: Subsystem Outage

17.1.164 Jms Producer Memory Leak

Description: JMS producer leaks memory when the producer is repeatedly created and closed while the session remains open.

Severity: Minor Warning

Rationale: Administration

17.1.165 Jms Producer Memory Leak (Upgrade)

Description: JMS producer leaks memory when the producer is repeatedly created and closed while the session remains open.This problem, described in Oracle Bug 8108465, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.1.166 Jms Producer Memory Leak (Upgrade)

Description: JMS producer leaks memory when the producer is repeatedly created and closed while the session remains open.This problem, described in Oracle Bug 8108465, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.1.167 Jms Server Byteshighcount Is Greater Than 50 Percent Of Jvm Heapsizecurrent

Description: When the JMS Server's BytesHighCount attribute is greater than 50 percent of the JVM's HeapSizeCurrent, and the BytesPagingEnabled and MessagesPagingEnabled attributes are not set, a JMS processing error may have occured or may occur in the future.

Severity: Critical

Rationale: Server Outage

17.1.168 Jms Wrapper Uses Wrong User Credentials For Creating Foreign Initial Context

Description: The JMS wrapper is overriding the given foreign JNDI properties for creating Initial Context.This leads to the following warning message:<Warning> <JMSPool> <BEA-169808> <There was an error while making the initial connection to the JMS resource named 'xxx' from the EJB 'yyy' inside application 'zzz.' The server will attempt the connection again later. The error was javax.jms.JMSSecurityException: invalid name or password>

Severity: Warning

Rationale: Administration

17.1.169 Jms Wrapper Uses Wrong User Credentials For Creating Foreign Initial Context. (Upgrade)

Description: The JMS wrapper is overriding the given foreign JNDI properties for creating Initial Context.This leads to the following warning message:<Warning> <JMSPool> <BEA-169808> <There was an error while making the initial connection to the JMS resource named xxx from the EJB yyy inside application zzz. The server will attempt the connection again later. The error was javax.jms.JMSSecurityException:

invalid name or password>This problem, described in Oracle Bug 8191156, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.1.170 Jms Wrappers Not Handled Properly When Using Jms 1.1 Api

Description: JMS wrappers not handled properly when using JMS 1.1 API.Using wrappers means configuring a Foreign Connection Factory and a Foreign Destination that correspond to remote JMS objects (either non-Oracle or Oracle WebLogic Server JMS) as entries in your local JNDI tree.For foreign and remote destinations, the simplest configuration strategy is to use Oracle WebLogic Server JMS wrappers. Wrappers allow you to create a "symbolic link" between a JMS object in a third-party JNDI provider or in a different Oracle WebLogic Server cluster or domain, and an object in the local Oracle WebLogic Server JNDI tree.

Severity: Minor Warning

Rationale: Administration

17.1.171 Jms Wrappers Not Handled Properly When Using Jms 1.1 Api (Upgrade)

Description: JMS wrappers not handled properly when using JMS 1.1 API.Using wrappers means configuring a Foreign Connection Factory and a Foreign Destination that correspond to remote JMS objects (either non-Oracle or Oracle WebLogic Server JMS) as entries in your local JNDI tree.For foreign and remote destinations, the simplest configuration strategy is to use Oracle WebLogic Server JMS wrappers. Wrappers allow you to create a "symbolic link" between a JMS object in a third-party JNDI provider or in a different Oracle WebLogic Server cluster or domain, and an object in the local Oracle WebLogic Server JNDI tree.This problem, described in Oracle Bug 8190861, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.1.172 Jmssecurityexception While Sending Message To Destination When Jms Access Is Restricted

Description: When sending a message to a distributed topic in Oracle WebLogic Server 10.0 after restricting JMS access to a specific user, a JMSSecurityException will occur. You may see "weblogic.jms.common.JMSSecurityException: Access denied to resource??????" at weblogic.jms.common.JMSSecurityHelper.checkPermission(JMSSecurityHelper.java: 157)...

Severity: Minor Warning

Rationale: Administration

17.1.173 Jmssecurityexception While Sending Message To Destination When Jms Access Is Restricted. (Upgrade)

Description: Sending a message to a distributed topic in Oracle WebLogic Server 10.0, after restricting JMS access to a specific user, generates a JMSSecurityException. The message is not forwarded to the secondary server due to the following exception:weblogic.jms.common.JMSSecurityException: Access denied to resource:

type=<jms>, application=DESystemModule, destinationType=topic,resource=DistributedTopic-0, action=send at weblogic.jms.common.JMSSecurityHelper.checkPermission(JMSSecurityHelper.java:157) ...This problem, described in Oracle Bug 8149019, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.1.174 Jrockit 1.4.2_08 Crashes When Calling Remote Web Services, Causing Null Pointer Exception

Description: A crash can occur in Oracle JRockit 1.4.2_0 when calling remote web services, causing a NullPointerException in the native code.The following is an example thread stack trace: - - - - - - - - - -Error code: 52Error Message: Null pointer exception in native codeSignal info : si_signo=11, si_code=2 - - - - - - - - - -Thread Stack Trace: at org/apache/axis/message/MessageElement.addTextNode(MessageElement.java:1388)@0xa77c3ae0 at org/apache/axis/message/SOAPHandler.addTextNode(SOAPHandler.java:148)@0xa77ea0d6 at org/apache/axis/message/SOAPHandler.endElement(SOAPHandler.java:112)@0xa77ea8ed at org/apache/axis/encoding/DeserializationContext.endElement(DeserializationContext.java:1087)@0xa77ea468

Severity: Warning

Rationale: Administration

17.1.175 Jrockit 1.5.0_08 R27.1.0 - Jrockit Does Not Calculate Date Correctly

Description: Application Java Byte code produces wrong date when it is compiled with Oracle JRockit 1.5.0_08 R27.1.0For example when using java.util.Calendar:calendar.set(Calendar.MONTH, (calendar.get(Calendar.MONTH) - 1));and when we print Calendar.getTime() the wrong value for month is returned.System.out.println("DATE: " + calendar.getTime());

Severity: Warning

Rationale: Development

17.1.176 Jrockit R27 - Exception Occurs For Servers > Monitoring > Performance Tab In Administration Console. (Upgrade)

Description: An exception can occur in the Oracle WebLogic Server 10.0 Administration Console when you click the Servers - Monitoring tab - Performance tab. This issue occurs only if you are using JRockit R27.3, R27.4, R27.5, or R27.6.The following exceptions may occur:Error opening /jsp/core/server/ServerMonitoringPerformanceForm.jsp.The source of this error is javax.servlet.ServletException: javax.xml.transform.TransformerException:com.sun.org.apache.xml.internal.utils.WrappedRuntimeException:The entity name must immediately follow the '&' in the entity reference.at weblogic.servlet.jsp.PageContextImpl.handlePageExceptionThis problem, described in Oracle Bug 8116840, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Administration

17.1.177 Jrockit R27 - Exception Occurs For Servers>Monitoring>Performance Tab In Admin Console

Description: An exception can occur in the Oracle WebLogic Server 10.0 Administration Console when you click the Servers - Monitoring tab - Performance tab. This issue occurs only if you are using JRockit R27.3, R27.4, R27.5, or R27.6.The following exceptions may occur:Error opening /jsp/core/server/ServerMonitoringPerformanceForm.jsp.The source of this error is javax.servlet.ServletException: javax.xml.transform.TransformerException:com.sun.org.apache.xml.internal.utils.WrappedRuntimeException:The entity name must immediately follow the '&' in the entity reference.at weblogic.servlet.jsp.PageContextImpl.handlePageException

Severity: Warning

Rationale: Administration

17.1.178 Jrockit R27.1.0 - Heap Snapshot Table Cannot Be Configured

Description: The Heap Snapshot table on the Heap Overview tab appears to be configurable, but is not.

Severity: Minor Warning

Rationale: Administration

17.1.179 Jrockit R27.1.0 - Memory Usage And Optimization Data Cannot Be Copied To Clipboard

Description: The Memory Usage data on the General tab and the Optimization data on the Optimization tab of JRockit Mission Control's JRA window cannot be copied to the clipboard using the right click context menu. This works for the other data fields in JRockit Mission Control.

Severity: Minor Warning

Rationale: Administration

17.1.180 Jrockit-R26.4.0 Crashes When A Java Application Has Inline Calculation In The Array

Description: When a Java application that has inline calculation in the array access is deployed on a Oracle WebLogic Server with Oracle JRockit R26.4.0-JDK1.5.0_06, a crash can occur.The error message is as follows:Error Message: Illegal memory access. [54]Signal info : si_signo=11, si_code=1

Severity: Warning

Rationale: Administration

17.1.181 Jsp Compilation Problem With Uppercase In Jsp Path

Description: A JSP compilation problem occurs if uppercase letters are used in the JSP path. For example, assume you compile two .jsp files, one with uppercase letters in the path (: /TEST/A.jsp) and and the other with lowercase letters (/test/A.jsp). After compilation, the generated jsp_servlet path will be the same for both (?/jsp_servlet/_test/A.jsp).

Severity: Warning

Rationale: Administration

17.1.182 Jsr 201 Varargs In Methods Of Ejb 3 Are Not Supported In Oracle Weblogic Server 10.0

Description: In Oracle WebLogic Server 10.0, an error occurs when deploying EJB 3 beans that have methods containing JSR 201 varargs.

Severity: Warning

Rationale: Administration

17.1.183 Jsr 201 Varargs In Methods Of Ejb 3 Are Not Supported In Oracle Weblogic Server 10.0. (Upgrade)

Description: In Oracle WebLogic Server 10.0, an error occurs when deploying EJB 3 beans that have methods containing JSR 201 varargs.This problem, described in Oracle Bug 8165732, has been fixed in Oracle WebLogic Server 10.3.

Severity: Minor Warning

Rationale: Administration

17.1.184 Jvm 1.4.1_X Assertion Failed [Invalid Assignment From 'Object' To 'Object']

Description: The following error occurs when starting the managed server with 1.4.1_X JVM:"weblogic.utils.AssertionError: ***** ASSERTION FAILED *****[invalid assignment from 'Object' to 'Object'] at weblogic.utils.Debug.assertion(Debug.java: 57)"The managed server startup failures due to weblogic.utils.AssertionError is because of JVM HotSpot optimizations. This is a JVM issue.

Severity: Minor Warning

Rationale: Administration

17.1.185 Jvm Could Crash At Parallel Gc Run Oracle Jrockit R27.1, R27.2, R27.3

Description: A crash can happen while executing Oracle JRockit R27.X parallel garbage collection(-Xgc:parallel)objPoolMarkAllWeak function passes a null object to refResweepWeakHandle, giving a Tread Stack Trace as the following one: at refResweepWeakHandle+117()@0xb7d0f245 at objPoolMarkAllWeak +630()@0xb7ce03a6 ...This can be observed mostly using JVMTI agent.

Severity: Minor Warning

Rationale: Administration

17.1.186 License Validation Error When Starting Edge3.0

Description: The system returns the following license verification errors when attempting to deploy the Edge Server from a Web Application Archive (WAR) file when running Oracle WebLogic Server 10.0:ExecuteThread: '0' for queue: 'weblogic.kernel.Default (self-tuning)'> <<WLS Kernel>> <> <> <1180720904590> <BEA-101216> <Servlet: "RFIDEdgeServlet" failed to preload on startup in Web application: "rfidedge-3.0.0.war".java.lang.RuntimeException: Unable to start due to license verification error: Exception occurred while reading the license file. at com.connecterra.servlet.RFIDEdgeServlet.init(RFIDEdgeServlet.java:91) at

weblogic.servlet.internal.StubSecurityHelper
$ServletInitAction.run(StubSecurityHelper.java:282) ...

Severity: Warning

Rationale: Administration

17.1.187 Long Deployment Time Of Ejb Compared To Jboss

Description: When the application is recompiled as hash code created by the EJB container, it is different from the previous recompilation. Because application recompilation takes a large part of the time required for deployment, this slows down Oracle WebLogic Server deployment time, as compared to that for JBoss.

Severity: Minor Warning

Rationale: Administration

17.1.188 Long Deployment Time Of Ejb Compared To Jboss (Upgrade)

Description: When the application is recompiled as hash code created by the EJB container, it is different from the previous recompilation. Since application recompilation takes a large part of the time required for deployment, this slows down Oracle WebLogic Server deployment time, as compared to that for JBoss.This problem, described in Oracle Bug 8121596, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.1.189 Mdb Fails To Connect To Jms Destination When Using Global Work Manager

Description: Using globally scoped Work Manager in Oracle WebLogic Server 10.x and the dispatch-policy element of the WebLogic Enterprise bean in weblogic-ejb-jar.xml, the Message Driven Bean (MDB) fails to connect to the destination throwing:The Message-Driven EJB: WMTestMDB is unable to connect to the JMS destination: queue.cap.TestQueue. The Error was: java.lang.NegativeArraySizeException: allocArray>The error is:1. Seen when Maximum Threads Constraint Count = -1 (default value).2. NOT seen if application scoped work manager used.To avoid this problem, use:1. Application scoped work manager.2. A positive integer for Maximum Threads Constraint Count != -13. A global work manager, delete the Maximum Threads Constraint.

Severity: Minor Warning

Rationale: Administration

17.1.190 Mdb Fails To Connect To Jms Destination When Using Global Work Manager (Upgrade)

Description: When using globally scoped Work Manager in Oracle WebLogic Server 10.x and specifying the work manager using the dispatch-policy element of the weblogic-enterprise-bean in weblogic-ejb-jar.xml, the Message Driven Bean (MDB) fails to connect to the destination and throws the following error message:[ACTIVE] ExecuteThread: '1' for queue: 'weblogic.kernel.Default (self-tuning)'> <<WLS Kernel>> <> <> <1227880827533> <BEA-010061> <The Message-Driven EJB: WMTestMDB is unable to connect to the JMS destination: queue.cap.TestQueue. The Error was:

java.lang.NegativeArraySizeException: allocArray>Oracle Bug 8179644 has been fixed in Oracle WebLogic Server 10.3 Maintenance Pack 2

Severity: Minor Warning

Rationale: Administration

17.1.191 Mdb Does Not Connect To Remote Distributed Queue Through Foreignjmsserver (Wls V10.0, Upgrade)

Description: A Message Driven Bean (MDB) does not connect to a remote distributed queue through local ForeignJMSServer without giving a provider URL in the deployment descriptor. However, it can connect to a remote Oracle WebLogic Server queue (not distributed) without providing a provider URL.This problem, described in Oracle Bug 8141201, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.1.192 Managed Servers Fail To Reconnect To Backup Admin Server Running On Different Ip

Description: If the Oracle WebLogic Server Administration Server goes down and the backup Administration Server is restarted at a different URL, managed servers connected to the Administration Server are disconnected.

Severity: Warning

Rationale: Administration

17.1.193 Managed Servers Fail To Reconnect To Backup Admin Server Running On Different Ip (Upgrade)

Description: If the Oracle WebLogic Server Administration Server goes down and the backup Administration Server is restarted at a different URL, Managed Servers connected to the Administration Server are disconnected.This problem, described in Oracle Bug 8110232, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Administration

17.1.194 Managed Servers May Periodically Drop In And Out Of A Cluster When Running On Solaris 10

Description: When an Oracle WebLogic Server cluster has been configured on a Solaris 10 box(es), Managed Server instance(s) may periodically drop in and out of the cluster.Even though the server instances automatically rejoin the cluster, there will be lost multicast messages, and response time will be impacted due to the increased cluster housekeeping being required (for example, increased failover of requests or additional session replication needing to be carried out). This will then result in slower performance being seen by the end user/client.This issue is seen only on Solaris 10, regardless of the version of Oracle WebLogic Server being used.

Severity: Warning

Rationale: Performance

17.1.195 Memory Leak With Distributed Garbage Collection, And Callback Method Is Not Invoked

Description: A memory leak occurs with distributed garbage collection. On the server side, once all RMI clients are disconnected and the remote object is unbound from the RMI service, the client code java.rmi.server.Unreferenced.unreferenced method is not invoked as expected.

Severity: Minor Warning

Rationale: Administration

17.1.196 Memory Leaks Can Occur In Javelin Framework When Compiling Jsp Pages

Description: Memory leaks can occur in the Javelin Framework, which can lead to an increase in the number of objects when a JSP page is compiled.

Severity: Warning

Rationale: Administration

17.1.197 Memory Leaks Can Occur In Javelin Framework When Compiling Jsp Pages (Upgrade)

Description: Memory leaks can occur in the Javelin Framework, which can lead to an increase in the number of objects when a JSP page is compiled.This problem, described in Oracle Bug 8196614, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.1.198 Message Bridge Does Not Forward Messages Until Restarted Again. (Upgrade)

Description: Message bridge does not forward messages after server restart via console until it (message bridge) is restarted again.This problem, described in Oracle Bug 8131966, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.1.199 Method Ejbtimout() In Superclass Not Recognized

Description: The ejbTimout() method in a superclass is not recognized. In an example scenario, assume there are several MessageDrivenBeans that derive from an abstract superclass that implements javax.ejb.MessageDrivenBean, javax.jms.MessageListener, and javax.ejb.TimedObject. The EJBTimer is also started. With Oracle WebLogic Server 10.0, the server throws the following exception:java.lang.IllegalStateException: [EJB: 011084]This EJB class does not support EJB timers and therefore is prohibited from using the TimerService.To use EJB timers, the bean class must implement javax.ejb.TimedObject or have a method annotated with @Timeout. at weblogic.ejb.container.internal.BaseEJBContext$1.invoke(BaseEJBContext.java:429)

Severity: Minor Warning

Rationale: Development

17.1.200 Method Ejbtimout() In Superclass Not Recognized (Upgrade)

Description: Method ejbTimout() in superclass is not recognized. With Oracle WebLogic Server 10.0, the server throws the following exception:java.lang.IllegalStateException: [EJB:011084]This EJB class does not support EJB timers and therefore is prohibited from using the TimerService.To use EJB timers, the bean class must implement javax.ejb.TimedObject or have a method annotated with @Timeout. at weblogic.ejb.container.internal.BaseEJBContext $1.invoke(BaseEJBContext.java:429) at $Proxy151.createTimer(Unknown Source) ...Oracle Bug 8120098 has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Development

17.1.201 Multicast Address Is Out Of Bounds

Description: The multicast address must be between 224.0.0.0 and 239.255.255.255.

Severity: Warning

Rationale: Subsystem Outage

17.1.202 Multiple Threads Waiting For A Message To Finish Paging Causing Server Unresponsiveness

Description: Many threads get blocked on weblogic.messaging.kernel.internal.MessageHandle.waitForPaging(MessageHandle.java:474)The block is as a result of waiting for the Paging on MessageHandle(s) to finish.The particular thread that appears to be holding the lock is: "[ACTIVE] ExecuteThread: '303' for queue: 'weblogic.kernel.Default (self-tuning)'" RUNNABLE weblogic.messaging.kernel.internal.PagingImpl.run(PagingImpl.java:455) weblogic.work.ServerWorkManagerImpl$WorkAdapterImpl.run (ServerWorkManagerImpl.java:518) weblogic.work.ExecuteThread.execute(ExecuteThread.java:207) weblogic.work.ExecuteThread.run(ExecuteThread.java:179)The thread is RUNNABLE and holds the lock on a MessageHandle.

Severity: Minor Warning

Rationale: Administration

17.1.203 Multiple Threads Waiting For A Message To Finish Paging Causing Server Unresponsiveness (Upgrade)

Description: Many threads get blocked on weblogic.messaging.kernel.internal.MessageHandle.waitForPaging(MessageHandle.java:474)The block is as a result of waiting for the Paging on MessageHandle(s) to finish.The particular thread that appears to be holding the lock is: "[ACTIVE] ExecuteThread: '303' for queue: 'weblogic.kernel.Default (self-tuning)'" RUNNABLE weblogic.messaging.kernel.internal.PagingImpl.run(PagingImpl.java:455) weblogic.work.ServerWorkManagerImpl$WorkAdapterImpl.run (ServerWorkManagerImpl.java:518)The thread is RUNNABLE and holds the lock on a MessageHandle.This problem, described in Oracle Bug 8112849, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.1.204 Multithreaded Client Fails Randomly On Entitymanager.Persist

Description: A Multithreaded Client receives the following exception when invoking an EJB3 entity bean using a session bean. The concurrent EJB method invocations are being succeeded, and also failing randomly. When the client is running with only one thread, there is no failure.The exception is as follows:javax.ejb.EJBException: nested exception is:javax.persistence.TransactionRequiredException: The method public abstractvoid javax.persistence.EntityManager.persist(java.lang.Object) must be called in the context of a transaction.javax.persistence.TransactionRequiredException: The method public abstractvoid javax.persistence.EntityManager.persist(java.lang.Object) must be calledin the context of a transaction.....

Severity: Warning

Rationale: Subsystem Outage

17.1.205 Multithreaded Client Fails Randomly On Entitymanager.Persist (Upgrade)

Description: A Multithreaded Client receives the following exception when invoking an EJB3 entity bean using a session bean. The concurrent EJB method invocations are being succeeded, and also failing randomly. When the client is running with only one thread, there is no failure.The exception is as follows:javax.ejb.EJBException: nested exception is:javax.persistence.TransactionRequiredException: The method public abstractvoid javax.persistence.EntityManager.persist(java.lang.Object) must be called in the context of a transaction.....The problem, described in Oracle Bug 8161389, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Subsystem Outage

17.1.206 Muxablesocket Objects Are Not Being Removed From Sockets(Hashset) In Socketmuxer On Client

Description: When using -Dweblogic.system.iiop.reconnectOnBootstrap=true on an IIOP client, IIOP sockets are created/closed per creating InitialContext. However, weblogic.iiop.MuxableSocketIIOP remains in sockets in SocketMuxer. As a result, an OutOfMemoryError occurs on IIOP client.

Severity: Minor Warning

Rationale: Administration

17.1.207 Muxablesocket Objects Are Not Being Removed From Sockets(Hashset) In Socketmuxer On Client (Upgrade)

Description: When using -Dweblogic.system.iiop.reconnectOnBootstrap=true on an IIOP client, IIOP sockets are created/closed per creating InitialContext. However, weblogic.iiop.MuxableSocketIIOP remains in sockets in SocketMuxer. As a result, an OutOfMemoryError occurs on the IIOP client.This problem, described in Oracle Bug 8157696, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.1.208 Native Performance Pack Was Not Loaded On Server Start-Up

Description: During the server startup the performance pack or native IO should be loaded if NativeIOEnabled switch is turned on. If this does not occur, usually the library path is not set correctly or the user rights for the directory or performance pack library file are not set properly.

Severity: Warning

Rationale: Performance

17.1.209 Noncompliant Interface And Implementation Classes Cause Oracle Jrockit To Crash

Description: When an interface is not compliant with the implementation classes, Oracle JRockit may crash or throw a NullPointerException. This occurs because Oracle JRockit does not perform verification of implemented interfaces before a call, unless it is started with the option -Xverify:all.Oracle JRockit R24.5.0 and previous versions crash under these conditions. Oracle JRockit R25.2.1-11 and later throw a NullPointerException where an IncompatibleClassChangeError could be expected.

Severity: Critical

Rationale: Server Outage

17.1.210 Not Able To Monitor Mdb Durable Subscriber In Admin Console

Description: Unable to monitor the MDB Durable Subscriber in the Oracle WebLogic Server Administration Console.

Severity: Minor Warning

Rationale: Development

17.1.211 Nullpointerexception At Javelin.Java.Typesystem.Paramtype.Equalsnonrecursive

Description: A NullPointer exception is thrown when trying to access an application that is deployed as a hot deployment.java.lang.NullPointerExceptionat javelin.java.typesystem.ParamType.equalsNonRecursive(ParamType.java:502) at javelin.java.typesystem.Method.paramsEqual(Method.java:318) at javelin.java.typesystem.Method.equals(Method.java:336)

Severity: Minor Warning

Rationale: Development

17.1.212 Nullpointerexception At Javelin.Java.Typesystem.Paramtype.Equalsnonrecursive (Upgrade)

Description: A NullPointer exception is thrown when trying to access an application that is deployed as a hot deployment.java.lang.NullPointerExceptionat javelin.java.typesystem.ParamType.equalsNonRecursive(ParamType.java:502) at javelin.java.typesystem.Method.paramsEqual(Method.java:318) at javelin.java.typesystem.Method.equals(Method.java:336)This problem, described in Oracle Bug 8106219, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Development

17.1.213 Nullpointerexception In Java.Nio.Directbytebuffer._Get()

Description: Running with Oracle JRockit 1.5.0_08(R27.1.0) and getting a NullPointerException in java.nio.DirectByteBuffer._get()Following is the stack trace along with the NPE thrown,java.lang.NullPointerException:java.nio.DirectByteBuffer._get(Unknown Source)java.nio.Bits.getIntL(Unknown Source)java.nio.Bits.getInt(Unknown Source)java.nio.HeapByteBuffer.getInt(Unknown Source)

Severity: Warning

Rationale: Administration

17.1.214 Nullpointerexception Occurs At Basewsservlet.Init() Method After Reloading A Servlet

Description: After reloading a servlet, a NullPointerException occurs when calling a Java Web Service.At first, WebServices(WSDL) call works fine; however, after reloading the servlet, it generates a NullPointerException when calling the WebServices again.java.lang.NullPointerException at weblogic.wsee.server.servlet.BaseWSServlet.init(BaseWSServlet.java:72) at javax.servlet.GenericServlet.init(GenericServlet.java:241) ...

Severity: Minor Warning

Rationale: Administration

17.1.215 Nullpointerexception Occurs At Basewsservlet.Init() Method After Reloading A Servlet (Upgrade)

Description: After reloading a servlet, a NullPointerException occurs when calling a Java Web Service.At first, WebServices(WSDL) call works fine; however, after reloading the servlet, it generates a NullPointerException when calling the Web Services again.java.lang.NullPointerException at weblogic.wsee.server.servlet.BaseWSServlet.init(BaseWSServlet.java:72) at javax.servlet.GenericServlet.init(GenericServlet.java:241) at weblogic.servlet.internal.StubSecurityHelper $ServletInitAction.run(StubSecurityHelper.java:282) ...This problem, described in Oracle Bug 8129336, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2

Severity: Minor Warning

Rationale: Administration

17.1.216 Nullpointerexception Occurs When Deploying A Web Service That Uses @Handlerchain

Description: A NullPointerException occurs when deploying a Web Service that uses @HandlerChain.weblogic.application.ModuleException: [HTTP:101216]Servlet: 'WSAATestService'failed to preload on startup in Web application: 'wsaa-jaxwshandlertest.war'.java.lang.NullPointerExceptionat weblogic.wsee.monitoring.WseeRuntimeMBeanManager.createJaxWsHandlers(WseeRuntimeMBeanManager.java:108)...

Severity: Minor Warning

Rationale: Development

17.1.217 Nullpointerexception Occurs When Deploying A Webservice That Uses @Handlerchain (Upgrade)

Description: A NullPointerException occurs when deploying a Web Service that uses @HandlerChain.The following exception occurs:weblogic.application.ModuleException: [HTTP:101216]Servlet: 'WSAATestService'failed to preload on startup in Web application: 'wsaa-jaxwshandlertest.war'.java.lang.NullPointerExceptionat weblogic.wsee.monitoring.WseeRuntimeMBeanManager.createJaxWsHandlers(WseeRuntimeMBeanManager.java:108)...This problem, described in Oracle Bug 8189587, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2

Severity: Minor Warning

Rationale: Development

17.1.218 Nullpointerexception When Compiling Web Service At Weblogic.Wsee.Tools.Anttasks.Jwsctask.E

Description: A NullPointerException is reported by JWSC (Java Web Service compiler) if portName in the implementation class does not match with the portName in Web Service Definition Language (WSDL).Sample error message:java.lang.NullPointerExceptionat weblogic.wsee.tools.anttasks.JwscTask.execute(JwscTask.java:190)at org.apache.tools.ant.UnknownElement.execute(UnknownElement.java:275)at org.apache.tools.ant.Task.perform(Task.java:364)at org.apache.tools.ant.Target.execute(Target.java:341)at org.apache.tools.ant.Target.performTasks(Target.java:369)at org.apache.tools.ant.Project.executeSortedTargets(Project.java:1216)at org.apache.tools.ant.Project.executeTarget(Project.java:1185)...

Severity: Warning

Rationale: Development

17.1.219 Oracle Bug 8151745 Patch Places A Restriction On The Size Of Jsps (Upgrade)

Description: The patch for Oracle Bug 8151745 places a restriction on the size of JSPs, if the class file generated by the JSP compiler generates methods that exceed the 64K.The server log shows that the JSP cannot be loaded because the requested class was not found in the classpath, and the browser cannot display a blank page.This problem has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.1.220 Oracle Jrockit 1.4.2_12 Crash At Mmgetobjectsize()

Description: Oracle JRockit 1.4.2_12 crashed on multiple WLS 8 SP4 servers.Oracle JRockit dump shows the following stack trace:Stack 0: start=0xb7a58000, end=0xb7a9c000, guards=0xb7a5d000 (ok),forbidden=0xb7a5b000Thread Stack Trace: at mmGetObjectSize+8()@0xb7e6b3c8 at findNext+166()@0xb7e9a006 at refIterGetNext +44()@0xb7e9a24c at trMarkRootsForThread+325()@0xb7ea83b5 at

mmMarkRootsForThread+44()@0xb7e2cc2c at mmParThreadInspection +45()@0xb7e7794d at tsDoGCInspectionForAllThreads+37()@0xb7ed8555 at mmParMark+118()@0xb7e77d16 at mmGCMainLoop+1074()@0xb7d73722 at tsiCallStartFunction+81()@0xb7e1ac81 at tsiThreadStub+126()@0xb7e1bd1e at ptiThreadStub+18()@0xb7e840d2 at start_thread+129()@0x9e6371 at clone +94()@0x88e9be - Java stack -

Severity: Critical

Rationale: Server Outage

17.1.221 Oracle Jrockit 1.5.0_4 Silently Ignores -Dfile.Encoding

Description: Oracle JRockit 5.0 - file.encoding does not work on Linux - instead the default system settings are usedIn java versions prior to 5.1 (or 1.5), the system property -D file.encoding defined an encoding that will be used by FileReader / FileWriter. This is still true for Sun Hotspot 1.5 and also for Oracle JRockit 5.0 on Windows.However, on Linux, setting the system property -Dfile.encoding does not have any effect on FileReader / FileWriter They take their encoding from the system default settings.This problem only happens on Linux - not on Windows.

Severity: Warning

Rationale: Administration

17.1.222 Oracle Jrockit R26.3.0 Sets System Time Back

Description: In Oracle JRockit R26 versions earlier than R26.4 on Windows operating systems, Oracle JRockit can expose a problem in the OS related to multimedia timers that causes the system time to be adjusted backwards.This can cause the system time to jump back by about 1 minute. If this happens, you can turn off the use of multimedia timers with -Djrockit.periodictask.usemmtimers=false, otherwise upgrade to R26.4 or later.

Severity: Warning

Rationale: Administration

17.1.223 Oracle Jrockit R26.4 And R27.1 Performance Is Slower Compared To Previous Versions

Description: For JRockit releases R26.4 and R27, if a thread was interrupted for garbage collection while it was in the process of copying an array, then the garbage collection may result in very long pauses.

Severity: Warning

Rationale: Performance

17.1.224 Oracle Jrockit R27.3.1 Crashes When Calling Inflate On A Closed Inflator

Description: Sometimes, calling inflate on a closed Inflater results in Oracle JRockit crashing, creating a core file. It can occur with Oracle JRockit R27.3.1.The relevant stack trace will be similar to the following:Thread Stack Trace: at inflate +73()@0x000000001027C409 at RJNI_java_util_zip_Inflater_inflateFast +90()@0x000000001020162A - Java stack - at java/util/zip/ Inflater.inflateFast(JJIJI)I(Native Method) at java/util/zip/ Inflater.inflateBytes(Inflater.java:354) at java/util/zip/Inflater.inflate(Inflater.java:216)

Severity: Critical

Rationale: Administration

17.1.225 Oracle Jrockit Does Not Support The Linux Elhugemem Kernel

Description: Oracle does not support Oracle JRockit running on the ELhugemem kernel.The ELhugemem kernel had been intended as a stopgap measure until 64-bit kernels, which are a better choice, became readily available. An example of problems with the ELhugemem kernel is 5-10 percent performance loss under normal I/O and even greater performance degradation when more calls are made into the kernel (for example, heavy I/O).

Severity: Warning

Rationale: Not Complying with Specifications

17.1.226 Oracle Weblogic Server Thin Client Is Not Supported On Aix

Description: Oracle WebLogic Server is running on an AIX platform and is configured with IIOP enabled. Please note that the thin client is not supported for this configuration.

Severity: Minor Warning

Rationale: Non-User Viewable Errors

17.1.227 Oracle Weblogic Tuxedo Connector Jatmi Classes Are Not In Weblogic.Jar

Description: In Oracle WebLogic Server 10.0, Tuxedo WTC JATMI classes such as "TuxedoConnection and TuxedoConnectionFactory " are not included in weblogic.wtc package. These classes are now available from com.bea.core.jatmi_1.0.0.0.jar (in the modules directory of Oracle WebLogic Server 10 installation).

Severity: Minor Warning

Rationale: Development

17.1.228 Parsing Of Nested Cdata In Xml Results In Missing Characters

Description: When using Oracle WebLogic Integration 9.2 Maintenance Pack 1/ Maintenance Pack 2, if input XML contains nested CDATA, parsing of this document results in some missing characters from the original input data.For example, the following line is part of the input XML:< ! [CDATA [<Category>< ! [CDATA [<data>data</data>]] ></Category>]] >Parsing results in the following line:< ! [CDATA [<Category>< ! [CDATA [<data>data</data>]] ></Category>]] >Note the two missing characters at the end of the line (after Category '>' becomes '>').

Severity: Minor Warning

Rationale: Administration

17.1.229 Patch Oracle Bug 8151745 Places A Restriction On The Size Of Jsps

Description: The patch for Oracle Bug 8151745 introduces a regression, in which it places a restriction on the size of JSPs. The class file generated by the JSP compiler generates methods that exceed the allowed size (64 KB).Server log shows the following:[weblogic.servlet.internal.WebAppServletContext@314ec947 - appName: 'application', name: '/eventManager', context-path: '/eventManager']: Servlet class com.on24.eventManager.__eventdescription for servlet /eventDescription.jsp could not be loaded because the requested class was not found in the classpath ... jsp_compile.java.lang.ClassFormatError: ...The browser displays a blank page.

Severity: Warning

Rationale: Administration

17.1.230 Patch Does Not Match The Version Of Oracle Weblogic Server You Are Running

Description: Typically, each Oracle patch corresponds to a specific version of Oracle WebLogic Server. Using a patch that is designated for a different version of Oracle WebLogic Server may result in failures or incorrect behavior.

Severity: Warning

Rationale: Administration

17.1.231 Performance Can Be Improved By Enabling Native Io In Production Mode

Description: Benchmarks show major performance improvements when native performance packs are used on machines that host Oracle WebLogic Server instances. Performance packs use a platform-optimized, native socket multiplexor to improve server performance.

Severity: Minor Warning

Rationale: Administration

17.1.232 Performance Degradation Due To Unnecessary Try/Catch Statement On Aix

Description: A significant performance degradation can occur for Oracle WebLogic Server 10.0 running on AIX.When using a user thread instead of an execute thread, high CPU usage can occur when an exception is thrown. This is due to unnecessary "try and catch" statements in the Oracle WebLogic Server code.Sun JVM in server mode, as well as Oracle JRockit JVM, automatically optimize exception generation when the exception is ignored in a catch. However, IBM JVM for AIX does not optimize exception generation.

Severity: Minor Warning

Rationale: Administration

17.1.233 Performance Degradation Due To Unnecessary Try/Catch Statement On Aix (Upgrade)

Description: A significant performance degradation can occur for Oracle WebLogic Server 10.0 running on AIX.When using a user thread instead of an execute thread, high CPU usage can occur when an exception is thrown. This is due to unnecessary "try and catch" statements in the Oracle WebLogic Server code.The Sun JVM in server mode, as well as Oracle JRockit JVM, automatically optimizes exception generation when the exception is ignored in a catch. However, the IBM JVM for AIX does not optimize exception generation.This problem, described in Oracle Bug 8174460, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.1.234 Performance May Be Impacted By Requests Waiting For A Connection

Description: If a thread requires a connection from a JDBC pool and no connection is available, the thread must wait until one becomes available. At some point in time, a connection pool in your domain had a number of requests waiting for a connection, which may impact the performance of waiting threads.

Severity: Warning

Rationale: Performance

17.1.235 Performance Of Jdbc Statementcachesize Can Be Further Tuned

Description: The use of a prepared statement or callable statement in an application or EJB creates a considerable processing overhead for the communication between the application server and the database server and on the database server itself.To minimize these processing costs, Oracle WebLogic Server can cache the prepared and callable statements that are used in your applications. When an application or EJB calls any of the statements stored in the cache, Oracle WebLogic Server reuses the cached statement. Reusing these statements reduces CPU usage on the database server, which improves the performance of the current statement and leaves the CPU available for other tasks.

Severity: Warning

Rationale: Performance

17.1.236 Permgen Leak - Memory Is Not Released Between Deployments. (Wls V10.0)

Description: PermGen space does not appear to be released between deployments. After undeploying an application, the PermGen space appears to be unreleased. This results in an OutOfMemoryError with PermGen space. This problem is more visible with Oracle WebLogic Portal-related application deployments.

Severity: Warning

Rationale: User Viewable Errors

17.1.237 Plug-In Is Unable To Send Response From Oracle Weblogic Server 10.0 To Client

Description: When using the IIS plug-in in Oracle WebLogic Server 10.0, the Chunked Transfer Encoding responses are buffered by the plug-in. However, the plug-in should stream the chunks when they are received.A new flag, WLFlushChunks, is added in the iisproxy.ini. Setting the WLFlushChunks flag to ON resolves the issue. By default, the flag is OFF.

Severity: Warning

Rationale: Administration

17.1.238 Plugin Is Unable To Send Response From Oracle Weblogic Server10.0 To Client (Upgrade)

Description: When using the IIS plug-in in Oracle WebLogic Server 10.0, the Chunked Transfer Encoding responses are buffered by the plug-in. However, the plug-in should stream the chunks when they are received.A new flag, WLFlushChunks, is added in the iisproxy.ini. Setting the WLFlushChunks flag to ON resolves the issue. By default,

the flag is OFF.This problem, described in Oracle Bug 7936746, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.1.239 Primary Key Could Not Be Found In The Lock Manager

Description: In the log of the server where entity EJBs are deployed, the following exception may be logged:javax.ejb.EJBException: [EJB:010108]The EJB Lock Manager has received an unlock request from EJB:<ejb-class-name> with primary key:<key-field-name>. However, this primary key could not be found in the Lock Manager. This indicates either an EJB container bug, or the equals and hashCode methods for the primary key class:<key-class>.UserPK are implemented incorrectly. Please check the equals and hashCode implementations. [java] at weblogic.ejb.container.locks.ExclusiveLockManager $LockBucket.unlock(ExclusiveLockManager.java:409) [java] at weblogic.ejb.container.locks.ExclusiveLockManager.unlock(ExclusiveLockManager.java:170)...

Severity: Warning

Rationale: Development

17.1.240 Primary Key Could Not Be Found In The Lock Manager. (Upgrade)

Description: In the log of the server where entity beans are deployed, the following exception may be logged:javax.ejb.EJBException: [EJB:010108]The EJB Lock Manager has received an unlock request from EJB:<ejb-class-name> with primary key:<key-field-name>. However, this primary key could not be found in the Lock Manager. This indicates either an EJB container bug, or the equals and hashCode methods for the primary key class:<key-class>.UserPK are implemented incorrectly. Please check the equals and hashCode implementations. [java] at weblogic.ejb.container.locks.ExclusiveLockManager $LockBucket.unlock(ExclusiveLockManager.java:409)This problem, described in Oracle Bug 8083963, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Development

17.1.241 Production Mode Error - Hostnameverification Setting Exposes Vulnerability To Attack

Description: The domain is running in production mode, but the HostnameVerification property has been disabled. When the HostnameVerification attribute has been disabled, Oracle WebLogic Server no longer ensures that the certificate received from a remote site matches the DNS name when making a remote SSL connection. This leaves the connection vulnerable to a "man in the middle" attack.

Severity: Warning

Rationale: Administration

17.1.242 Reading An Environment Variable On In A Wslt Script Under Windows 2003 Does Not Work

Description: Reading an environment variable in a WebLogic Scripting Tool script under Windows 2003 does not work. wls:/offline> import os wls:/offline> sys.version '2.1' wls:/offline> os.environ['WL_HOME'] Failed to get environment, environ will be empty: (0, "Failed to execute command (['sh', '-c', 'env']): java.io.IOException: CreateProcess: sh -c env error=2")

Severity: Minor Warning

Rationale: Subsystem Outage

17.1.243 Request Wrapper Bean Names Must Be Unique

Description: Issue appears if the Web Services Definition Language (WSDL) has a operation name that is identical to the name of an element in the schema it references. For example, WSDL contains the following:<portType name="TestServiceSOAP"> <operation name="getMethod1"> <input message="ts:getMethod1Request"/> <output message="ts:getMethod1Response"/> </operation> <operation name="getMethod2"> <input message="ts:getMethod2Request"/> <output message="ts:getMethod2Response"/> </operation> </portType> And the schema it references contain: <xs:element name="getMethod1" type="ns1:EmptyRequest"/> <xs:element name="getMethod1Response" type="ns1:Holder"/> <xs:element name="getMethod2" type="ns1:EmptyRequest"/> <xs:element name="getMethod2Response"

Severity: Minor Warning

Rationale: Development

17.1.244 Requestdispatcher.Forward() Responds Very Slowly With Httpservletresponsewrapper(Response)

Description: The problem is related to sending back an HTTP-304 (not modified) response.When an HTTP response is wrapped with an HttpServletResponseWrapper or a child class, the response from the server does not send a 'Content-Length: 0' header. Instead the server sends 'Transfer-Encoding: chunked'. This response causes slow processing or unexpected behavior with Firefox, but works fine in Internet Explorer.

Severity: Minor Warning

Rationale: Performance

17.1.245 Requestdispatcher.Forward() Responds Very Slowly With Httpservletresponsewrapper(Response) (Upgrade)

Description: The problem is caused by sending back an HTTP-304 (not modified) response.When an HTTP response is wrapped with an HttpServletResponseWrapper or a child class, the response from the server does not send a 'Content-Length: 0' header. Instead the server sends 'Transfer-Encoding: chunked'. This response causes slow processing or unexpected behavior with Firefox, but works fine in Internet Explorer.This problem, described in Oracle Bug 8087247, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Performance

17.1.246 Resourceaccessexception While Delivering Message Causes Message To Stay In Pending State

Description: A ResourceAccessException from a JTA sub-system while delivering a message causes the message to stay in the pending state permanently until a server restart.javax.transaction.SystemException: start() failed on resource 'WLStore_domain_BUS01_BIZ_FileStore-mgd02BUS01': XAER_RMERR : A resource manager error has occured in the transaction branch weblogic.transaction.internal.ResourceAccessException: Transaction has timed out when making request to XAResource 'WLStore_domain_BUS01_BIZ_FileStore-mgd02BUS01'. at weblogic.transaction.internal.XAResourceDescriptor.startResourceUse(XAResourceDescriptor.java:712)...

Severity: Minor Warning

Rationale: User Viewable Errors

17.1.247 Saf Agent Discarding Messages

Description: SAF is discarding messages causing message loss.

Severity: Critical

Rationale: Administration

17.1.248 Saf Agent Discarding Messages (Upgrade)

Description: SAF is discarding messages causing message loss.This problem, described in Oracle Bug 8964001, has been fixed in Oracle WebLogic Server 10.3 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.1.249 Saf Sometimes Stops Forwarding Messages When Receiving Server Is Restarted

Description: SAF sometimes stops forwarding messages when the receiving server(s) are restarted.

Severity: Minor Warning

Rationale: Administration

17.1.250 Saf Sometimes Stops Forwarding Messages When Receiving Server Is Restarted (Upgrade)

Description: SAF sometimes stops forwarding messages when the receiving server(s) are restarted.This problem, described in Oracle Bug 8118031, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3.

Severity: Minor Warning

Rationale: Administration

17.1.251 Sip Servlet In Conjunction With Commonj Is Failing

Description: When generating SNMP Traps from a SIP Servlet using SipServletSnmpTrapRuntimeMBean in conjunction with CommonJ timers, the traps fail with NullPointerExceptions. Without CommonJ timers, the traps work as expected.

Severity: Warning

Rationale: User Viewable Errors

17.1.252 Ssl Socket Connection Timeout Support For Out-Of-The-Box Jvm

Description: This is required to support SSL socket connection timeout using out-of-the-box (JRockit) JVM.

Severity: Warning

Rationale: Non-User Viewable Errors

17.1.253 Ssl Socket Connection Timeout Support For Out-Of-The-Box Jvm (Upgrade)

Description: This is required to support SSL socket connection timeout using out-of-the-box (JRockit) JVM.This problem, described in Oracle Bug 8183018, has been fixed in Oracle WebLogic Server 10.3 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Non-User Viewable Errors

17.1.254 Ssl Incompatibility When Upgrading To Jdk Version 1.6.0_14 And 1.5.0_19

Description: Upgrading to the versions 1.6.0_14 and 1.5.0_19 of the Sun JDK or Oracle JRockit causes compatibility issues between Sun JDK and Oracle JRockit handling of SSL and Oracle WebLogic Server handling of SSL.

Severity: Critical

Rationale: Non-User Viewable Errors

17.1.255 Ssl Incompatibility When Upgrading To Jdk Version 1.6.0_14 And 1.5.0_19 (Wls V10.0)

Description: Upgrading to the versions 1.6.0_14 and 1.5.0_19 of the Sun JDK or Oracle JRockit causes compatibility issues between Sun JDK and Oracle JRockit handling of SSL and Oracle WebLogic Server handling of SSL.

Severity: Critical

Rationale: Non-User Viewable Errors

17.1.256 Server Hangs With All Execute Threads In Standby State

Description: Oracle WebLogic Server may hang with every execute thread in STANDBY state.Note that Minimum Thread Constraint is not applied..Every ExecuteThread become as following.."[STANDBY] ExecuteThread: '1' for queue: 'weblogic.kernel.Default(self-tuning)'" daemon prio=10 tid=0x017ad9b8 nid=0x32 in Object.wait()[0xbcd7f000..0xbcd7faf0] at java.lang.Object.wait(Native Method) - waiting on <0xd96795d8> (a weblogic.work.ExecuteThread) at

java.lang.Object.wait(Object.java:474) at weblogic.work.ExecuteThread.waitForRequest(ExecuteThread.java:156) - locked <0xd96795d8> (a weblogic.work.ExecuteThread) at weblogic.work.ExecuteThread.run(ExecuteThread.java:177)

Severity: Warning

Rationale: User Viewable Errors

17.1.257 Server Hangs With All Execute Threads In Standby State. (Upgrade)

Description: Oracle WebLogic Server may hang with every execute thread in STANDBY state.Note that Minimum Thread Constraint is not applied..Every ExecuteThread become as following.."[STANDBY] ExecuteThread: '1' for queue: 'weblogic.kernel.Default(self-tuning)'" daemon prio=10 tid=0x017ad9b8 nid=0x32 in Object.wait()[0xbcd7f000..0xbcd7faf0] at java.lang.Object.wait(Native Method) - waiting on <0xd96795d8> (a weblogic.work.ExecuteThread) at java.lang.Object.wait(Object.java:474) at weblogic.work.ExecuteThread.waitForRequest(ExecuteThread.java:156) - locked <0xd96795d8> (a weblogic.work.ExecuteThread) at weblogic.work.ExecuteThread.run(ExecuteThread.java:177)This problem, described in 8636905, has been fixed in Oracle WebLogic Server 10.3 Maintenance Pack 2.

Severity: Minor Warning

Rationale: User Viewable Errors

17.1.258 Session Bean With Credentials Passed In A Foreign Jms Server Setup Gives Null Pointer Exception

Description: With a configuration of a Foreign JMS Server between two Oracle WebLogic Server domains (Oracle WebLogic Server 10.0) and a Session Bean with wrapper class deployed, when trying to send messages, a java.lang.NullPointerException is thrown.

Severity: Warning

Rationale: Development

17.1.259 Sessioncookie Name Is Not The Default Jsessionid On Application Deployed To A Cluster

Description: A web application is deployed to a cluster, and the session cookie has been modified from the default (JSESSIONID). If the application is being accessed by means of a webserver running the Oracle WebLogic plugin, and the configuration has not been updated, the plugin may route Oracle WebLogic Server requests incorrectly.

Severity: Minor Warning

Rationale: Administration

17.1.260 Sessions Get Lost After Configuring Saml With Two Domains

Description: Sessions are lost after configuring SAML with two domains (Oracle WebLogic Server 10.0) running on one system.It is a SAML requirement to set all Web application cookie names to the default (JSESSIONID). With this setting, the client browser can differentiate cookies originating from different domains only if the IPAddress or hostname of the SAML source and destination domain are not the same.

Severity: Critical

Rationale: User Viewable Errors

17.1.261 Shrinking Not Disabled Whenever Shrink Frequency Is Set To Zero (Wls V10)

Description: Setting shrink frequency seconds to 0 failed to disable connection pool shrinking. Turning shrinking off did not take effect until restart. This has been fixed.

Severity: Minor Warning

Rationale: Administration

17.1.262 Shrinking Not Disabled Whenever Shrink Frequency Is Set To Zero. (Wls V10, Upgrade)

Description: Setting shrink frequency seconds to "0" failed to disable connection pool shrinking. Turning shrinking off did not take effect until reboot. This issue has been fixed.This problem, described in Oracle Bug 8173564, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.1.263 Solaris Os Has Problems With Default Threading Libraries

Description: When starting Oracle WebLogic Server on Solaris 8 or 5.8, the default threading libraries of the operating system may cause various JVM threading issues, which can ultimately result in the server hanging or crashing.

Severity: Critical

Rationale: Server Outage

17.1.264 Some Signatures Require That Sessionmonitoring Be Enabled

Description: Some signatures require runtime MBeans to be created for Session Monitoring, in order to collect MBean data. If Session Monitoring is not enabled, data collection may be erratic or incomplete.

Severity: Minor Warning

Rationale: Non-User Viewable Errors

17.1.265 Specifying Precompile-Continue=True Is Not Working As Expected

Description: The specification "precompile-continue=true" does not function.If you specify the following: <precompile>true</precompile> <precompile-continue>true</precompile-continue>the application should continue to compile and deploy, even if compilation errors exist in the .jsp files. However, the actual behavior is as if "precompile-continue" was not specified. Errors are reported, and the application is not deployed.

Severity: Minor Warning

Rationale: Administration

17.1.266 Standalone Weblogic.Jar Does Not Work For $Java Weblogic.Xxxx Commands

Description: In Oracle WebLogic Server 10.0, using the weblogic.jar in standalone mode to build ANT scripts fails. For instance, if you copy the weblogic.jar file to a separate location and then run the following command, it will fail:java -cp <classpath of weblogic.jar> weblogic.Deployer/ weblogic.version

Severity: Minor Warning

Rationale: Development

17.1.267 Sun Jdk 1.6 Is Not Supported For Oracle Weblogic Server 10.0

Description: When JDK 1.6 is used for Oracle WebLogic Server 10.0, java.rmi.UnmarshalException is thrown. This is because JDK 1.6 is not supported for Oracle WebLogic Server 10.0. Oracle recommends to revert to a supported JDK configuration based on your Operating System, as you might encounter unforeseen issues.

Severity: Minor Warning

Rationale: Administration

17.1.268 Sun Jdk Has Issues Performing Basic Date Handling Due To Changes In Dst Definitions

Description: Recent changes to the definition of US timezones to remove Daylight Savings Time (DST) awareness has broken basic functionality in date handling. The DateFormat parser uses the contents of String zoneStrings[][] in class DateFormatSymbols to identify the timezone based on the zone value in the input date string.For example, the zoneStrings[][] array defines "EST" before "America/ New_York" so sets the timezone for the parser to the now non-DST aware "EST" zone.This issue only affects sites using the these three-letter abbreviations of DST times zones denotations, which have been deprecated, and any of the following versions of the Sun JDK:* Sun JDK 1.6* Sun JDK 1.5.0_08 and later* Sun JDK 1.4.2_12 and later

Severity: Warning

Rationale: Not Complying with Specifications

17.1.269 Sybase Driver 12.5.1 Throws Exception On Getdatabasemajorversion Method

Description: In Oracle WebLogic Server 10.0, Sybase driver 12.5.1 throws exception on getDatabaseMajorVersion method, as follows:javax.ejb.EJBException: EJB Exception: : java.lang.AbstractMethodError:weblogic.jdbc.wrapper.DatabaseMetaData_COM_ibm _db2_jdbc_net_DB2DatabaseMetaData.getDatabaseMajorVersion()This means that the getDatabaseMajorVersion() method is not implemented in the Sybase driver com.sybase.jdbc2.jdbc.SybDriver.

Severity: Minor Warning

Rationale: Administration

17.1.270 System Properties May Not Have Been Passed In Correctly If A $ Is Found

Description: Typically, a dollar sign ("$") in the system properties indicates an attempt to reference an environment variable that has not been evaluated correctly. As a result, the property may not have the desired effect.

Severity: Warning

Rationale: Administration

17.1.271 System Properties May Not Have Been Passed In Correctly If A % Is Found

Description: Typically, a percent sign ("%") in the system properties indicates an attempt to reference an environment variable that has not been evaluated correctly. Therefore, the property may not be having the desired effect.

Severity: Warning

Rationale: Administration

17.1.272 The Appc Compiler Fails On Ejb3.0 Jar When The Size Of The Ejb Class File Is Large (>40 Kb) On Windows (Upgrade)

Description: When the appc compiler is run on an EJB 3.0 JAR file larger than 40kb, the following exception occurs:weblogic.ejb.container.compliance.ComplianceException: No EJBs found in the ejb-jar file 'server.jar'. Please ensure the ejb-jar contains EJB declarations via an ejb-jar.xml deployment descriptor or at least one class annotated with the @Stateless, @Stateful or @MessageDriven EJB annotation.This problem, described in Oracle Bug 8165618, has been fixed in Oracle WebLogic Server 10.3.

Severity: Minor Warning

Rationale: Development

17.1.273 The Appc Compiler Fails On Ejb3.0 Jar When The Size Of The Ejb Class File Is Large (>40Kb) On Windows

Description: When appc is run on an EJB 3.0 JAR file where the size of the class file is more than 40 KB, you get the following exception:weblogic.ejb.container.compliance.ComplianceException: No EJBs found in the ejb-jar file 'server.jar'. Please ensure the ejb-jar contains EJB declarations via an ejb-jar.xml deployment descriptor or at least one class annotated with the @Stateless, @Stateful or @MessageDriven EJB annotation.

Severity: Warning

Rationale: Development

17.1.274 The Appc Compiler Recompiles Jsps In Webapp Library Unnecessarily

Description: weblogic.appc recompiles most of the JSPs from a Web application library shipped with Oracle WebLogic Server, even though they were properly precompiled in the JAR file within /WEB-INF/lib/.The appc compiler should not recompile any of the JSPs that are precompiled even when the command is executed.

Severity: Minor Warning

Rationale: Administration

17.1.275 The Appc Compiler Recompiles Jsps In Webapp Library Unnecessarily (Upgrade)

Description: weblogic.appc recompiles most of the JSPs from a Web application library shipped with Oracle WebLogic Server, even though they were properly precompiled in the JAR file within WEB-INF/lib/.The appc compiler should not recompile any of the JSPs that are precompiled even when the command is executed.This problem, described in Oracle Bug 8158866, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.1.276 The Getmessagespendingcount And Getbytespendingcount Sometimes Return Negative Values

Description: The getMessagesPendingCount and getBytesPendingCount of the JMSDestinationRuntimeMBean sometimes return negative values. Consequently, the JMS pending message count (MessagesPendingCount) and pending bytes count (BytesPendingCount) attributes in the JMSDestinationRuntimeMBean are intermittently set to a negative value.

Severity: Minor Warning

Rationale: Administration

17.1.277 The Getmessagespendingcount And Getbytespendingcount Sometimes Return Negative Values (Upgrade)

Description: The getMessagesPendingCount and getBytesPendingCount of the JMSDestinationRuntimeMBean sometimes return negative values. Consequently, the JMS pending message count (MessagesPendingCount) and pending bytes count (BytesPendingCount) attributes in the JMSDestinationRuntimeMBean are intermittently set to a negative value.This problem, described in Oracle Bug 8128500, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.1.278 The Jsp:Usebean Body Gets Executed Even If The Named Javabean Already Exists In The Scope

Description: In JSP, when Java Beans are used:<jsp:useBean> body gets executed even if named JavaBean already exists in the scope.

Severity: Minor Warning

Rationale: Administration

17.1.279 The Jsp:Usebean Body Gets Executed Even If The Named Javabean Already Exists In The Scope. (Upgrade)

Description: In JSP, when Java Beans are used:<jsp:useBean> body gets executed even if named JavaBean already exists in the scope.This problem, described in Oracle Bug 8093561, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Administration

17.1.280 The Mayscript Attribute Of Jsp:Plugin Is Not Recognized By The Jsp Compiler

Description: The mayscript attribute of jsp:plugin is not recognized by the JSP compiler, causing the following error:weblogic.servlet.jsp.CompilationException: Failed to compile JSP /A/daemon.jsp daemon.jsp:12:3: This attribute is not recognized. mayscript='true'> ^ - - - -^ at weblogic.servlet.jsp.JavelinxJSPStub.compilePage(JavelinxJSPStub.java:298) at weblogic.servlet.jsp.JspStub.prepareServlet(JspStub.java:216) at weblogic.servlet.jsp.JspStub.prepareServlet(JspStub.java:165) at weblogic.servlet.internal.ServletStubImpl.execute(ServletStubImpl.java:235).....

Severity: Minor Warning

Rationale: Development

17.1.281 The Mayscript Attribute Of Jsp:Plugin Is Not Recognized By The Jsp Compiler (Upgrade)

Description: The mayscript attribute of jsp:plugin is not recognized by the JSP compiler, causing the following error:weblogic.servlet.jsp.CompilationException: Failed to compile JSP /A/daemon.jsp daemon.jsp:12:3: This attribute is not recognized. mayscript='true'> ^ - - - -^ at weblogic.servlet.jsp.JavelinxJSPStub.compilePage(JavelinxJSPStub.java:298) at weblogic.servlet.jsp.JspStub.prepareServlet(JspStub.java:216) at weblogic.servlet.jsp.JspStub.prepareServlet(JspStub.java:165) at weblogic.servlet.internal.ServletStubImpl.execute(ServletStubImpl.java:235).....This problem, described in Oracle Bug 8179188, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Development

17.1.282 Timed Out Exception Trying To Setmonitoredattributename For Snmpgaugemonitor

Description: The following stacktrace is obtained when trying to setMonitoredAttributeName for SNMPGaugeMonitor on Solaris platform:Caught java.lang.RuntimeException: Timed out waiting for completionjava.lang.RuntimeException: Timed out waiting for completion at weblogic.management.provider.internal.ActivateTaskImpl.waitForCompletion(ActivateTaskImpl.java:374) at weblogic.management.provider.internal.ActivateTaskImpl.waitForTaskCompletion(ActivateTaskImpl.java:349) ...

Severity: Warning

Rationale: Administration

17.1.283 Too Many Open Files Errors Can Be Remedied By Limiting The Number Of Open Sockets Allowed

Description: The "Too Many Open Files" error usually occurs after several concurrent users get a connection to the Server. Java opens many files in order to read in the

classes required to run your application. High volume applications can use a lot of file descriptors. This could lead to a lack of new file descriptors. Also, each new socket requires a descriptor. Clients and Servers communicate via TCP sockets. Each browser's HTTP request consumes TCP sockets when a connection is established to a Server. Limiting the number of open sockets allowed prevents your server from running out of file descriptors.

Severity: Warning

Rationale: Performance

17.1.284 Transaction Commit() Delay When Using Usertransaction With Jms Module

Description: A few transactions are delayed when the transactions commit using UserTransaction with JMS during a LoadRunner Test.This is a timing issue related to the endPoint in the request object. When this happens, Oracle WebLogic Server throws a java.rmi.server.ServerNotActiveException in the getClientEndPoint() in the ServerHelper class. This sometimes causes a stoppage of the startCommit() process in SubCoordinatorImpl class. And it commits only after the JTA timeout value. This happens between Oracle WebLogic Server instances on a cluster.

Severity: Warning

Rationale: Performance

17.1.285 Unable To Set Protocol Specific Max Message Size (Wls V10)

Description: MaxHTTPMessageSize, MaxT3MessageSize, and MaxCOMMessageSize are deprecated since Oracle WebLogic Server 8.1. Instead of using these protocol specific parameters, use separate network channels configured with a MaxMessageSize to limit the incoming messages.

Severity: Minor Warning

Rationale: Administration

17.1.286 Unable To Use Dependency Injection For Jsf Managed Bean To Inject Ejb

Description: In Oracle WebLogic Server 10.0, the Dependency Injection for JSF Managed Bean fails with the following warning:WARNING JSF1033: Resource injection is DISABLEDThis occurs when using @Resource annotation to inject an EJB 3.0 dependency.The same issue also occurs for JDBC resource injection.During deployment the following error may occur: "The DataSource gotten from ManagedBean is null"This means the DataSource is not injected into ManagedBean correctly.

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.1.287 Unable To Use Dependency Injection For Jsf Managed Bean To Inject Ejb. (Upgrade)

Description: In Oracle WebLogic Server 10.0, the Dependency Injection for JSF Managed Bean fails with the following warning:WARNING JSF1033: Resource injection is DISABLEDThis occurs when using @Resource annotation to inject EJB 3.0 dependency.Also, the same issue also occurs for JDBC resource injection.During deployment you will get something like: "The DataSource gotten from ManagedBean is null"This means the DataSource is not injected into ManagedBean correctly.This

problem, described in Oracle Bug 8112023, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.1.288 Uncaught Throwable Found In Processsockets Errors

Description: Uncaught Throwable found in processSockets Errors in the server log files, as follows:<Oct 2, 2007 2:13:44 PM MEST> <Error> <Socket> <su80sr716> <b1d_adm_v20_30748_su80sr716_server> <ExecuteThread: '8' for queue: 'weblogic.socket.Muxer'> <<Oracle WebLogic Server Kernel>> <> <> <1191327224287> <BEA-000405> <Uncaught Throwable in processSocketsjava.lang.NullPointerException.java.lang.NullPointerExceptionat weblogic.socket.MuxableSocketDiscriminator.dispatch(MuxableSocketDiscriminator.java:156)at weblogic.socket.SSLFilter.dispatch(SSLFilter.java:258)...

Severity: Minor Warning

Rationale: Development

17.1.289 Uncaught Throwable Found In Processsockets Errors. (Upgrade)

Description: Uncaught Throwable found in processSockets Errors in the server log files, as follows:<Oct 2, 2007 2:13:44 PM MEST> <Error> <Socket> <su80sr716> <b1d_adm_v20_30748_su80sr716_server> <ExecuteThread: '8' for queue: 'weblogic.socket.Muxer'> <<WLS Kernel>> <> <> <1191327224287> <BEA-000405> <Uncaught Throwable in processSocketsjava.lang.NullPointerException.java.lang.NullPointerExceptionat weblogic.socket.MuxableSocketDiscriminator.dispatch(MuxableSocketDiscriminator.java:156)...This problem, described in Oracle Bug 8128732, has been fixed in Oracle WebLogic Server 10.3.

Severity: Minor Warning

Rationale: Development

17.1.290 Under High Load, The Sybase Jdbc Connectionpool Becomes Disabled

Description: If you use a Sybase database with Oracle JRockit R27.1, R27.2, or R27.3, under high load the Sybase JDBC Connection Pool becomes disabled, with the following error:"java.sql.SQLException: JZ006: Caught IOException: java.io.IOException: JZ0EM: End of data."

Severity: Warning

Rationale: Subsystem Outage

17.1.291 Unsynccircularqueue$Fullqueueexception Occurs In Workmanager

Description: UnsyncCircularQueue$FullQueueException can occur in WorkManager, as shown in the following excerpt from the Oracle WebLogic Server Administration Server log:<Aug 1, 2008 7:08:59 PM EDT> <Critical> <WorkManager> <BEA-002911> <WorkManager weblogic.kernel.System failed to schedule a request due toweblogic.utils.UnsyncCircularQueue$FullQueueException: Queue exceed maximum capacity of: '65536' elements weblogic.utils.UnsyncCircularQueue $FullQueueException: Queue exceed maximum capacity of: '65536' elements at weblogic.utils.UnsyncCircularQueue.expandQueue(UnsyncCircularQueue.java:106) ...

Severity: Minor Warning

Rationale: Administration

17.1.292 Unsynccircularqueue$Fullqueueexception Occurs In Workmanager (Upgrade)

Description: UnsyncCircularQueue$FullQueueException can occur in WorkManager. The managed servers continue to run fine, but the Administration Server becomes unresponsive. Thread dumps showwaiting on condition [0xc2981000..0xc2981888] at weblogic.platform.SunVM.threadDump0(Native Method) - waiting to lock <0xd859c620> (a weblogic.platform.SunVM) ...Other threads waiting on the thread shown above, for example:waiting for monitor entry [0xc2b81000..0xc2b81788] at weblogic.timers.internal.TimerManagerImpl.complete(TimerManagerImpl.java:664) - waiting to lock <0xd9236db0> (a weblogic.timers.internal.TimerThread) ...This problem, described in Oracle Bug 8179406, has been fixed in Oracle WebLogic Server 10.3.

Severity: Minor Warning

Rationale: Administration

17.1.293 Users Created Via Pat On Managed Server With Defaultatn Is Not Replicated To Masterldap

Description: A new user created on a managed server for DefaultAuthenticator (Embedded LDAP) in Oracle WebLogic Portal 10.x via PAT will not be replicated to the Admin Server. The user information is lost after the managed server is restarted.Using master first for embedded LDAP generally would be a workaround. However, this makes the Admin Server a single point of failure for all LDAP requests and can lead to connection problems under load.

Severity: Warning

Rationale: Administration

17.1.294 Users Created Via Pat On Managed Server With Defaultatn Is Not Replicated To Masterldap (Upgrade)

Description: Creating a new user for DefaultAuthenticator (Embedded LDAP) in Oracle WebLogic Portal 10.x via PAT on a managed server does not replicate this user to the admin server. After managed server restart, the user information is lost.Using master first for embedded LDAP generally would be a workaround. However, this makes the admin server a single point of failure for all LDAP requests and can lead to connection problems under load.This problem, described in Oracle Bug 8187790, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.1.295 Using Administration Console To Export/Import Large Jms Message Queue Causes Out Of Memory Error. (Wls V10)

Description: A system OutofMemory error can occur if you use Oracle WebLogic Server Administration Console to export or import a large JMS queue.

Severity: Critical

Rationale: Server Outage

17.1.296 Using The Post-Bind Option With Jrockit On Linux Causes Server Core Dump

Description: Attempting to start a server on a Linux platform when setting the post-bind option in a UNIX machine can cause the server to core dump with a StackOverflow exception.This applies to Oracle JRockit R26.2 and above.

Severity: Critical

Rationale: Administration

17.1.297 Verify That A File Being Opened As A Jra Recording Is A Jra Recording Before Opening It

Description: JRockit throws a divide by zero ArithmeticException when opening a file other than a JRA recording or a corrupted JRA recording. This issue has been fixed in JRockit R27.5.0. Here is an example error message:java.lang.ArithmeticException: / by zero at com.jrockit.jra.model.MemoryInfo.getAllocationFrequencySmallObjects(MemoryInfo.java:415) at com.jrockit.mc.jra.ui.general.GeneralContent.getFieldData(GeneralContent.java:129) at com.jrockit.mc.jra.ui.general.MiscSectionPart.createClient(MiscSectionPart.java:39) at com.jrockit.mc.jra.ui.sections.InfoSectionPart.initialize(InfoSectionPart.java:81) ...

Severity: Minor Warning

Rationale: Administration

17.1.298 Wlst Fails To Create A Second Remote Managed Server With Node Manager (Upgrade)

Description: If you use WLST (Oracle WebLogic Scripting Tool) to create managed servers, the first Managed Server is created and started successfully, but the second fails with a FileNotFoundException.....java.io.IOException: java.io.IOException: java.io.FileNotFoundException:/opt/u01/skurumel/remotedom/servers/domain_bak/config_bak/config.xml (No such file or directory) at java.io.FileOutputStream.open(Native Method) at java.io.FileOutputStream.<init>(FileOutputStream.java:179) at java.io.FileOutputStream.<init>(FileOutputStream.java:131) at weblogic.utils.FileUtils.writeToFile(FileUtils.java:114) .....This problem, described in Oracle Bug 8166242, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Development

17.1.299 Wlst Fails To Create A Second Remote Managed Server With Node Manager

Description: If you use WebLogic Scripting Tool to create Managed Servers, the first Managed Server is created and started successfully, but the second fails with a FileNotFoundException.....java.io.IOException: java.io.IOException: java.io.FileNotFoundException:/opt/u01/skurumel/remotedom/servers/domain_bak/config_bak/config.xml (No such file or directory) at java.io.FileOutputStream.open(Native Method) at java.io.FileOutputStream.<init>(FileOutputStream.java:179) at java.io.FileOutputStream.<init>(FileOutputStream.java:131) at weblogic.utils.FileUtils.writeToFile(FileUtils.java:114) .....

Severity: Warning

Rationale: Development

17.1.300 Wlst Offline Error When Managing Deliveryparamsoverrides For Jms Queues

Description: When using WebLogic Scripting Tool offline for managing DeliveryParamsOverrides parameter for JMS (Java Message Service) Queue, you encounter the following issue:When trying to cd() to existing delivery-params-overrides, the following exception occurs:Error: cd() failed. Do dumpStack() to see details.Problem invoking WLST - Traceback (innermost last): File "c:\support \repro.py", line 4, in ? File "C:\TEMP\WLSTOfflineIni27203.py", line 22, in cdcom.bea.plateng.domain.script.jython.WLSTException:com.bea.plateng.domain.script.ScriptException: No nested elementDeliveryParamsOverride is found...

Severity: Minor Warning

Rationale: Administration

17.1.301 Wlst Offline Error When Managing Deliveryparamsoverrides For Jms Queues (Upgrade)

Description: When using WLST (Oracle WebLogic Scripting Tool) offline for managing DeliveryParamsOverrides parameter for JMS (Java Message Service) Queue, you encounter the following issue. When trying to cd() to existing delivery-params-overrides, the following exception occurs:Traceback (innermost last): File "c:\support \repro.py", line 4, in ? File "C:\TEMP\WLSTOfflineIni27203.py", line 22, in cd ...The following command gives the error:cd('/JMSSystemResource/testJMSModule/JmsResource/NO_NAME_0/Queue/myq')This problem, Oracle Bug 8109003, is fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.1.302 Waitingforconnectionsuccesstotal Is Incorrect

Description: In the Oracle WebLogic Server console, the value of "Waiting For Connection Success Total" JDBC Connection pool monitoring is incorrect. Even when there are no waiters connection, "Waiting For Connection Success Total" count increases.

Severity: Minor Warning

Rationale: Administration

17.1.303 Waitingforconnectionsuccesstotal Is Incorrect. (Upgrade)

Description: In the Oracle WebLogic Server console, the value of "Waiting For Connection Success Total" JDBC Connection pool monitoring is incorrect. Even when there are no waiters connection, "Waiting For Connection Success Total" count increases.This problem, described in Oracle Bug 8125231, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.1.304 Web Service Classloading Performance Issue (Upgrade)

Description: Classloading inside the JWS Container object on every request results in huge bottleneck, effecting the performance.This problem, described in Oracle Bug 8176389, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.1.305 Webservice Class-Loading Performance Issue

Description: Classloading inside the JWS Container object on every request results in huge bottleneck, effecting the performance.

Severity: Warning

Rationale: Administration

17.1.306 Windows 2000 Sp2 And Higher Required For Oracle Jrockit 1.5_02 And 1.5_03

Description: Oracle JRockit 1.5_02 (R25.0.0) and Oracle JRockit 1.5_03 (R25.2.0) running on Windows 2000 requires Service Pack 2 or higher. This signature indicates that you are running no service pack or one less than Service Pack 2. Upgrade to Windows 2000 SP 2 or higher.

Severity: Critical

Rationale: Not Complying with Specifications

17.1.307 Windows 2000 Sp2 And Higher Required For Oracle Jrockit 1.4.2_03 Through 1.4.2_11 On X86

Description: Windows 2000 SP2 and higher is required for Oracle JRockit 1.4.2_03 through 1.4.2_11

Severity: Warning

Rationale: Not Complying with Specifications

17.1.308 Windows 2000 Sp4 And Higher Required For Oracle Jrockit 1.5_04 (R26.0.0) Through 1.5_06

Description: Windows 2000 SP4 and higher required for Oracle JRockit 1.5_04 through Oracle JRockit 1.5_06.

Severity: Critical

Rationale: Not Complying with Specifications

17.1.309 With Oracle Jrockit R27.3.0, Ctrl-C Can Cause Improper Shutdown And Loss Of Data

Description: If you are running on Linux or Solaris and press Ctrl-C to properly shut down your application, it will actually terminate immediately and you risk losing any runtime data that hasn't been saved to disk or a database. This happens because Oracle JRockit fails to register the SIGINT signal handler used for the shut down hooks.This issue does not apply to applications running on Windows.

Severity: Critical

Rationale: Administration

17.1.310 With Oracle Jrockit R27.4.0, Ldap Users Are Not Populated In Administration Console

Description: The users in the Administration Console (Security Realms > myrealm > Users and Groups) are not visible when Oracle JRockit R27.4.0 is used. However, this is not the case with previous Oracle JRockit versions.

Severity: Warning

Rationale: Administration

17.1.311 Xaer_Nota Occurs During Global Transaction

Description: Sometimes, XAER_NOTA occurs during processing of a global transaction.

Severity: Warning

Rationale: Administration

17.1.312 Findmonitordeadlockedthreads() Detects False Positive Java Deadlock

Description: When running Oracle JRockit R27.1.0 with the load environment, the JVM detects a false positive Java-level deadlock, as follows:[deadlocked thread] [ACTIVE] ExecuteThread: '334' for queue:'weblogic.kernel.Default (self-tuning)': -Thread '[ACTIVE] ExecuteThread: '334' for queue: 'weblogic.kernel.Default(self-tuning)'' is waiting to acquire lock'weblogic.messaging.kernel.internal.QueueImpl@43fbf06' that is held by thread'[ACTIVE] ExecuteThread: '334' for queue: 'weblogic.kernel.Default(self-tuning)''After this, the Server state is changed to FAILED. This thread is unblocked already in the next thread dump that is taken automatically by the core health monitoring system.

Severity: Warning

Rationale: Administration

17.1.313 Isconnected Method On Ssllayeredsocket Always Results In A Socket Not Connected

Description: Calls of isConnected on SSLLayeredSocket always results in a socket not connected indication. This is now fixed and isConnected returns the true connected state of the socket.

Severity: Warning

Rationale: Non-User Viewable Errors

17.1.314 Isconnected Method On Ssllayeredsocket Always Results In A Socket Not Connected (Upgrade)

Description: Calls of isConnected on SSLLayeredSocket always results in a socket not connected indication. This is now fixed and isConnected returns the true connected state of the socket.This problem, described in Oracle Bug 8187246, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Non-User Viewable Errors

17.1.315 Java.Lang.Classcastexception At Distributeddestinationimpl.Java In Oracle Jrockit R27.4.0

Description: With JRockit R27.4.0, when an Oracle WebLogic Server cluster peer attempts to synchronize with a peer, a java.lang.ClassCastException is raised in DistributedDestinationImpl.java, without a successful cluster peer synchronization.For example, the following stack trace excerpt occurred in an Oracle WebLogic Portal 8.1 Maintenance Pack 3 cluster domain with JRockit 142_15 (R27.4.0) and migratable JMS Servers configured for managed servers. During the start up of managed servers, the following exception was raised:...java.lang.ClassCastException: weblogic.rmi.internal.CBVOutputStream$CBVObjectOutputStream at weblogic.jms.common.DistributedDestinationImpl.writeExternal(DistributedDestinationImpl.java:328) at...

Severity: Warning

Rationale: Administration

17.1.316 Precompile-Continue=True Is Not Working As Expected (Upgrade)

Description: The specification "precompile-continue=true" does not function.If you specify the following: <precompile>true</precompile> <precompile-continue>true</precompile-continue>- the application should continue to compile and deploy, even when compilation errors exist in the .jsp files. However, the actual behavior is as if "precompile-continue" was not specified. Errors are reported, and the application does not deploy.This problem, described in Oracle Bug 8083879, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.1.317 Wlcompile On Ejb3.0 On Split Directory Environment Fails

Description: When using wlcompile and wlappc for the split directory environment, the build script is failing with the following error message:BUILD FAILEDbuild.xml: 45: weblogic.utils.compiler.ToolFailureException: No EJBs found in the ejb-jar file 'wlTestEjb'. Please ensure the ejb-jar contains EJB declarations via an ejb-jar.xml deployment descriptor or at least one class annotated with the @Stateless, @Stateful or @MessageDriven EJB annotation. at weblogic.ant.taskdefs.j2ee.CompilerTask.invokeMain(CompilerTask.java:299)...

Severity: Minor Warning

Rationale: Administration

17.1.318 Wlcompile On Ejb3.0 On Split Directory Environment Fails (Upgrade)

Description: When using wlcompile and wlappc for the split directory environment, the build script is failing with the following error message:BUILD FAILEDC:\projects \development\mves\wlTest\ant\build.xml:45: weblogic.utils.compiler.ToolFailureException: No EJBs found in the ejb-jar file 'wlTestEjb'. Please ensure the ejb-jar contains EJB declarations via an ejb-jar.xml deployment descriptor or at least one class annotated with the @Stateless, @Stateful or @MessageDriven EJB annotation. at

weblogic.ant.taskdefs.j2ee.CompilerTask.invokeMain(CompilerTask.java:299) at...This problem, described in Oracle Bug 8171601, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2

Severity: Minor Warning

Rationale: Administration

17.1.319 Wlfullclient.Jar Is Not Included In The Oracle Weblogic Server 10.X Installation

Description: A wlfullclient.jar file is not included in the Oracle WebLogic Server 10.0 and later installations.From Oracle WebLogic Server 10.0 onwards Oracle has stopped providing the wlfullclient.jar file.Oracle suggests you to use the Oracle WebLogic Server JarBuilder Tool Programming for Standalone Clients.Creating a wlfullclient.jar file for a client application:Use the following steps to create a wlfullclient.jar file for a clientapplication:1. Change directories to the server/lib directory.cd WL_HOME/server/lib2. Use the following command to create a wlfullclient.jar file in the server/lib directory:java -jar ../../../modules/com.bea.core.jarbuilder_1.0.0.0.jar3. Add the wlfullclient.jar file to the client application's classpath

Severity: Minor Warning

Rationale: Administration

17.2 All WLS V11 Rules (Deprecated)

The compliance rules for the All Wls V11 Rules standard follow.

17.2.1 Administration Server Is Hosting Applications Other Than Oracle System Applications

Description: Your Administration Server is hosting applications other than Oracle system applications. Oracle recommends hosting these applications only on the managed servers within your domain. The only applications that should be deployed to your Administration Server are Oracle applications (for example, the Oracle WebLogic Server Administration Console and Oracle agents).

Severity: Warning

Rationale: Administration

17.2.2 Administration Console Hangs During Restart Of A Remote Managed Server

Description: Cannot display the JNDI tree on the Oracle WebLogic Server console on a managed server. It seems that the problem is caused by an empty <jndi-name> tag, which was accidentally added in the datasource configuration file.<jdbc-data-source-params> <jndi-name>dsGestionRepresentations</jndi-name> <jndi-name></jndi-name><global-transactions-protocol>TwoPhaseCommit</global-transactions-protocol></jdbc-data-source-params>Will see a StackOverflowError in the logs as a symptom of this problem.

Severity: Critical

Rationale: Server Outage

17.2.3 After Several Hours And Over 100000 Incoming Requests The Bean Instance Goes Into Waiting

Description: A stateless session bean with max-beans-in-free-pool=1 and initial-beans-in-free-pool=1 is deployed on a cluster (consist of two managed servers).The reason for only having one instance in the pool is due to customer's application restrictions.After several hours and over 100000 incoming requests the bean instance goes into waiting state.Since there is only one bean in the pool, this effectively hangs all incoming calls.In the Oracle WebLogic Server admin console it shows 1 instance in the bean pool, 0 beans in use, and 1 waiting incoming request.This problems occurs 2-3 times every day, and the servers have to be restarted.

Severity: Warning

Rationale: Subsystem Outage

17.2.4 Annotation Does Not Work With Unchecked Exceptions

Description: For Oracle WebLogic Server 10.3 with EJB3.0, an ApplicationException occurs. Annotation does not work with unchecked exceptions.

Severity: Critical

Rationale: Server Outage

17.2.5 Annotation Does Not Work With Unchecked Exceptions (Upgrade)

Description: For Oracle WebLogic Server 10.3 with EJB3.0, an ApplicationException occurs. Annotation does not work with unchecked exceptions.This problem, described in Oracle Bug 8179501, has been fixed in Oracle WebLogic Server 10.3 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Server Outage

17.2.6 Async Topic Subscribers Not Receiving Messages

Description: JMS Uniform Distributed Topic does not behave as expected when upgrading from Oracle WebLogic Server 10.3.2 to 10.3.3. JMS Topic messages are not being delivered to clients if there is a Distributed JMS Topic, multiple subscribers with the same username are connected to the Topic, and the topic has a security constraint where only a particular user can receive the results.

Severity: Warning

Rationale: Development

17.2.7 Bea07-177.00 - Multiple Security Vulnerabilities In The Java Runtime Environment

Description: Contact Oracle Support or visit support.oracle.com for the following information:- A JavaDoc defect may lead to the generation of HTML documentation pages with potential cross-site scripting (XSS) vulnerability.- A buffer overflow vulnerability in the JRE image parsing code may allow an untrusted applet or application to elevate its privileges.- A vulnerability in the JRE font parsing code may allow an untrusted applet to elevate its privileges.- The Java XML Digital Signature implementation in JDK and JRE 6 does not securely process XSLT stylesheets in XSLT

Transforms in XML Signatures.- A JRE Applet Class Loader security vulnerability may allow an untrusted applet that is loaded from a remote system to circumvent network access.

Severity: Critical

Rationale: Administration

17.2.8 Bea07-178.00 - Java Secure Socket Extension Does Not Correctly Process Ssl/Tls Handshake

Description: The Java Secure Socket Extension (JSSE) that is included in various releases of the Java Runtime Environment does not correctly process SSL/TLS handshake requests. This vulnerability may be exploited to create a Denial of Service (DoS) condition to the system as a whole on a server that listens for SSL/TLS connections using JSSE for SSL/TLS support. For more information, please contact Oracle Support or visit support.oracle.com.This advisory corrects this issue by supplying patched versions of JRockit.

Severity: Critical

Rationale: Administration

17.2.9 Bea08-201.00 - Multiple Security Vulnerabilities In The Java Runtime Environment

Description: This is a combined security advisory. These vulnerabilities are fixed in JRockit R27.5.0. Installers, updates, patches and more information are available at support.oracle.com.

Severity: Critical

Rationale: Administration

17.2.10 Blocked Threads In Timermanagerimpl.Cancel()

Description: When using Oracle WebLogic Server 10.3 and load testing an application that uses Web Services and JMS, a deadlock occurs after several hours of load testing the application. Oracle WebLogic Server finally stops replying over HTTP.

Severity: Warning

Rationale: Subsystem Outage

17.2.11 Blocked Threads In Timermanagerimpl.Cancel() (Upgrade)

Description: When using Oracle WebLogic Server 10.3 and load testing an application that uses Webservices and JMS, a deadlock occurs after several hours of load testing the application. Oracle WebLogic Server eventually stops replying over HTTP.This problem, described in Oracle Bug 8445786, has been fixed in Oracle WebLogic Server 10.3 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Subsystem Outage

17.2.12 Boxing Conversion Of Small Integer Values Incorrect In Oracle Jrockit R27.2.X And R27.3.X

Description: The following Java class should produce TRUE for Integer values within the range(-128...+127). However, with Oracle JRockit releases R27.2.X and R27.3.X, this may return FALSE.public class Test { public static void main(String[] args) { Integer i1 = 4, i2 = 4; System.out.println(i1 == i2); }}

Severity: Minor Warning

Rationale: Development

17.2.13 Cve-2008-1006 - Multiple Security Vulnerabilities In Jrockit

Description: Advisory CVE-2009-1006 refers to all the vulnerability fixes that have been made in JRockit for addressing the applicable issues. The applicable advisories include:CVE 2008-5347CVE 2008-5348CVE 2008-5349CVE 2008-5350CVE 2008-5351CVE 2008-5352CVE 2008-5353CVE 2008-5354CVE 2008-5356CVE 2008-5360xFor more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.2.14 Cve-2008-3103 - Security Vulnerability In Java Management Extensions (Jmx)

Description: A vulnerability in the Java Management Extensions (JMX) management agent included in the Java Runtime Environment (JRE) may allow a JMX client running on a remote host to perform unauthorized operations on a system running JMX with local monitoring enabled.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.2.15 Cve-2008-3104 - Security Vulnerabilities In Java Runtime Environment Allows Same Origin

Description: Security vulnerabilities in the Java Runtime Environment may allow an untrusted applet that is loaded from a remote system to circumvent network access restrictions and establish socket connections to certain services running on machines other than the one that the applet was downloaded from. This may allow the untrusted remote applet the ability to exploit any security vulnerabilities existing in the services it has connected to.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.2.16 Cve-2008-3105 - Security Vulnerability In The Java Runtime Environment Related Xml Data

Description: A vulnerability in the Java Runtime Environment related to the processing of XML data may allow unauthorized access to certain URL resources (such as some files and web pages) or a Denial of Service (DoS) condition to be created

on the system running the JRE.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.2.17 Cve-2008-3106 - Security Vulnerability In The Java Runtime Environment Related To Xlm Data

Description: A vulnerability in the Java Runtime Environment with processing XML data may allow an untrusted applet or application that is downloaded from a website unauthorized access to certain URL resources (such as some files and web pages).For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.2.18 Cve-2008-3108 - A Security Vulnerability With The Processing Of Fonts In The Java Runtime

Description: A buffer overflow security vulnerability with the processing of fonts in the Java Runtime Environment (JRE) may allow an untrusted applet or application to elevate its privileges. For example, an untrusted applet may grant itself permissions to read and write local files or execute local applications that are accessible to the user running the untrusted applet.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.2.19 Cve-2008-3109 - Security Vulnerability In The Java Runtime Environment Scripting Language

Description: A vulnerability in the Java Runtime Environment relating to scripting language support may allow an untrusted applet or application to elevate its privileges. For example, an untrusted applet may grant itself permissions to read and write local files or execute local applications that are accessible to the user running the untrusted applet.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.2.20 Cve-2008-3110 - Security Vulnerability In The Java Runtime Environment Scripting Language

Description: A vulnerability in the Java Runtime Environment relating to scripting language support may allow an untrusted applet to access information from another applet.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.2.21 Cve-2008-4008 - Security Vulnerability In Weblogic Plug-In For Apache

Description: This vulnerability may impact the availability, confidentiality, or integrity of WebLogic Server applications which use the Apache web server configured with the WebLogic plug-in for Apache. This vulnerability may be remotely exploitable without authentication, that is, it may be exploited over a network without the need for a username and password.

Severity: Critical

Rationale: Administration

17.2.22 Cve-2008-4010 - Elevation Of Privilege Vulnerability In Some Netui Tags (Wls V10)

Description: This vulnerability in some NetUI tags may allow an attacker to read unauthorized data. This may be exploited over a network.

Severity: Critical

Rationale: Administration

17.2.23 Cve-2008-5457 - Security Vulnerability In Wls Plug-Ins For Apache, Sun, And Iis Web Server (Wls V10)

Description: This vulnerability may impact the availability, confidentiality or integrity of WebLogic Server applications, which use the Apache, Sun, or IIS web server configured with the WebLogic plug-in for Apache, Sun, or IIS, respectively. This vulnerability may be remotely exploitable without authentication, that is, it may be exploited over a network without the need for a username and password.

Severity: Critical

Rationale: Administration

17.2.24 Cve-2008-5459 - Security Policy Not Enforced For Wls Web Services

Description: Under certain circumstances security policies may not be enforced for web services.

Severity: Critical

Rationale: Administration

17.2.25 Cve-2008-5460 - Information Disclosure Vulnerability In Jsp And Servlets (Wls V10)

Description: Certain circumstances may cause some information disclosure in WebLogic Server JSPs and servlets.

Severity: Critical

Rationale: Subsystem Outage

17.2.26 Cve-2008-5461 - Elevation Of Privilege Vulnerability In Oracle Weblogic Console

Description: This vulnerability in Oracle WebLogic Console may allow information disclosure and elevation of privileges. This may be exploited over a network.

Severity: Critical

Rationale: Subsystem Outage

17.2.27 Cve-2008-5462 - Elevation Of Privilege Vulnerability In Weblogic Portal (Wls V10)

Description: This vulnerability in WebLogic Portal may allow elevation of privileges. This may be exploited over a network.

Severity: Critical

Rationale: Administration

17.2.28 Cve-2009-0217 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle JRockit R27.6.3 JRE/JDK 1.6.0_11. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.2.29 Cve-2009-0217 - Critical Patch Update Notice (Wls V10.3)

Description: Oracle has released Critical Patch Updates for July 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 10.3. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Server Outage

17.2.30 Cve-2009-1002 - Elevation Of Privilege Vulnerability In Weblogic Server (Wls V10)

Description: This vulnerability in WebLogic Server may allow elevation of privileges. This may be exploited over a network.

Severity: Critical

Rationale: Administration

17.2.31 Cve-2009-1003 - Source Code Access Vulnerability In Web Pages, Weblogic Server (Wls V10)

Description: This vulnerability in WebLogic Server may allow access to source code of web pages. This may be exploited over a network.

Severity: Critical

Rationale: Administration

17.2.32 Cve-2009-1004 - Strengthened?Weblogic Server Web Services Security

Description: WebLogic Server web services security was strengthened.

Severity: Critical

Rationale: Administration

17.2.33 Cve-2009-1012 - Security Vulnerability In Weblogic Plug-In For Apache Web Server

Description: This vulnerability may impact the availability, confidentiality, or integrity of WebLogic Server applications, which use the Apache, Sun, or IIS web server configured with the WebLogic plug-in for Apache, Sun, or IIS servers, respectively. This vulnerability may be remotely exploitable without authentication. That is. it may be exploited over a network without the need for a username and password.

Severity: Critical

Rationale: Administration

17.2.34 Cve-2009-1016 - Security Vulnerability In Oracle Weblogic Server Plug-Ins For Apache, Sun, And Iis Servers

Description: This vulnerability may impact the availability, confidentiality, or integrity of Oracle WebLogic Server applications, which use the Apache, Sun, or IIS web server configured with the WebLogic Server plug-ins for Apache, Sun, or IIS servers, respectively.

Severity: Critical

Rationale: Administration

17.2.35 Cve-2009-1094 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for July 2009 that provide corrective action for potential security vulnerabilities for Oracle JRockit R27.6.3 and earlier JRE and JDK 6, R27.6.3 and earlier JRE and JDK 5.0, R27.6.3 and earlier SDK and JRE 1.4.2. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.2.36 Cve-2009-1974 - Critical Patch Update Notice (Wls V10.3)

Description: Oracle has released Critical Patch Updates for July 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 10.3. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Server Outage

17.2.37 Cve-2009-1975 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for July 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 10.3. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Server Outage

17.2.38 Cve-2009-2002 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Portal 10.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.2.39 Cve-2009-2625 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle JRockit 1.5.0_19 and 1.6.0_14.Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.2.40 Cve-2009-3396 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.0, 9.1, and 9.2. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Server Outage

17.2.41 Cve-2009-3396 - Critical Patch Update Notice (Wls V10.3)

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 10.3. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Server Outage

17.2.42 Cve-2009-3403 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle JRockit 1.6.0_14, 1.5.0_19 and 1.4.2_21. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.2.43 Cve-2009-3555 - Critical Patch Update Notice (Wls V10.3)

Description: Oracle has released a Critical Patch Update that provides corrective action for a potential security vulnerability for Oracle WebLogic Server 10.3. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Development

17.2.44 Cve-2010-0068 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.2.45 Cve-2010-0069 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.2.46 Cve-2010-0069 - Critical Patch Update Notice (Wls V10.3)

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 10.3. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Development

17.2.47 Cve-2010-0073 - Critical Patch Update Notice (Wls V10.3)

Description: Oracle has released a Critical Patch Update that provides corrective action for a potential security vulnerability for Oracle WebLogic Server 10.3. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Development

17.2.48 Cve-2010-0074 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.2.49 Cve-2010-0074 - Critical Patch Update Notice (Wls V10.3)

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 10.3. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Development

17.2.50 Cve-2010-0078 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.2.51 Cve-2010-0078 - Critical Patch Update Notice (Wls V10.3)

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 10.3. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Development

17.2.52 Cve-2010-0079 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle JRockit 1.6.0_14, 1.5.0_19 and 1.4.2_21. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.2.53 Cve-2010-0849 - Critical Patch Update Notice

Description: Oracle has released a Critical Patch Update that provides corrective action for a potential security vulnerability for Oracle JRockit R27.6.6: JRE/JDK 1.4.2, 5 and 6; R28.0.0, JRE/JDK 5 and 6. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.2.54 Cve-2010-2375 - Critical Patch Update Notice (Wls V10.3)

Description: Oracle has released a Critical Patch Update that provides corrective action for a potential security vulnerability for Oracle WebLogic Server 10.3. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Development

17.2.55 Cacerts Do Not Work With Demotrust.Jks And Demoidentity.Jks

Description: Bad Certificate Error is thrown during NodeManager startup.Workaround or Apply patch: 1. Use JDK 1.6.0_12 or lower. 2. Copy cacerts from WL_HOME/server/lib directory to JDK_HOME/jre/lib/security/ Installers, updates, patches and more information are available at support.oracle.com.

Severity: Warning

Rationale: Not Complying with Specifications

17.2.56 Cacerts Do Not Work With Demotrust.Jks And Demoidentity.Jks (Wls V10.3, Upgrade)

Description: Bad Certificate Error is thrown during NodeManager startup.Workaround: 1. Use JDK 1.6.0_12 or lower. 2. Copy cacerts from WL_HOME/server/lib directory to JDK_HOME/jre/lib/security/This problem, described in Oracle Bug 8715553, has been fixed in Oracle WebLogic Server 10.3 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.2.57 Changes In Dst Definitions Cause Issues With Basic Date Handling In Oracle Jrockit Jdk

Description: The recent change to the definition of US timezones to remove Daylight Savings Time (DST) awareness has broken basic functionality in date handling in multiple vendor JVMs, including Oracle JRockit 1.4.2_12. This issue affects sites using the three letter abbreviations for the deprecated DST timezone denotations, when using any affected JVM.The DateFormat parser uses the contents of String zoneStrings[][] in class DateFormatSymbols to identify the timezone based on the zone value in the input date string. For example, the zoneStrings[][] array defines "EST" before "America/New_York" and so sets the timezone for the parser to the EST zone, which is now unaware of DST.

Severity: Warning

Rationale: Not Complying with Specifications

17.2.58 Changes In Dst Definitions Cause Issues With Basic Date Handling In Oracle Jrockit Jdk

Description: The recent change to the definition of US timezones to remove Daylight Savings Time (DST) awareness has broken basic functionality in date handling in multiple vendor JVMs, including Oracle JRockit 1.5.0_08. This issue only affects sites using three-letter abbreviations of DST times zones denotations, which have been deprecated, and any affected JVM.The DateFormat parser uses the contents of String zoneStrings[][] in class DateFormatSymbols to identify the timezone based on the zone value in the input date string.The bug will only have an impact if and only if the application is using the deprecated denotation of three-letter abbreviations for US timezones (for example, EST, MST, or HST).

Severity: Warning

Rationale: Not Complying with Specifications

17.2.59 Cluster Has No Frontendhost Server Specified

Description: A cluster has the Oracle WebLogic Plugin enabled, but the FrontEndHost server setting has not been specified. Oracle WebLogic Server uses this setting to specify the host for HTTP responses. If no FrontEndHost server has been specified, Oracle WebLogic Server uses the hostname of the server that processed the request.

Severity: Warning

Rationale: Non-User Viewable Errors

17.2.60 Compaction(S) Aborted Due To Counters Do Not Reset Between Each Garbage Collection

Description: Compaction of objects is the process of moving objects closer to each other in the heap, thus reducing the fragmentation and making object allocation easier for the JVM. Oracle JRockit compacts a part of the heap at each garbage collection (or old collection, if the garbage collector is generational).It has been observed in Oracle JRockit releases R27.3.1 and R27.4.0 that the compaction is being aborted when it should not be aborted due to the counter not being set to 0 between Garbage Collections.In some cases, the counter will continue to increase until it grows too large, leading to an aborted compaction. Since it is not set to 0, all the following Garbage Collections will be aborted as well.

Severity: Warning

Rationale: Performance

17.2.61 Connection Pool Performance May Be Degraded Due To The Test Settings That Are Specified

Description: A connection pool has been set up to perform all of the following tests:* TestOnCreate* TestOnReserve* TestOnReleaseAs a result of enabling all three of these settings, the connection will be tested when it is retrieved from the pool and then again when it is put back into the pool. This can lead to performance issues in JDBC access code.

Severity: Minor Warning

Rationale: Performance

17.2.62 Console Shows Wrong Config Values If Production Mode Is Enabled/Disabled From Command Line

Description: When Production Mode is enabled or disabled with the command line option "-Dweblogic.ProductionModeEnabled=[true

Severity: false]" but the setting does not agree with the config.xml "ProductionMode" setting, the Adminstration Console may show incorrect values for some configuration options. This can occur for any configuration options for which the default values for production mode differ from the default values for development mode.Note: Command line overrides are not persisted in config.xml. The Administration Console shows the configuration attribute values and defaults that correspond to the persisted version in the config.xml file.

Rationale: Warning

17.2.63 Consumers Not Recreated After Server Is Rebooted

Description: When a Message Driven Bean (MDB) is deployed on a multiserver domain and is listening on a distributed queue, and the MDB is configured to connect to all of the distributed queue members. However, if a remote distributed queue member server is restarted, the deployed MDB server does not reconnect with the remote distributed queue member server.

Severity: Warning

Rationale: Subsystem Outage

17.2.64 Crashes In Conjunction With A Native Library

Description: If you are using Oracle JRockit in conjunction with a native library that relies on OS signals you may experience crashes due to a signal handling conflict between Oracle JRockit and the native library.Dump stack matches known issue:Thread Stack Trace: at pthread_kill+62()@0xb75c00ee at ptSendSignal +34()@0xb71aedc6 at trapiConvertToDeferredSigsegv+199()@0xb719d207 at trapiSigSegvHandler+40()@0xb719d23c at xehInterpretSavedSigaction +219(amqxerrx.c)@0xb72f276b at xehExceptionHandler+543()@0xb72f2b3f at __libc_sigaction+272()@0xb75c2f80Oracle Engineering found this conflict using IBM's MQSeries native drivers, and it may be present in other libraries that rely on native code.

Severity: Critical

Rationale: Server Outage

17.2.65 Deadlock Occurs In Oracle Weblogic Server (Wls V10.3)

Description: Java level deadlock between weblogic.deployment.jms.JMSSessionPoolTester and weblogic.deployment.jms.JMSSessionPool reveal in Oracle WebLogic Server Thread dump.

Severity: Critical

Rationale: Server Outage

17.2.66 Deadlock Occurs In Oracle Weblogic Server (Wls V10.3, Upgrade)

Description: Java level deadlock between weblogic.deployment.jms.JMSSessionPoolTester and weblogic.deployment.jms.JMSSessionPool reveal in Oracle WebLogic Server Thread dump. Java stack information: ========== "[ACTIVE] ExecuteThread: '46' for queue: 'weblogic.kernel.Default (self-tuning)'": at weblogic.deployment.jms.JMSSessionPoolTester.run(JMSSessionPoolTester.java:515) - waiting to lock <0x07dca908> (a weblogic.deployment.jms.JMSSessionPoolTester) - locked < 0x07bfe8e0> (a weblogic.deployment.jms.JMSSessionPool) at weblogic.work.ExecuteThread.execute(ExecuteThread.java:201) at weblogic.work.ExecuteThread.run(ExecuteThread.java:173) "[ACTIVE] ExecuteThread: '45' for queue:

Severity: Minor Warning

Rationale: Server Outage

17.2.67 Document Style Operation Must Not Have A Non-Header Inout Or Out Parameter

Description: When generating a webservice using JAX-RPC 1.1 with document style from a Web Service Definition Language (WSDL) file, the customer is getting the following error: [jwsc] [ERROR] - A document style operation must not have a non header INOUT or OUT Parameter.

Severity: Critical

Rationale: Development

17.2.68 Document Style Operation Must Not Have A Non-Header Inout Or Out Parameter (Upgrade)

Description: When generating a webservice using JAX-RPC 1.1 with document style from a Web Service Definition Language (WSDL) file, you may see the following error: [jwsc] [ERROR] - A document style operation must not have a non header INOUT or OUT Parameter.This problem, described in Oracle Bug 9340163, has been fixed in Oracle WebLogic Server 10.3 Maintenance Pack 3.

Severity: Minor Warning

Rationale: Development

17.2.69 Dweblogic.Management.Nologsystemproperties=True Has No Effect

Description: In Oracle WebLogic Server 8.1 Maintenance Pack 5, it was possible to disable the writing of system properties to the Oracle WebLogic Server log file by using the -Dweblogic.management.noLogSystemProperties=true parameter.However, after upgrading to Oracle WebLogic Server 9.x, this setting no longer has any effect.

Severity: Minor Warning

Rationale: Performance

17.2.70 Dynamic Wsdl Host Address Incorrect When Deployed In A Cluster

Description: An incorrect dynamic Web Service Definition Language (WSDL) location address is generated when a Web service is deployed on a cluster with multiple front-end hosts and ports. A new property, weblogic.wsee.useRequestHost, has been introduced in Oracle WebLogic Server 9.2.1 that allows generation of the WSDL location address either from the host header or by following the topology design.

Severity: Minor Warning

Rationale: Administration

17.2.71 Ejb3 Web Service Fails To Compile When Using Static Nested Class

Description: Problem Statement: EJB3 Web Service fails to compile when using static nested class.Issue Clarification: A stateless EJB3 annotated as a JAX-WS Web Service fails to compile when using a static nested class as a parameter. 1. user-defined data that contains static nested class public class Outer { public static class Inner { } } 2. stateless EJB3 annotated JAX-WS Web service @Stateless @WebService(name = "Simple", portName = "SimpleEJBPort", serviceName = "SimpleEjbService", targetNamespace = "http://www.bea.com/wls/samples") public class SimpleEjbImpl { public String sayHello(Outer.Inner inner) { return "Hello"; } }

Severity: Minor Warning

Rationale: Development

17.2.72 Eager Refresh Of Entity Bean To Refresh Entity Cache

Description: If it has to refresh both the query cache and entity cache, Eager Refresh of Read-Only Entity Beans takes a long time. Eager refresh initiated by the container can restrict the refresh to only the entity cache, and the query cache will get updated only when the normal application executes the query in its code path.

Severity: Minor Warning

Rationale: Performance

17.2.73 Ejbhomequery Causes Nullpointerexception In Cachekey

Description: ejbHomeQuery causes NullPointerException in the EJB container.

Severity: Minor Warning

Rationale: Administration

17.2.74 Ejbhomequery Causes Nullpointerexception In Cachekey (Upgrade)

Description: ejbHomeQuery causes NullPointerException in the EJB container.This problem, described in Oracle Bug 8115318, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3.

Severity: Minor Warning

Rationale: Administration

17.2.75 Enabling Oracle Weblogic Tuxedo Connector Debug Shows Info Messages

Description: Enabling Oracle WebLogic Tuxedo Connector Debug shows "DEBUG" messages as info in the logs rather than "DEBUG" even after setting log severity to DEBUG.

Severity: Warning

Rationale: Administration

17.2.76 End-Of-Support Announcement For Microsoft Windows 2000 Server

Description: As of June 30, 2005, Microsoft has announced the end of mainstream support for the following platforms:* Windows 2000 Server* Advanced Server* Datacenter ServerOracle will continue supporting Oracle applications (for example Oracle JRockit on these platforms) at least through December 2006. A final notice of the end of support for Oracle JRockit on Windows 2000 will appear at least 12 months before the actual end of support.Note: Support for any Windows-specific issues must addressed by Microsoft via their extended support services.

Severity: Warning

Rationale: Not Complying with Specifications

17.2.77 End-Of-Support Announcement For Red Hat Enterprise Linux 2.1

Description: Oracle stopped supporting Red Hat Linux 2.1 on April 30, 2006.

Severity: Warning

Rationale: Not Complying with Specifications

17.2.78 Enhancement To Disable Passivation/Activation During Sfsb Replication In Cluster

Description: Enhancement to add deployment descriptor to turn off passivation/ activation during replication of Stateful Session Bean (SFSB) in cluster.A new flag <passivate-during-replication> is added to weblogic-ejb-jar.xml. This flag is part of <stateful-session-descriptor> as below:<!ELEMENT stateful-session-clustering (home-is-clusterable?, home-load-algorithm?, home-call-router-class-name?, use-serverside-

stubs?, replication-type?, passivate-during-replication?)>Set the flag to 'false' to avoid passivation/activation during SFSB replication. The default value for the flag is 'true'.

Severity: Minor Warning

Rationale: Administration

17.2.79 Entity Bean Creation With Primary Key Of Sequence Generator Int Type Fails In A Global Tx

Description: When a new Entity bean has been created with a primary key ID of sequence generator int type, attempts to persist this bean as part of a global transaction will fail with a javax.ejb.EJBException if a nontransactional datasource is used.No issues will be encountered if the annotation is removed from the Primary Key value, or if the uid-string generator is used and the field type changed to String.

Severity: Minor Warning

Rationale: User Viewable Errors

17.2.80 Failure In A Class Preprocessing Recursive Calls In Oracle Jrockit R27.X

Description: In Oracle JRockit R27.1, the class bytes preprocessing facility was changed to allow for recursive preprocessing. This meant that a class preprocessor instance that was currently doing class preprocessing and through this caused a new class to be loaded would be recursively called with the new class bytes. This caused failures in some existing preprocessor implementations that relied on the old behavior of JRockit R27.1. In Oracle JRockit R27.5, this has been reverted. A thread doing class preprocessing will now silently refuse to preprocess any types created by executing the preprocessor itself.For example, in Oracle SOA Manager (ALSM), the error "Nanoagents not loading" occurs when used with Oracle JRockit R27.3.1.

Severity: Warning

Rationale: Subsystem Outage

17.2.81 Foreign-Connection-Factory Credentials Are Not Taken To Account If Provider-Url Specified

Description: JMS proxy using local foreign JMS server configuration with credentials given is not able to connect to the remote system.

Severity: Warning

Rationale: Subsystem Outage

17.2.82 Getting 'Nullpointerexception' When Running The Servlet As A Beehive Control

Description: When you insert the control manually, you get a 'nullPointerException' when running the servlet.In Oracle Workshop for WebLogic 10.0 there is no direct procedure to call a control from a Java class, but there are the workarounds available. See the Remedy section.

Severity: Minor Warning

Rationale: Development

17.2.83 Global Multicast Address Has Cluster Jndi Replication Issues

Description: Using global multicast addresses between 230.0.0.1 and 239.192.0.0 causes cluster issues. For example, the JMS destination may not replicate to all members of the cluster although the JNDINameReplicated attribute is set to "true."

Severity: Warning

Rationale: Administration

17.2.84 Group Circular Reference In External Authenticator Causes Ldap To Hang

Description: By default, Oracle WebLogic Server does not check for Group circularity for any externally configured LDAP Authenticators (iPlanet, Active Directory, Novell, Open LDAP, etc.).Circular reference:Group A is a member of Group BGroup B is a member of Group AWhen a group circularity exists in the backend LDAP, so many LDAP connections are created (due to the backend LDAP group having itself as a member), that a server crash can result.

Severity: Minor Warning

Rationale: Subsystem Outage

17.2.85 Http Post Method Can Be Tuned Via Maxpostsize To Harden Security

Description: A denial-of-service attack is a malicious attempt to overload a server by sending more requests than it can handle, preventing access to a service. Attackers may overload the server by sending huge amounts of data in an HTTP POST method. The client can get an HTTP error code 413 (Request Entity Too Large) or the connection may be broken.Prevent this type of attack by setting the MaxPostSize parameter. This limits the number of bytes of data that can be received in a POST from a single request. (By default, the value for MaxPostSize is -1, i.e. unlimited.) If an attacker sends an HTTP POST that exceeds the limit you specify, it triggers a MaxPostSizeExceeded exception and the server logs a "POST size exceeded the parameter MaxPostSize" message.

Severity: Critical

Rationale: Server Outage

17.2.86 Hibernate And Ehcache Cache Locking Problem With Multiple Managed Servers On Same Server

Description: When Hibernate and ehcache are used with Oracle WebLogic Server, the ehcache component writes cached objects to the file system defined by the property java.io.tmpDir. This, in itself, is not an issue. However, when there are two or more managed servers running on each physical server, these managed servers write to the same directory in the file system using the same file names. Consequently, the servers are sharing resources that require explicit locks in order to modify the files, which can result in a deadlock condition.

Severity: Critical

Rationale: Administration

17.2.87 Ibm Jdk 64 Bit Is Not Supported By All Versions Of Oracle Weblogic Server

Description: IBM JDK 64 bit is not supported for all versions of Oracle WebLogic Server. Oracle will provide support to the best of its ability. You may be advised to revert to a supported JVM configuration if you encounter an Oracle issue that appears to be JVM-related.

Severity: Warning

Rationale: Administration

17.2.88 If Weblogic_Patch.Jar Is After Weblogic.Jar The Installed Patches Have No Effect

Description: Some customers write their own startup and environment scripts. Sometimes they invert the CLASSPATH order. When this occurs, patches applied with BSU are not active even if Oracle Enterprise Manager detects them. The weblogic_patch.jar must always come before weblogic_sp.jar and weblogic.jar in the classpath.

Severity: Critical

Rationale: Administration

17.2.89 Increased Garbage Collection Time In Oracle Jrockit R27.1.X And R27.2.X

Description: In rare cases, external compaction can cause very long pause times when attempting to move a large object from the highest heap parts, if the heap is fragmented.

Severity: Warning

Rationale: Performance

17.2.90 Inner Classes Are Public Local Variable, Resulting In Wrong Types Definition In Wsdl

Description: When a Web Service uses inner classes as data types to a web method the resulting types are incorrect in the Web Service Definition Language (WSDL) produced by JWSC.

Severity: Critical

Rationale: Server Outage

17.2.91 Jax-Ws Under Load Throws Java.Util.Nosuchelementexception

Description: Customers reported NoSuchElementException under load for jaxws client with SAML configurations. The problem is resolved now, by isolating the critical section and synchronizing the same to avoid this problem.

Severity: Minor Warning

Rationale: Administration

17.2.92 Jax-Ws Under Load Throws Java.Util.Nosuchelementexception (Upgrade)

Description: A NoSuchElementException error has been reported under load for jaxws client with SAML configurations. The problem is resolved now by isolating the

critical section and synchronizing the same to avoid this problem.This problem, described in Oracle Bug 8183459, has been fixed in Oracle WebLogic Server 10.3 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Administration

17.2.93 Jms Server'S Runtime Monitoring View Does Not Work After Migration

Description: After a JMS server was auto-migrated to a non-user preferred server, the JMS server's runtime monitoring view in the Admin console does not work correctly. The "does not work correctly" message means there are no destinations in the "Active Destinations" even if destinations exist.

Severity: Warning

Rationale: Administration

17.2.94 Jms Producer Memory Leak

Description: JMS producer leaks memory when the producer is repeatedly created and closed while the session remains open.

Severity: Minor Warning

Rationale: Administration

17.2.95 Jms Producer Memory Leak (Upgrade)

Description: JMS producer leaks memory when the producer is repeatedly created and closed while the session remains open.This problem, described in Oracle Bug 8108465, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.2.96 Jms Producer Memory Leak (Upgrade)

Description: JMS producer leaks memory when the producer is repeatedly created and closed while the session remains open.This problem, described in Oracle Bug 8108465, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.2.97 Jms Server Byteshighcount Is Greater Than 50 Percent Of Jvm Heapsizecurrent

Description: When the JMS Server's BytesHighCount attribute is greater than 50 percent of the JVM's HeapSizeCurrent, and the BytesPagingEnabled and MessagesPagingEnabled attributes are not set, a JMS processing error may have occured or may occur in the future.

Severity: Critical

Rationale: Server Outage

17.2.98 Jrockit 1.4.2_08 Crashes When Calling Remote Web Services, Causing Null Pointer Exception

Description: A crash can occur in Oracle JRockit 1.4.2_0 when calling remote web services, causing a NullPointerException in the native code.The following is an example thread stack trace: - - - - - - - - - -Error code: 52Error Message: Null pointer exception in native codeSignal info : si_signo=11, si_code=2 - - - - - - - - - -Thread Stack Trace: at org/apache/axis/message/MessageElement.addTextNode(MessageElement.java:1388)@0xa77c3ae0 at org/apache/axis/message/SOAPHandler.addTextNode(SOAPHandler.java:148)@0xa77ea0d6 at org/apache/axis/message/SOAPHandler.endElement(SOAPHandler.java:112)@0xa77ea8ed at org/apache/axis/encoding/DeserializationContext.endElement(DeserializationContext.java:1087)@0xa77ea468

Severity: Warning

Rationale: Administration

17.2.99 Jrockit 1.5.0_08 R27.1.0 - Jrockit Does Not Calculate Date Correctly

Description: Application Java Byte code produces wrong date when it is compiled with Oracle JRockit 1.5.0_08 R27.1.0For example when using java.util.Calendar:calendar.set(Calendar.MONTH, (calendar.get(Calendar.MONTH) - 1));and when we print Calendar.getTime() the wrong value for month is returned.System.out.println("DATE: " + calendar.getTime());

Severity: Warning

Rationale: Development

17.2.100 Jrockit R27 - Exception Occurs For Servers > Monitoring > Performance Tab In Administration Console. (Upgrade)

Description: An exception can occur in the Oracle WebLogic Server 10.0 Administration Console when you click the Servers - Monitoring tab - Performance tab. This issue occurs only if you are using JRockit R27.3, R27.4, R27.5, or R27.6.The following exceptions may occur:Error opening /jsp/core/server/ServerMonitoringPerformanceForm.jsp.The source of this error is javax.servlet.ServletException: javax.xml.transform.TransformerException:com.sun.org.apache.xml.internal.utils.WrappedRuntimeException:The entity name must immediately follow the '&' in the entity reference.at weblogic.servlet.jsp.PageContextImpl.handlePageExceptionThis problem, described in Oracle Bug 8116840, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Administration

17.2.101 Jrockit R27 - Exception Occurs For Servers>Monitoring>Performance Tab In Admin Console

Description: An exception can occur in the Oracle WebLogic Server 10.0 Administration Console when you click the Servers - Monitoring tab - Performance tab. This issue occurs only if you are using JRockit R27.3, R27.4, R27.5, or R27.6.The

following exceptions may occur:Error opening /jsp/core/server/ServerMonitoringPerformanceForm.jsp.The source of this error is javax.servlet.ServletException: javax.xml.transform.TransformerException:com.sun.org.apache.xml.internal.utils.WrappedRuntimeException:The entity name must immediately follow the '&' in the entity reference.at weblogic.servlet.jsp.PageContextImpl.handlePageException

Severity: Warning

Rationale: Administration

17.2.102 Jrockit R27.1.0 - Heap Snapshot Table Cannot Be Configured

Description: The Heap Snapshot table on the Heap Overview tab appears to be configurable, but is not.

Severity: Minor Warning

Rationale: Administration

17.2.103 Jrockit R27.1.0 - Memory Usage And Optimization Data Cannot Be Copied To Clipboard

Description: The Memory Usage data on the General tab and the Optimization data on the Optimization tab of JRockit Mission Control's JRA window cannot be copied to the clipboard using the right click context menu. This works for the other data fields in JRockit Mission Control.

Severity: Minor Warning

Rationale: Administration

17.2.104 Jrockit-R26.4.0 Crashes When A Java Application Has Inline Calculation In The Array

Description: When a Java application that has inline calculation in the array access is deployed on a Oracle WebLogic Server with Oracle JRockit R26.4.0-JDK1.5.0_06, a crash can occur.The error message is as follows:Error Message: Illegal memory access. [54]Signal info : si_signo=11, si_code=1

Severity: Warning

Rationale: Administration

17.2.105 Jsf Backbean/Ejb3 Statelessbean Cannot Inject Dependency Correctly

Description: 1. If you create two faces-config.xml files for a Web application2. Each faces-config.xml file registers one managed bean classWhere:Each managed bean class has a method that injects a stateless EJB (Enterprise Java Bean) with a local interface (EJB 3.0).Result:You get an NPE (Null Pointer Exception) when you visit one of the faces (for example, h1.jsf), because the stateless EJB cannot be injected.

Severity: Warning

Rationale: Development

17.2.106 Jsf Backbean/Ejb3 Statelessbean Cannot Inject Dependency Correctly (Upgrade)

Description: If you create two 'faces-config.xml' files for a Web application, and each faces-config.xml file registers one managed bean class, each managed bean class has a method that injects a stateless EJB (Enterprise Java Bean) with a local interface (EJB 3.0), then you get an NPE (Null Pointer Exception) when you visit one of the faces (for example, h1.jsf), because the stateless EJB cannot be injected.This problem, described in Oracle Bug 8691274, has been fixed in Oracle WebLogic Server 10.3 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Development

17.2.107 Jvm 1.4.1_X Assertion Failed [Invalid Assignment From 'Object' To 'Object']

Description: The following error occurs when starting the managed server with 1.4.1_X JVM:"weblogic.utils.AssertionError: ***** ASSERTION FAILED *****[invalid assignment from 'Object' to 'Object'] at weblogic.utils.Debug.assertion(Debug.java: 57)"The managed server startup failures due to weblogic.utils.AssertionError is because of JVM HotSpot optimizations. This is a JVM issue.

Severity: Minor Warning

Rationale: Administration

17.2.108 Jvm Could Crash At Parallel Gc Run Oracle Jrockit R27.1, R27.2, R27.3

Description: A crash can happen while executing Oracle JRockit R27.X parallel garbage collection(-Xgc:parallel)objPoolMarkAllWeak function passes a null object to refResweepWeakHandle, giving a Tread Stack Trace as the following one: at refResweepWeakHandle+117()@0xb7d0f245 at objPoolMarkAllWeak +630()@0xb7ce03a6 ...This can be observed mostly using JVMTI agent.

Severity: Minor Warning

Rationale: Administration

17.2.109 Mdb Fails To Connect To Jms Destination When Using Global Work Manager

Description: Using globally scoped Work Manager in Oracle WebLogic Server 10.x and the dispatch-policy element of the WebLogic Enterprise bean in weblogic-ejb-jar.xml, the Message Driven Bean (MDB) fails to connect to the destination throwing:The Message-Driven EJB: WMTestMDB is unable to connect to the JMS destination: queue.cap.TestQueue. The Error was: java.lang.NegativeArraySizeException: allocArray>The error is:1. Seen when Maximum Threads Constraint Count = -1 (default value).2. NOT seen if application scoped work manager used.To avoid this problem, use:1. Application scoped work manager.2. A positive integer for Maximum Threads Constraint Count != -13. A global work manager, delete the Maximum Threads Constraint.

Severity: Minor Warning

Rationale: Administration

17.2.110 Managed Servers May Periodically Drop In And Out Of A Cluster When Running On Solaris 10

Description: When an Oracle WebLogic Server cluster has been configured on a Solaris 10 box(es), Managed Server instance(s) may periodically drop in and out of the cluster.Even though the server instances automatically rejoin the cluster, there will be lost multicast messages, and response time will be impacted due to the increased cluster housekeeping being required (for example, increased failover of requests or additional session replication needing to be carried out). This will then result in slower performance being seen by the end user/client.This issue is seen only on Solaris 10, regardless of the version of Oracle WebLogic Server being used.

Severity: Warning

Rationale: Performance

17.2.111 Message Bridge Does Not Forward Messages Until Restarted Again. (Upgrade)

Description: Message bridge does not forward messages after server restart via console until it (message bridge) is restarted again.This problem, described in Oracle Bug 8131966, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.2.112 Method Ejbtimout() In Superclass Not Recognized

Description: Method ejbTimout() in superclass is not recognized.java.lang.IllegalStateException: [EJB:011084]This EJB class does not support EJB timers and therefore is prohibited from using the TimerService.To use EJB timers, the bean class must implement javax.ejb.TimedObject or have a method annotated with @Timeout. at weblogic.ejb.container.internal.BaseEJBContext $1.invoke(BaseEJBContext.java:429)...

Severity: Minor Warning

Rationale: Development

17.2.113 Method Ejbtimout() In Superclass Not Recognized (Upgrade)

Description: Method ejbTimout() in superclass is not recognized. With Oracle WebLogic Server 9.1, this works fine. With Oracle WebLogic Server 10.3, the server throws the following exception:java.lang.IllegalStateException: [EJB:011084]This EJB class does not support EJB timers and therefore is prohibited from using the TimerService.To use EJB timers, the bean class must implement javax.ejb.TimedObject or have a method annotated with @Timeout. at weblogic.ejb.container.internal.BaseEJBContext$1.invoke(BaseEJBContext.java: 429) ...This problem, described in Oracle Bug 8120098, has been fixed in Oracle WebLogic Server 10.3 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Development

17.2.114 Multicast Address Is Out Of Bounds

Description: The multicast address must be between 224.0.0.0 and 239.255.255.255.

Severity: Warning

Rationale: Subsystem Outage

17.2.115 Multiple Threads Waiting For A Message To Finish Paging Causing Server Unresponsiveness

Description: Many threads get blocked on weblogic.messaging.kernel.internal.MessageHandle.waitForPaging(MessageHandle.java:474)The block is as a result of waiting for the Paging on MessageHandle(s) to finish.The particular thread that appears to be holding the lock is: "[ACTIVE] ExecuteThread: '303' for queue: 'weblogic.kernel.Default (self-tuning)'" RUNNABLE weblogic.messaging.kernel.internal.PagingImpl.run(PagingImpl.java:455) weblogic.work.ServerWorkManagerImpl$WorkAdapterImpl.run (ServerWorkManagerImpl.java:518) weblogic.work.ExecuteThread.execute(ExecuteThread.java:207) weblogic.work.ExecuteThread.run(ExecuteThread.java:179)The thread is RUNNABLE and holds the lock on a MessageHandle.

Severity: Minor Warning

Rationale: Administration

17.2.116 Multiple Threads Waiting For A Message To Finish Paging Causing Server Unresponsiveness (Upgrade)

Description: Many threads get blocked on weblogic.messaging.kernel.internal.MessageHandle.waitForPaging(MessageHandle.java:474)The block is as a result of waiting for the Paging on MessageHandle(s) to finish.The particular thread that appears to be holding the lock is: "[ACTIVE] ExecuteThread: '303' for queue: 'weblogic.kernel.Default (self-tuning)'" RUNNABLE weblogic.messaging.kernel.internal.PagingImpl.run(PagingImpl.java:455) weblogic.work.ServerWorkManagerImpl$WorkAdapterImpl.run (ServerWorkManagerImpl.java:518)The thread is RUNNABLE and holds the lock on a MessageHandle.This problem, described in Oracle Bug 8112849, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.2.117 Native Performance Pack Was Not Loaded On Server Start-Up

Description: During the server startup the performance pack or native IO should be loaded if NativeIOEnabled switch is turned on. If this does not occur, usually the library path is not set correctly or the user rights for the directory or performance pack library file are not set properly.

Severity: Warning

Rationale: Performance

17.2.118 Noncompliant Interface And Implementation Classes Cause Oracle Jrockit To Crash

Description: When an interface is not compliant with the implementation classes, Oracle JRockit may crash or throw a NullPointerException. This occurs because Oracle JRockit does not perform verification of implemented interfaces before a call, unless it

is started with the option -Xverify:all.Oracle JRockit R24.5.0 and previous versions crash under these conditions. Oracle JRockit R25.2.1-11 and later throw a NullPointerException where an IncompatibleClassChangeError could be expected.

Severity: Critical

Rationale: Server Outage

17.2.119 Not Able To Monitor Mdb Durable Subscriber In Admin Console

Description: Unable to monitor the MDB Durable Subscriber in the Oracle WebLogic Server Administration Console.

Severity: Minor Warning

Rationale: Development

17.2.120 Nullpointerexception In Java.Nio.Directbytebuffer._Get()

Description: Running with Oracle JRockit 1.5.0_08(R27.1.0) and getting a NullPointerException in java.nio.DirectByteBuffer._get()Following is the stack trace along with the NPE thrown,java.lang.NullPointerException:java.nio.DirectByteBuffer._get(Unknown Source)java.nio.Bits.getIntL(Unknown Source)java.nio.Bits.getInt(Unknown Source)java.nio.HeapByteBuffer.getInt(Unknown Source)

Severity: Warning

Rationale: Administration

17.2.121 Nullpointerexception When Compiling Web Service At Weblogic.Wsee.Tools.Anttasks.Jwsctask.E

Description: A NullPointerException is reported by JWSC (Java Web Service compiler) if portName in the implementation class does not match with the portName in Web Service Definition Language (WSDL).Sample error message:java.lang.NullPointerExceptionat weblogic.wsee.tools.anttasks.JwscTask.execute(JwscTask.java:190)at org.apache.tools.ant.UnknownElement.execute(UnknownElement.java:275)at org.apache.tools.ant.Task.perform(Task.java:364)at org.apache.tools.ant.Target.execute(Target.java:341)at org.apache.tools.ant.Target.performTasks(Target.java:369)at org.apache.tools.ant.Project.executeSortedTargets(Project.java:1216)at org.apache.tools.ant.Project.executeTarget(Project.java:1185)...

Severity: Warning

Rationale: Development

17.2.122 Oracle Jrockit 1.4.2_12 Crash At Mmgetobjectsize()

Description: Oracle JRockit 1.4.2_12 crashed on multiple WLS 8 SP4 servers.Oracle JRockit dump shows the following stack trace:Stack 0: start=0xb7a58000, end=0xb7a9c000, guards=0xb7a5d000 (ok),forbidden=0xb7a5b000Thread Stack Trace: at mmGetObjectSize+8()@0xb7e6b3c8 at findNext+166()@0xb7e9a006 at refIterGetNext +44()@0xb7e9a24c at trMarkRootsForThread+325()@0xb7ea83b5 at mmMarkRootsForThread+44()@0xb7e2cc2c at mmParThreadInspection +45()@0xb7e7794d at tsDoGCInspectionForAllThreads+37()@0xb7ed8555 at mmParMark+118()@0xb7e77d16 at mmGCMainLoop+1074()@0xb7d73722 at

tsiCallStartFunction+81()@0xb7e1ac81 at tsiThreadStub+126()@0xb7e1bd1e at ptiThreadStub+18()@0xb7e840d2 at start_thread+129()@0x9e6371 at clone +94()@0x88e9be - Java stack -

Severity: Critical

Rationale: Server Outage

17.2.123 Oracle Jrockit 1.5.0_4 Silently Ignores -Dfile.Encoding

Description: Oracle JRockit 5.0 - file.encoding does not work on Linux - instead the default system settings are usedIn java versions prior to 5.1 (or 1.5), the system property -D file.encoding defined an encoding that will be used by FileReader / FileWriter. This is still true for Sun Hotspot 1.5 and also for Oracle JRockit 5.0 on Windows.However, on Linux, setting the system property -Dfile.encoding does not have any effect on FileReader / FileWriter They take their encoding from the system default settings.This problem only happens on Linux - not on Windows.

Severity: Warning

Rationale: Administration

17.2.124 Oracle Jrockit R26.3.0 Sets System Time Back

Description: In Oracle JRockit R26 versions earlier than R26.4 on Windows operating systems, Oracle JRockit can expose a problem in the OS related to multimedia timers that causes the system time to be adjusted backwards.This can cause the system time to jump back by about 1 minute. If this happens, you can turn off the use of multimedia timers with -Djrockit.periodictask.usemmtimers=false, otherwise upgrade to R26.4 or later.

Severity: Warning

Rationale: Administration

17.2.125 Oracle Jrockit R26.4 And R27.1 Performance Is Slower Compared To Previous Versions

Description: For JRockit releases R26.4 and R27, if a thread was interrupted for garbage collection while it was in the process of copying an array, then the garbage collection may result in very long pauses.

Severity: Warning

Rationale: Performance

17.2.126 Oracle Jrockit R27.3.1 Crashes When Calling Inflate On A Closed Inflator

Description: Sometimes, calling inflate on a closed Inflater results in Oracle JRockit crashing, creating a core file. It can occur with Oracle JRockit R27.3.1.The relevant stack trace will be similar to the following:Thread Stack Trace: at inflate +73()@0x000000001027C409 at RJNI_java_util_zip_Inflater_inflateFast +90()@0x000000001020162A - Java stack - at java/util/zip/ Inflater.inflateFast(JJIJI)I(Native Method) at java/util/zip/ Inflater.inflateBytes(Inflater.java:354) at java/util/zip/Inflater.inflate(Inflater.java:216)

Severity: Critical

Rationale: Administration

17.2.127 Oracle Jrockit Does Not Support The Linux Elhugemem Kernel

Description: Oracle does not support Oracle JRockit running on the ELhugemem kernel.The ELhugemem kernel had been intended as a stopgap measure until 64-bit kernels, which are a better choice, became readily available. An example of problems with the ELhugemem kernel is 5-10 percent performance loss under normal I/O and even greater performance degradation when more calls are made into the kernel (for example, heavy I/O).

Severity: Warning

Rationale: Not Complying with Specifications

17.2.128 Oracle Weblogic Server Thin Client Is Not Supported On Aix

Description: Oracle WebLogic Server is running on an AIX platform and is configured with IIOP enabled. Please note that the thin client is not supported for this configuration.

Severity: Minor Warning

Rationale: Non-User Viewable Errors

17.2.129 Parseexception Occurs While Deploying Ear

Description: The application fails when being accessed at first. Once Oracle WebLogic Server is rebooted, the server can be accessed successfully. ParseException occurs while deploying an EAR that has a Kodo connector.

Severity: Critical

Rationale: Server Outage

17.2.130 Parseexception Occurs While Deploying Ear (Upgrade)

Description: The application fails when being accessed at first. Once Oracle WebLogic Server is rebooted, the server can be accessed successfully. ParseException occurs while deploying an EAR that has a Kodo connector.This problem, described in Oracle Bug 8979755, has been fixed in Oracle WebLogic Server 10.3 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Server Outage

17.2.131 Parsing Of Nested Cdata In Xml Results In Missing Characters

Description: When using Oracle WebLogic Integration 9.2 Maintenance Pack 1/ Maintenance Pack 2, if input XML contains nested CDATA, parsing of this document results in some missing characters from the original input data.For example, the following line is part of the input XML:< ! [CDATA [<Category>< ! [CDATA [<data>data</data>]] ></Category>]] >Parsing results in the following line:< ! [CDATA [<Category>< ! [CDATA [<data>data</data>]] ></Category>]] >Note the two missing characters at the end of the line (after Category '>' becomes '>').

Severity: Minor Warning

Rationale: Administration

17.2.132 Patch Does Not Match The Version Of Oracle Weblogic Server You Are Running

Description: Typically, each Oracle patch corresponds to a specific version of Oracle WebLogic Server. Using a patch that is designated for a different version of Oracle WebLogic Server may result in failures or incorrect behavior.

Severity: Warning

Rationale: Administration

17.2.133 Performance Can Be Improved By Enabling Native Io In Production Mode

Description: Benchmarks show major performance improvements when native performance packs are used on machines that host Oracle WebLogic Server instances. Performance packs use a platform-optimized, native socket multiplexor to improve server performance.

Severity: Minor Warning

Rationale: Administration

17.2.134 Performance May Be Impacted By Requests Waiting For A Connection

Description: If a thread requires a connection from a JDBC pool and no connection is available, the thread must wait until one becomes available. At some point in time, a connection pool in your domain had a number of requests waiting for a connection, which may impact the performance of waiting threads.

Severity: Warning

Rationale: Performance

17.2.135 Performance Of Jdbc Statementcachesize Can Be Further Tuned

Description: The use of a prepared statement or callable statement in an application or EJB creates a considerable processing overhead for the communication between the application server and the database server and on the database server itself.To minimize these processing costs, Oracle WebLogic Server can cache the prepared and callable statements that are used in your applications. When an application or EJB calls any of the statements stored in the cache, Oracle WebLogic Server reuses the cached statement. Reusing these statements reduces CPU usage on the database server, which improves the performance of the current statement and leaves the CPU available for other tasks.

Severity: Warning

Rationale: Performance

17.2.136 Production Mode Error - Hostnameverification Setting Exposes Vulnerability To Attack

Description: The domain is running in production mode, but the HostnameVerification property has been disabled. When the HostnameVerification attribute has been disabled, Oracle WebLogic Server no longer ensures that the certificate received from a remote site matches the DNS name when making a remote SSL connection. This leaves the connection vulnerable to a "man in the middle" attack.

Severity: Warning

Rationale: Administration

17.2.137 Reading An Environment Variable On In A Wslt Script Under Windows 2003 Does Not Work

Description: Reading an environment variable in a WebLogic Scripting Tool script under Windows 2003 does not work. wls:/offline> import os wls:/offline> sys.version '2.1' wls:/offline> os.environ['WL_HOME'] Failed to get environment, environ will be empty: (0, "Failed to execute command (['sh', '-c', 'env']): java.io.IOException: CreateProcess: sh -c env error=2")

Severity: Minor Warning

Rationale: Subsystem Outage

17.2.138 Resourceaccessexception While Delivering Message Causes Message To Stay In Pending State

Description: A ResourceAccessException from a JTA sub-system while delivering a message causes the message to stay in the pending state permanently until a server restart.javax.transaction.SystemException: start() failed on resource 'WLStore_domain_BUS01_BIZ_FileStore-mgd02BUS01': XAER_RMERR : A resource manager error has occured in the transaction branch weblogic.transaction.internal.ResourceAccessException: Transaction has timed out when making request to XAResource 'WLStore_domain_BUS01_BIZ_FileStore-mgd02BUS01'. at weblogic.transaction.internal.XAResourceDescriptor.startResourceUse(XAResourceDescriptor.java:712)...

Severity: Minor Warning

Rationale: User Viewable Errors

17.2.139 Saf Agent Discarding Messages

Description: SAF is discarding messages causing message loss.

Severity: Critical

Rationale: Administration

17.2.140 Saf Sometimes Stops Forwarding Messages When Receiving Server Is Restarted

Description: SAF sometimes stops forwarding messages when the receiving server(s) are restarted.

Severity: Minor Warning

Rationale: Administration

17.2.141 Saf Sometimes Stops Forwarding Messages When Receiving Server Is Restarted (Upgrade)

Description: SAF sometimes stops forwarding messages when the receiving server(s) are restarted.This problem, described in Oracle Bug 8118031, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3.

Severity: Minor Warning

Rationale: Administration

17.2.142 Saml2Namemapperinfo Getgroups Is Always Null

Description: When propagating the security context in the form of an SAML assertion between consumer and producers, and if using both JAX-RPC and JAX-WS and both SAML1 and SAML2, on the Producer side the SAMLIdentityAssertionNameMapper must check the groups, and possibly remove old groups or add new ones. This was possible with a SAML1 custom SAMLIdentityAssertionNameMapper, through the "mapGroupInfo" method. However, with SAML2 this is not possible. This is because in the "mapNameInfo" method of the SAML2IdentityAsserterNameMapper interface, the passed SAML2NameMapperInfo always returns NULL, when calling the 'getGroups()' method. This is true even if the groups are available in the SAML assertion and will be correctly added to the security context afterwards.

Severity: Minor Warning

Rationale: Administration

17.2.143 Sip Servlet In Conjunction With Commonj Is Failing

Description: When generating SNMP Traps from a SIP Servlet using SipServletSnmpTrapRuntimeMBean in conjunction with CommonJ timers, the traps fail with NullPointerExceptions. Without CommonJ timers, the traps work as expected.

Severity: Warning

Rationale: User Viewable Errors

17.2.144 Ssl Socket Connection Timeout Support For Out-Of-The-Box Jvm

Description: This is required to support SSL socket connection timeout using out-of-the-box (JRockit) JVM.

Severity: Warning

Rationale: Non-User Viewable Errors

17.2.145 Ssl Socket Connection Timeout Support For Out-Of-The-Box Jvm (Upgrade)

Description: This is required to support SSL socket connection timeout using out-of-the-box (JRockit) JVM.This problem, described in Oracle Bug 8183018, has been fixed in Oracle WebLogic Server 10.3 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Non-User Viewable Errors

17.2.146 Ssl Incompatibility When Upgrading To Jdk Version 1.6.0_14 And 1.5.0_19

Description: Upgrading to the versions 1.6.0_14 and 1.5.0_19 of the Sun JDK or Oracle JRockit causes compatibility issues between Sun JDK and Oracle JRockit handling of SSL and Oracle WebLogic Server handling of SSL.

Severity: Critical

Rationale: Non-User Viewable Errors

17.2.147 Ssl Incompatibility When Upgrading To Jdk Version 1.6.0_14 And 1.5.0_19 (Wls V10.3)

Description: Upgrading to the versions 1.6.0_14 and 1.5.0_19 of the Sun JDK or Oracle JRockit causes compatibility issues between Sun JDK and Oracle JRockit handling of SSL and Oracle WebLogic Server handling of SSL.

Severity: Critical

Rationale: Non-User Viewable Errors

17.2.148 Server Hangs With All Execute Threads In Standby State

Description: Oracle WebLogic Server may hang with every execute thread in STANDBY state.Note that Minimum Thread Constraint is not applied..Every ExecuteThread becomes as follows:."[STANDBY] ExecuteThread: '1' for queue: 'weblogic.kernel.Default(self-tuning)'" daemon prio=10 tid=0x017ad9b8 nid=0x32 in Object.wait()[0xbcd7f000..0xbcd7faf0] at java.lang.Object.wait(Native Method) - waiting on <0xd96795d8> (a weblogic.work.ExecuteThread) at java.lang.Object.wait(Object.java:474) at weblogic.work.ExecuteThread.waitForRequest(ExecuteThread.java:156) - locked <0xd96795d8> (a weblogic.work.ExecuteThread) at weblogic.work.ExecuteThread.run(ExecuteThread.java:177)

Severity: Warning

Rationale: User Viewable Errors

17.2.149 Server Hangs With All Execute Threads In Standby State. (Upgrade)

Description: Oracle WebLogic Server may hang with every execute thread in STANDBY state.Note that Minimum Thread Constraint is not applied..Every ExecuteThread becomes as follows:."[STANDBY] ExecuteThread: '1' for queue: 'weblogic.kernel.Default(self-tuning)'" daemon prio=10 tid=0x017ad9b8 nid=0x32 in Object.wait()[0xbcd7f000..0xbcd7faf0] at java.lang.Object.wait(Native Method) - waiting on <0xd96795d8> (a weblogic.work.ExecuteThread) at java.lang.Object.wait(Object.java:474) at weblogic.work.ExecuteThread.waitForRequest(ExecuteThread.java:156) - locked <0xd96795d8> (a weblogic.work.ExecuteThread) at weblogic.work.ExecuteThread.run(ExecuteThread.java:177)This problem, described in 8636905, has been fixed in Oracle WebLogic Server 10.3 Maintenance Pack 2.

Severity: Minor Warning

Rationale: User Viewable Errors

17.2.150 Sessioncookie Name Is Not The Default Jsessionid On Application Deployed To A Cluster

Description: A web application is deployed to a cluster, and the session cookie has been modified from the default (JSESSIONID). If the application is being accessed by means of a webserver running the Oracle WebLogic plugin, and the configuration has not been updated, the plugin may route Oracle WebLogic Server requests incorrectly.

Severity: Minor Warning

Rationale: Administration

17.2.151 Solaris Os Has Problems With Default Threading Libraries

Description: When starting Oracle WebLogic Server on Solaris 8 or 5.8, the default threading libraries of the operating system may cause various JVM threading issues, which can ultimately result in the server hanging or crashing.

Severity: Critical

Rationale: Server Outage

17.2.152 Some Signatures Require That Sessionmonitoring Be Enabled

Description: Some signatures require runtime MBeans to be created for Session Monitoring, in order to collect MBean data. If Session Monitoring is not enabled, data collection may be erratic or incomplete.

Severity: Minor Warning

Rationale: Non-User Viewable Errors

17.2.153 Sun Jdk Has Issues Performing Basic Date Handling Due To Changes In Dst Definitions

Description: Recent changes to the definition of US timezones to remove Daylight Savings Time (DST) awareness has broken basic functionality in date handling. The DateFormat parser uses the contents of String zoneStrings[][] in class DateFormatSymbols to identify the timezone based on the zone value in the input date string.For example, the zoneStrings[][] array defines "EST" before "America/New_York" so sets the timezone for the parser to the now non-DST aware "EST" zone.This issue only affects sites using the these three-letter abbreviations of DST times zones denotations, which have been deprecated, and any of the following versions of the Sun JDK:* Sun JDK 1.6* Sun JDK 1.5.0_08 and later* Sun JDK 1.4.2_12 and later

Severity: Warning

Rationale: Not Complying with Specifications

17.2.154 System Properties May Not Have Been Passed In Correctly If A $ Is Found

Description: Typically, a dollar sign ("$") in the system properties indicates an attempt to reference an environment variable that has not been evaluated correctly. As a result, the property may not have the desired effect.

Severity: Warning

Rationale: Administration

17.2.155 System Properties May Not Have Been Passed In Correctly If A % Is Found

Description: Typically, a percent sign ("%") in the system properties indicates an attempt to reference an environment variable that has not been evaluated correctly. Therefore, the property may not be having the desired effect.

Severity: Warning

Rationale: Administration

17.2.156 The Published Site Url For Saml Must End With /Saml2 Or Saml2 Will Not Work

Description: The Published Site URL for SAML2 must end with the string "/saml2" (without quotes) or SAML2 will not function properly. In addition, the published site URL must be the URL of the server that is configured for SAML2, for both the Identity Provider (IdP) and Service Provider (SP). This affects only SAML2.

Severity: Minor Warning

Rationale: Administration

17.2.157 The Jsp:Usebean Body Gets Executed Even If The Named Javabean Already Exists In The Scope

Description: In JSP, when Java Beans are used:<jsp:useBean> body gets executed even if named JavaBean already exists in the scope.

Severity: Minor Warning

Rationale: Administration

17.2.158 The Jsp:Usebean Body Gets Executed Even If The Named Javabean Already Exists In The Scope. (Upgrade)

Description: In JSP, when Java Beans are used:<jsp:useBean> body gets executed even if named JavaBean already exists in the scope.This problem, described in Oracle Bug 8093561, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Administration

17.2.159 Timed Out Exception Trying To Setmonitoredattributename For Snmpgaugemonitor

Description: The following stacktrace is obtained when trying to setMonitoredAttributeName for SNMPGaugeMonitor on Solaris platform:Caught java.lang.RuntimeException: Timed out waiting for completionjava.lang.RuntimeException: Timed out waiting for completion at weblogic.management.provider.internal.ActivateTaskImpl.waitForCompletion(ActivateTaskImpl.java:374) at weblogic.management.provider.internal.ActivateTaskImpl.waitForTaskCompletion(ActivateTaskImpl.java:349) ...

Severity: Warning

Rationale: Administration

17.2.160 Too Many Open Files Errors Can Be Remedied By Limiting The Number Of Open Sockets Allowed

Description: The "Too Many Open Files" error usually occurs after several concurrent users get a connection to the Server. Java opens many files in order to read in the classes required to run your application. High volume applications can use a lot of file descriptors. This could lead to a lack of new file descriptors. Also, each new socket requires a descriptor. Clients and Servers communicate via TCP sockets. Each browser's HTTP request consumes TCP sockets when a connection is established to a

Server. Limiting the number of open sockets allowed prevents your server from running out of file descriptors.

Severity: Warning

Rationale: Performance

17.2.161 Unable To Set Protocol Specific Max Message Size (Wls V10)

Description: MaxHTTPMessageSize, MaxT3MessageSize, and MaxCOMMessageSize are deprecated since Oracle WebLogic Server 8.1. Instead of using these protocol specific parameters, use separate network channels configured with a MaxMessageSize to limit the incoming messages.

Severity: Minor Warning

Rationale: Administration

17.2.162 Under High Load, The Sybase Jdbc Connectionpool Becomes Disabled

Description: If you use a Sybase database with Oracle JRockit R27.1, R27.2, or R27.3, under high load the Sybase JDBC Connection Pool becomes disabled, with the following error:"java.sql.SQLException: JZ006: Caught IOException: java.io.IOException: JZ0EM: End of data."

Severity: Warning

Rationale: Subsystem Outage

17.2.163 Using The Post-Bind Option With Jrockit On Linux Causes Server Core Dump

Description: Attempting to start a server on a Linux platform when setting the post-bind option in a UNIX machine can cause the server to core dump with a StackOverflow exception.This applies to Oracle JRockit R26.2 and above.

Severity: Critical

Rationale: Administration

17.2.164 Verify That A File Being Opened As A Jra Recording Is A Jra Recording Before Opening It

Description: JRockit throws a divide by zero ArithmeticException when opening a file other than a JRA recording or a corrupted JRA recording. This issue has been fixed in JRockit R27.5.0. Here is an example error message:java.lang.ArithmeticException: / by zero at com.jrockit.jra.model.MemoryInfo.getAllocationFrequencySmallObjects(MemoryInfo.java:415) at com.jrockit.mc.jra.ui.general.GeneralContent.getFieldData(GeneralContent.java:129) at com.jrockit.mc.jra.ui.general.MiscSectionPart.createClient(MiscSectionPart.java:39) at com.jrockit.mc.jra.ui.sections.InfoSectionPart.initialize(InfoSectionPart.java:81) ...

Severity: Minor Warning

Rationale: Administration

17.2.165 Wsee Logs Even When -Dweblogic.Wsee.Verbose Is Not Set

Description: On the producer side, messages like the following are logged at each call, even when -Dweblogic.wsee.verbose is not set:<WSEE:14>Trying to validate identity

assertion token http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0<SecurityMessageInspector.inspectIdentity:629><WSEE:14>Validated identity assertion token http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0<SecurityMessageInspector.inspectIdentity:632>saml2namemapperinfo=com.bea.security.saml2.providers.SAML2NameMapperInfo@2d24dfa<WSEE:14>Trying to validate identity assertion token http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0<SecurityMessageInspector.inspectIdentity:629>

Severity: Minor Warning

Rationale: Administration

17.2.166 Wsee Logs Even When -Dweblogic.Wsee.Verbose Is Not Set (Upgrade)

Description: On the producer side, the following messages were logged at each call, even when -Dweblogic.wsee.verbose is not set:<WSEE:14>Trying to validate identity assertion token http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0<SecurityMessageInspector.inspectIdentity:629><WSEE:14>Validated identity assertion token http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0<SecurityMessageInspector.inspectIdentity:632>saml2namemapperinfo=com.bea.security.saml2.providers.SAML2NameMapperInfo@2d24dfa...Oracle Bug 8184141 has been fixed in Oracle WebLogic Server 10.3 Maintenance Pack 1

Severity: Minor Warning

Rationale: Administration

17.2.167 Wtc Remote-Access-Point-List Cannot Be Configured With More Than Three Remote Access Point

Description: Oracle WebLogic Server Administration Console running Oracle WebLogic Tuxedo Connector (WTC) does not allow the creation of more than three Remote Access Points to Tuxedo. Adding more than three connections will typically fail with the error displaying in the Oracle WebLogic Server log file: Could not create a TDMImport Remote access point cannot have more than three elements.

Severity: Minor Warning

Rationale: Administration

17.2.168 Waitingforconnectionsuccesstotal Is Incorrect

Description: In the Oracle WebLogic Server console, the value of "Waiting For Connection Success Total" JDBC Connection pool monitoring is incorrect. Even when there are no waiters connection, "Waiting For Connection Success Total" count increases.

Severity: Minor Warning

Rationale: Administration

17.2.169 Waitingforconnectionsuccesstotal Is Incorrect. (Upgrade)

Description: In the Oracle WebLogic Server console, the value of "Waiting For Connection Success Total" JDBC Connection pool monitoring is incorrect. Even when there are no waiters connection, "Waiting For Connection Success Total" count

increases.This problem, described in Oracle Bug 8125231, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.2.170 Windows 2000 Sp2 And Higher Required For Oracle Jrockit 1.5_02 And 1.5_03

Description: Oracle JRockit 1.5_02 (R25.0.0) and Oracle JRockit 1.5_03 (R25.2.0) running on Windows 2000 requires Service Pack 2 or higher. This signature indicates that you are running no service pack or one less than Service Pack 2. Upgrade to Windows 2000 SP 2 or higher.

Severity: Critical

Rationale: Not Complying with Specifications

17.2.171 Windows 2000 Sp2 And Higher Required For Oracle Jrockit 1.4.2_03 Through 1.4.2_11 On X86

Description: Windows 2000 SP2 and higher is required for Oracle JRockit 1.4.2_03 through 1.4.2_11

Severity: Warning

Rationale: Not Complying with Specifications

17.2.172 Windows 2000 Sp4 And Higher Required For Oracle Jrockit 1.5_04 (R26.0.0) Through 1.5_06

Description: Windows 2000 SP4 and higher required for Oracle JRockit 1.5_04 through Oracle JRockit 1.5_06.

Severity: Critical

Rationale: Not Complying with Specifications

17.2.173 With Oracle Jrockit R27.3.0, Ctrl-C Can Cause Improper Shutdown And Loss Of Data

Description: If you are running on Linux or Solaris and press Ctrl-C to properly shut down your application, it will actually terminate immediately and you risk losing any runtime data that hasn't been saved to disk or a database. This happens because Oracle JRockit fails to register the SIGINT signal handler used for the shut down hooks.This issue does not apply to applications running on Windows.

Severity: Critical

Rationale: Administration

17.2.174 With Oracle Jrockit R27.4.0, Ldap Users Are Not Populated In Administration Console

Description: The users in the Administration Console (Security Realms > myrealm > Users and Groups) are not visible when Oracle JRockit R27.4.0 is used. However, this is not the case with previous Oracle JRockit versions.

Severity: Warning

Rationale: Administration

17.2.175 Work Manager Requires Authentication During Sever Startup (Wls V10, Upgrade)

Description: If you are using ALBPM 6.0.4 on Oracle WebLogic Server 10.3 and have ALBPM processes with Global Automatic Activities, these Global Automatic Activities listen to JMS queues for messages. You may not notice any consumers on some queues after server startup.This problem, described in Oracle Bug 8176788, has been fixed in Oracle WebLogic Server 10.3 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Server Outage

17.2.176 Workmanager Requires Authentication During Sever Startup (Wls V10)

Description: If you are using ALBPM 6.0.4 on Oracle WebLogic Server 10.3, and if you have ALBPM processes that contain Global Automatic Activities, then these Global Automatic Activities listen to JMS queues for messages.In ALBPM 6.x implementation, the engine implements this type of Global Automatic Activity by scheduling a work item with the WorkManager (default or custom). The WorkManager runs the work item in one of its threads. The work item, when executed, dynamically creates a JMS queue consumer that represents a Global Automatic Activity.The issue is that you may not notice any consumers on some queues after server start up.

Severity: Critical

Rationale: Server Outage

17.2.177 Findmonitordeadlockedthreads() Detects False Positive Java Deadlock

Description: When running Oracle JRockit R27.1.0 with the load environment, the JVM detects a false positive Java-level deadlock, as follows:[deadlocked thread] [ACTIVE] ExecuteThread: '334' for queue:'weblogic.kernel.Default (self-tuning)': -Thread '[ACTIVE] ExecuteThread: '334' for queue: 'weblogic.kernel.Default(self-tuning)'' is waiting to acquire lock'weblogic.messaging.kernel.internal.QueueImpl@43fbf06' that is held by thread'[ACTIVE] ExecuteThread: '334' for queue: 'weblogic.kernel.Default(self-tuning)''After this, the Server state is changed to FAILED. This thread is unblocked already in the next thread dump that is taken automatically by the core health monitoring system.

Severity: Warning

Rationale: Administration

17.2.178 Java.Lang.Classcastexception At Distributeddestinationimpl.Java In Oracle Jrockit R27.4.0

Description: With JRockit R27.4.0, when an Oracle WebLogic Server cluster peer attempts to synchronize with a peer, a java.lang.ClassCastException is raised in DistributedDestinationImpl.java, without a successful cluster peer synchronization.For example, the following stack trace excerpt occurred in an Oracle WebLogic Portal 8.1 Maintenance Pack 3 cluster domain with JRockit 142_15 (R27.4.0) and migratable JMS Servers configured for managed servers. During the start up of managed servers, the following exception was raised:...java.lang.ClassCastException: weblogic.rmi.internal.CBVOutputStream$CBVObjectOutputStream at

weblogic.jms.common.DistributedDestinationImpl.writeExternal(DistributedDestinationImpl.java:328) at...

Severity: Warning

Rationale: Administration

17.3 All WLS V9 Rules (Deprecated)

The compliance rules for the All Wls V9 Rules standard follow.

17.3.1 A Nullpointerexception Occurs When Oracle Weblogic Server Timer Has Fixed Rate

Description: In Oracle WebLogic Server 9.2, a NullPointerException occurs on the server side when a registered listener has a Oracle WebLogic Server Timer with a fixed rate.

Severity: Minor Warning

Rationale: Administration

17.3.2 A Better Way Of Handling Large Log Messages Is Required. (Upgrade)

Description: The LogBroadcaster fails to broadcast log messages when the log message is large. Messages bigger than 64k fail to be broadcast. This size limitation was introduced in Oracle WebLogic Server 9.x.Error message:<BEA-170011> <The LogBroadcaster on this server failed to broadcast log messages to the admin server. The Admin server may not be running. Message broadcasts to the admin server will be disabled.>This problem, described in Oracle Bug 8166717, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3.

Severity: Minor Warning

Rationale: Administration

17.3.3 A Duplicate Global Type Error Is Thrown In A Web Service When <Xs:Include> Is Used

Description: When a Oracle WebLogic Server Web Service has two operations in it and each operation takes one XMLBean, and these XSDs include an XML type via <xs:include> statement, it results in the following error when publishing the Web Service to the server:weblogic.wsee.ws.WsException: Failed to create binding providercom.bea.xml.XmlException: ...: error:sch-props-correct.2: Duplicate global type: Item@http://www.sample.org/model (Original global type found in file:URI_SHA_1_26F162A02C0B8E453B3528125B8B9A9E38A76D2C/SaleService.wsdl) at weblogic.wsee.ws.WsBuilder.createRuntimeBindingProvider(WsBuilder.java:355)

Severity: Warning

Rationale: Development

17.3.4 A Java.Lang.Illegalstateexception: Httpsession Is Invalid Under Load Occurs In Cluster

Description: In a cluster of Oracle WebLogic Servers, if there is a Web Application using in-memory session replication, the following Exception can occur when the servers are under load: - -java.lang.IllegalStateException: HttpSession is invalid at

weblogic.servlet.internal.session.SessionData.getInternalAttribute(SessionData.java:633) at weblogic.servlet.internal.session.SessionData.updateVersionIfNeeded(SessionData.java:1237) at weblogic.servlet.internal.session.ReplicatedSessionContext.getSessionInternal(ReplicatedSessionContext.java:357) at weblogic.servlet.internal.ServletRequestImpl$SessionHelper.getValidSession(ServletRequestImpl.java:2412) at weblogic.servlet.internal.ServletRequestImpl$SessionHelper.getSession(ServletRequestImpl.java:1985) -

Severity: Minor Warning

Rationale: User Viewable Errors

17.3.5 A Java.Lang.Illegalstateexception: Httpsession Is Invalid Under Load Occurs In Cluster (Upgrade)

Description: If an Oracle WebLogic Server cluster is hosting a Web application using in-memory session replication, the following exception can occur when the servers are under load:java.lang.IllegalStateException: HttpSession is invalid at weblogic.servlet.internal.session.SessionData.getInternalAttribute(SessionData.java:633) at weblogic.servlet.internal.session.SessionData.updateVersionIfNeeded(SessionData.java:1237)...This problem, described in Oracle Bug 8109736, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: User Viewable Errors

17.3.6 A Session Id With Urlrewriting No Longer Written To Http Access

Description: The access.log file is being truncated at the URL query parameters, so the session ID after the semicolon is not being recorded. For example, the access should be written to the log file as follows:127.0.0.1 - - [03/Jan/2007:17:17:58 +0100] "GET/rewrite/hello2.jsp;jsessionid=FbX0Mqltwff3MLyKbSQLTv0qTp3phqQmg1LYTMZXJLhB!1289340431HTTP/1.1" 200 35Instead, the access is being written to the log file as follows:127.0.0.1 - - [03/Jan/2007:17:17:58 +0100] "GET /rewrite/hello2.jsp HTTP/1.1" 200 35

Severity: Minor Warning

Rationale: Administration

17.3.7 A Session Id With Urlrewriting No Longer Written To Http Access. (Upgrade)

Description: The access.log file is being truncated at the URL query parameters, so the session ID after the semicolon is not being recorded. For example, the access should be written to the log file as follows:127.0.0.1 - - [03/Jan/2007:17:17:58 +0100] "GET/rewrite/hello2.jsp;jsessionid=FbX0Mqltwff3MLyKbSQLTv0qTp3phqQmg1LYTMZXJLhB!1289340431HTTP/1.1" 200 35Instead, the access is being written to the log file as follows:127.0.0.1 - - [03/Jan/2007:17:17:58 +0100] "GET /rewrite/hello2.jsp HTTP/1.1" 200 35This problem, described in Oracle Bug 8108185, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.3.8 Ant Task Wlserver Raises Javax.Xml.Namespace.Qname; Local Class Incompatible

Description: When using the ANT task <wlserver> to create a domain, the creation is accomplished correctly. However, when the Oracle WebLogic Server starts (using the same ANT script), the following exception can occur:[WLServer Admin-1] weblogic.management.ManagementException: [Management:141266]Parsing Failure in config.xml: javax.xml.namespace.QName; local class incompatible: stream classdesc serialVersionUID = 4418622981026545151, local class serialVersionUID = -9120448754896609940Cause:Starting with JDK 1.5.0_07 (and later), Sun changed the version UID of the class javax.xml.namespace.QName. A new Java system property was introduced to have a compatibility mode: -Dcom.sun.xml.namespace.QName.useCompatibleSerialVersionUID=1.0This property must be set to avoid this error.

Severity: Minor Warning

Rationale: Administration

17.3.9 Apt Error When Exported Build.Xml File Is Run

Description: When a build file is exported and run as an ANT task, the error shown below occurs. The error does not occur if the build is performed through Workshop for Oracle WebLogic Server 9.2.Error message:"This operation uses a Java type that cannot be transmitted by the web service."

Severity: Minor Warning

Rationale: User Viewable Errors

17.3.10 Apt Error When Exported Build.Xml File Is Run (Upgrade)

Description: When a build is performed through Workshop for Oracle WebLogic Server 9.2, the error shown below does not occur. However, when the build file is exported and run as an ANT task, the error occurs.Error message:"This operation uses a Java type that cannot be transmitted by the web service."This problem, described in Oracle Bug 8123975, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3.

Severity: Minor Warning

Rationale: User Viewable Errors

17.3.11 Activation Error Not Being Thrown To The Client Leading To Client Timeout

Description: If a JDBC module exception is thrown, WebLogic Scripting Tool activate command will time out and never complete. In addition, the underlying JDBC module exception is not returned to the caller due to the activation timeout.

Severity: Minor Warning

Rationale: Administration

17.3.12 Activation Error Not Being Thrown To The Client Leading To Client Timeout. (Upgrade)

Description: If a JDBC module exception is thrown, WebLogic Scripting Tool activate command will time out and never complete. In addition, the underlying JDBC module

exception is not returned to the caller due to the activation timeout.This problem, described in Oracle Bug 8071550, has been fixed in Oracle WebLogic Server 9.2.

Severity: Minor Warning

Rationale: Administration

17.3.13 Active Directory Authenticator Does Not Display Group Membership For Users In Console

Description: The Active Directory Authenticator in the Oracle WebLogic Server Administration Console does not display the groups that a user belongs to.

Severity: Minor Warning

Rationale: Administration

17.3.14 Active Execute Thread Count Is Incorrect

Description: The Oracle WebLogic Server 9.2 console Environment - Servers - "select server" - Monitoring tab - Threads tab, a value named "Active Execute Thread" count is displayed. This count is the number of threads that have a status of "Active"; however, this value is calculated as threads with status of "Active" or "Standby".

Severity: Minor Warning

Rationale: Administration

17.3.15 Active Execute Thread Count Is Incorrect (Upgrade)

Description: The Oracle WebLogic Server 9.2 console Environment - Servers - "select server" - Monitoring tab - Threads tab, a value named "Active Execute Thread" count is displayed. This count is the number of threads that have a status of "Active"; however, this value is calculated as threads with status of "Active" or "Standby".This problem, described in Oracle Bug 8105211, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.3.16 Add The Host And Port Into The Snmp Trap Destination Creation Assistant

Description: When creating an SNMP trap destination, the assistant page only has the destination name. You will have to change the "Host" and "Port" of the trap destination. Modifying those attributes will require a server restart.

Severity: Warning

Rationale: Administration

17.3.17 Admin Console Provider Import And Export Pages Prompt To 'Save' Even If No Changes Made

Description: The Administration Console Provider Import and Export pages prompt you to save, even if you haven't made any changes. To duplicate this scenario:1. Click the provider's migration tab.2. Click either the Import or Export tab, and do not make any changes on the screen.3. Click the other tab (either Import or Export). A pop-up box prompts you to save changes.

Severity: Minor Warning

Rationale: Administration

17.3.18 Admin Console Does Not Allow Editing Jdbc Datasource Configuration If It Fails To Deploy

Description: Leaving Customize This Table without making any changes causes a dialog box to pop up.The following scenario describes how to duplicate this error:1. Lock, create JDBC DataSource with XA driver, activate changes.2. Lock, select JDBC DataSource, connection pool, Advanced options, uncheck.3. Remove Infected Connections Enabled (change any non-dynamic attribute), Save, Activate changes.This generates the following on the console:An error occurred during activation of changes, please see the log for details.[Deployer:149001]No application named 'JDBC DataSource-000' exists for operation redeploy

Severity: Minor Warning

Rationale: Administration

17.3.19 Admin Console Does Not Redirect To A New Host/Port Combination If Admin Port Enabled

Description: When you enable the administration port from the Administration Console and then click Activate, the Administration Console is not reachable until the URL used to communicate with the Administration Console is changed to HTTPS and the administration port number.

Severity: Minor Warning

Rationale: Administration

17.3.20 Admin Console Dumps Thread Stacks Incorrectly When Using A Vjm Other Than Oracle Jrockit

Description: If your server is not running on Oracle JRockit and you try to use the Dump Thread Stacks feature in the Administration Console, the Console shows "This page displays the current stacks for each thread" but the Threads table is empty, and there is no thread dump on the server.

Severity: Minor Warning

Rationale: Administration

17.3.21 Admin Console'S Classnotfoundexception Error Generates Voluminous Stack Trace Errors

Description: During auto-refresh of server monitoring/performance, a ClassNotFoundException error occurs in the Administration Console. The Administration Console refresh works, but a large number of stack traces appear in the administration server log.javax.servlet.ServletException:[HTTP:101249] [weblogic.servlet.internal.WebAppServletContext@11ff258 -appName: 'consoleapp', name: 'console', context-path: '/console']: Servletclass jsp_servlet._jsp._common._images.__spacer_gif for servlet/jsp/common/images/spacer.gif could not be loaded because the requested classwas not found in the classpath .java.lang.ClassNotFoundException:jsp_servlet._jsp._common._images.__spacer_gif.
atweblogic.servlet.internal.ServletStubImpl.prepareServlet(ServletStubImpl.java:516)...

Severity: Minor Warning

Rationale: Non-User Viewable Errors

17.3.22 Admin Console: Admin Server Shutdown Message: Must Restart Server From Node Manager/Cli

Description: When you use the Administration Console to shut down an Administration Server or Managed Server, the following message is displayed:"The Administration Server is shutting down, and the console is no longer available. You will have to manually start the Administration Server using the node manager or a command line to continue administering this domain."However, the Node Manager is not available in Oracle WebLogic Server Virtual Edition.

Severity: Warning

Rationale: Administration

17.3.23 Admin Console: Runtimeoperationsexception Occurs If You Click On Deployed Libraries

Description: In the Oracle WebLogic Server Admin Console, a javax.management.RuntimeOperationsException is raised if you click on a deployed library that is referenced by any deployed application.

Severity: Warning

Rationale: User Viewable Errors

17.3.24 Admin Console: Runtimeoperationsexception Occurs If You Click On Deployed Libraries (Upgrade)

Description: In the Oracle WebLogic Server Administration Console , a javax.management.RuntimeOperationsException is raised if you click on a deployed library that is referenced by any deployed application.This problem, described in Oracle Bug 8097920, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: User Viewable Errors

17.3.25 Admin Server Should Not Have Listen Address As '0.0.0.0' In A Distributed Environment

Description: If the Listen Address for the Admin Server is set to "0.0.0.0", managed servers will be unable to connect to the Admin Server if they are started on remote machines via the Node Manager.

Severity: Minor Warning

Rationale: Administration

17.3.26 Admin Console Creates Temporary Files But Does Not Delete Them

Description: When uploading and deploying modules (WAR, EAR, JAR, etc.), the Administration Console creates temporary files but neglects to delete them later when they are no longer necessary.The naming convention of these files is strtsXXXXX.tmp. They are written to the ${java.tmp.dir} directory as follows: Windows: C:\Documents and Settings\<user>\Local Settings\Temp\ UNIX: /var/tmp, /tmp, or /etc

Severity: Minor Warning

Rationale: Performance

17.3.27 Admin Console Creates Temporary Files But Does Not Delete Them (Upgrade)

Description: When uploading and deploying modules (WAR, EAR, JAR, etc.), the Administration Console creates temporary files but neglects to delete them later when they are no longer necessary.The naming convention of these files is strtsXXXXX.tmp. They are written to the ${java.tmp.dir} directory as follows: Windows: C:\Documents and Settings\<user>\Local Settings\Temp\ UNIX: /var/tmp, /tmp, or /etcThis problem, described in Oracle Bug 8066216, has been fixed in Oracle WebLogic Server 9.2.

Severity: Minor Warning

Rationale: Performance

17.3.28 Admin Console Fails To Open Table Form Pages With Javax.Servlet.Servletexception

Description: The admin console fails to open table form pages with 'javax.servlet.ServletException: Index: 0, Size: 0'. When this problem occurs, you can see the following errors in the admin server's log:####<Oct 5, 2007 11:49:57 AM JST> <Error> <Console> <akitada04> <AdminServer> <[ACTIVE] ExecuteThread: '3' for queue: 'weblogic.kernel.Default (self-tuning)'> <weblogic> <> <> <1191552597171> <BEA-240003> <Console encountered the following error Exception during RequestDispatcher.include().This problem occurs after editing form tables. Once this problem occurs, opening the specific table form pages fail even after rebooting the admin server.

Severity: Minor Warning

Rationale: Administration

17.3.29 Admin Console Throws Npe On The Show Messages Page Of A Jms Queue

Description: Console throws an NPE on the Show messages page of a JMS queue.

Severity: Warning

Rationale: Administration

17.3.30 Admin Server Running Out Of Heap Space

Description: Using WebLogic Scripting Tool or the Admin Console to upload and deploy the Oracle Service Bus configuration definition (sbconfig.xml) multiple times can cause "out of memory" errors.Cause:Oracle Service Bus deployment tasks are not properly cleaned up in Oracle WebLogic Server deployment framework, and thus remain in memory and not eligible for Garbage Collection.

Severity: Warning

Rationale: Performance

17.3.31 Adminserver Does Not Listen On Ip - Aliasing When Listen Address Is Blank

Description: When the Listen Address for the Administration Server is undefined (left blank), Oracle WebLogic Server listens only to the physical IP and is unable to be accessed by other aliased IP.

Severity: Minor Warning

Rationale: Non-User Viewable Errors

17.3.32 Adminserver Does Not Listen On Ip - Aliasing When Listen Address Is Blank. (Upgrade)

Description: When the Listen Address for the Administration Server is undefined (left blank), Oracle WebLogic Server listens only to the physical IP and is unable to be accessed by other aliased IP.This problem, described in Oracle Bug 8107797, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Non-User Viewable Errors

17.3.33 Administration Console - Does Not Display Accurate Monitoring Info About Mdbs

Description: The Administration Console does not display accurate information for runtime mbeans for a running message driven bean.For example, if you deploy an application to a server, then select a message driven bean that is part of this application, and select the monitoring tab, it displays a message "This EJB is not currently active on any running server," even if the application is targeted correctly and active in the server.

Severity: Warning

Rationale: Administration

17.3.34 Administration Console Jndi Tree Viewer Does Not Work If Console Context Path Is Changed

Description: If you modify the Oracle WebLogic Server Administration Console context path by changing the URL, the JNDI View for the Server JNDI tree fails to use the new context path, and does not display correctly.

Severity: Minor Warning

Rationale: Administration

17.3.35 Administration Console Jndi Tree Viewer Does Not Work If Console Context Path Is Changed. (Upgrade)

Description: If you modify the Oracle WebLogic Server Administration Console context path by changing the URL, the JNDI View for the Server JNDI tree fails to use the new context path, and so does not display correctly.This problem, described in Oracle Bug 8122349, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3.

Severity: Minor Warning

Rationale: Administration

17.3.36 Administration Console Deployment Fails With Weblogic.Management.Provider.Editfailedexception (Wls V9.1)

Description: Occasionally during deployment, the "Deployment Settings" window allows the selection of incorrect options, and these incorrect selections are allowed to

pass through.For example, while deploying an application to one cluster member, the "All Servers" option is selected, which is incorrect. Now these incorrect selections will result in the following error message:weblogic.management.provider.EditFailedExceptionIf this problem occurs, the domain must be rebooted.

Severity: Warning

Rationale: Not Complying with Specifications

17.3.37 Administration Console Deployment Fails With Weblogic.Management.Provider.Editfailedexception (Wls V9.2)

Description: Occasionally during deployment, the "Deployment Settings" window allows the selection of incorrect options, and these incorrect selections are allowed to pass through. For example, while deploying an application to one cluster member, the "All Servers" option is selected, which is incorrect. These incorrect selections result in the following error message:javascript:void(null);Remedyweblogic.management.provider.EditFailedExceptionIf this problem occurs, the domain must be rebooted.

Severity: Warning

Rationale: Not Complying with Specifications

17.3.38 Administration Console Does Not Allow Adding Constraints To The Work Manager

Description: When using the Administration Console to define an application-level Work Manager, adding constraints to the Work Manager causes validation problems.

Severity: Warning

Rationale: Development

17.3.39 Administration Console Does Not Display A List Of Deployed Applications

Description: The Administration console does not display a list of applications deployed on each server of a cluster. The Console should display this list in the Deployments tab for the Settings of the server.

Severity: Minor Warning

Rationale: Administration

17.3.40 Administration Console Does Not Display The 'Re-Order Authentication Providers' Link

Description: Changing the security realm from default to a custom realm for which the realm configuration is not complete throws an exception with the following key items:BEA-141191The prepare phase of the configuration update failed with an exception:weblogic.descriptor.DescriptorUpdateRejectedException: [Security: 090818]under this exception there is also one exception with the following key items:BEA-240000java.lang.Runtime Exception: Unable to load the exception class [Securityat weblogic.management.jmx.CompositeTypeThrowable.reconstitute

Severity: Minor Warning

Rationale: Administration

17.3.41 Administration Console Does Not Support Unicast Clustering Mbean Attributes

Description: The current Oracle WebLogic Server cluster implementation uses multicast sockets for broadcasting messages to cluster members. These messages are called GroupMessages. Unicast-based cluster messaging provides cluster-wide broadcast of GroupMessages without the use of multicast sockets. However, the Oracle WebLogic Server 9.2 Administration Console does not provide support for unicast clustering MBeans.

Severity: Minor Warning

Rationale: Administration

17.3.42 Administration Server Is Hosting Applications Other Than Oracle System Applications

Description: Your Administration Server is hosting applications other than Oracle system applications. Oracle recommends hosting these applications only on the managed servers within your domain. The only applications that should be deployed to your Administration Server are Oracle applications (for example, the Oracle WebLogic Server Administration Console and Oracle agents).

Severity: Warning

Rationale: Administration

17.3.43 Administration Console Hangs During Restart Of A Remote Managed Server

Description: When the Administration Console is used to stop and restart a remote Managed Server, the Administration Console hangs until the remote Managed Server has been fully started.

Severity: Warning

Rationale: Administration

17.3.44 Administration Console Hangs During Restart Of A Remote Managed Server

Description: Cannot display the JNDI tree on the Oracle WebLogic Server console on a managed server. It seems that the problem is caused by an empty <jndi-name> tag, which was accidentally added in the datasource configuration file.<jdbc-data-source-params> <jndi-name>dsGestionRepresentations</jndi-name> <jndi-name></jndi-name><global-transactions-protocol>TwoPhaseCommit</global-transactions-protocol></jdbc-data-source-params>When reading the tree a java.lang.StackOverflowError appears in the logs.

Severity: Critical

Rationale: Server Outage

17.3.45 After Leaving The Server Running Idle, Relogging Into The Jndi Window Only Shows Null

Description: After leaving the server idle, when you come back to the JNDI window and click any link, you are asked to login again, which is expected. However, after logging in, the window only displays the word "Null" instead of the tree.

Severity: Minor Warning

Rationale: Administration

17.3.46 After Upgrading To Oracle Weblogic Server 9.2 Maintenance Pack 1, Bsu.Cmd Cannot Start

Description: When installing Oracle WebLogic Server 9.2 GA without running Smart Update, and then upgrading to Oracle WebLogic Server 9.2 Maintenance Pack 1 using the upgrade installer, Oracle Smart Update (bsu.cmd) cannot start.For example, the following installers were used:- server920_win32.exe (EN GA kit)- server921_upgrade_win32.exe (EN GA kit)In the three example scenarios below, Oracle Smart Update can start successfully for (1) and (2) but cannot start for (3).(1) install 9.2 -> start Oracle Smart Update(2) install 9.2 -> start and close Oracle Smart Update -> upgrade to MP1 -> start Oracle Smart Update(3) install 9.2 -> upgrade to MP1 -> start Oracle Smart Update

Severity: Minor Warning

Rationale: Administration

17.3.47 All Attributes Are Selected By Default Under Jdbc Monitoring Tab

Description: Create a Datasource called mydatasourceJDBC - > DataSource - > mydatasource - > Monitoring tabIn this page it shows all attributes (around 26 columns in the table) in tabular form with their corresponding data. Change it to show only 6 or 8 attributes (columns), also there is a "Customize this table" link, which will help users to select and see all attributes.

Severity: Minor Warning

Rationale: Administration

17.3.48 An Error From Publish Action Creates Blank $Fault

Description: The $fault variable is populated if you explicitly set an XQuery function in the "Request Actions" of the "Publish Action," and fails to be populated if a "Raise Error" action is used in the "Publish Action." This behavior is independent of the QoS ("Best Effort" or "Exactly Once"). In a "Best Effort" scenario, the exception will be consumed.Resolution:Apply Oracle Bug 8105659. After you apply the patch, the $fault variable will be populated in the original context for a "Publish Action" on a "Raise Error" action in a Qos "Exactly Once" scenario.

Severity: Warning

Rationale: Administration

17.3.49 An Org.Hibernate.Lazyinitializationexception Occurs For Calls Over Iiop (Wls V9.2, Upgrade)

Description: When using the -Dweblogic.iiop.useJavaSerialization flag in a call over IIOP, an org.hibernate.LazyInitializationException occurs.This problem, described in Oracle Bug 8145565, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3.

Severity: Minor Warning

Rationale: Server Outage

17.3.50 An Org.Hibernate.Lazyinitializationexception Occurs For Calls Over Iiop. (Wls V9.2)

Description: When using the -Dweblogic.iiop.useJavaSerialization flag in a call over IIOP, an org.hibernate.LazyInitializationException occurs.

Severity: Critical

Rationale: Server Outage

17.3.51 Apache Plug-In - Server List Is Empty. Cannot Locate Preferred Servers

Description: Using the Apache plugin, the following exception appears in the log:"Server list is empty. Can't locate preferred servers "

Severity: Warning

Rationale: Subsystem Outage

17.3.52 Apache Plug-In - Server List Is Empty. Cannot Locate Preferred Servers. (Upgrade)

Description: Using the Apache plugin, following exception appears in the log:"Server list is empty. Can't locate preferred servers "This problem, described in Oracle Bug 8115635, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Subsystem Outage

17.3.53 Applet Jms Consumer Reconnects But Fails To Receive Messages

Description: When Oracle WebLogic Server was restarted, an Applet JMS consumer failed to receive any messages, even though it was reconnected.While Oracle WebLogic Server is down, or in the process of restarting, the following exception in Applet JMS consumer output occurs:javax.naming.CommunicationException [Root exception is java.net.ConnectException: t3://xxxxxx01:7001: Destination unreachable; nested exception is: java.net.ConnectException: Connection refused: connect; No available router to destination] ...

Severity: Minor Warning

Rationale: Administration

17.3.54 Applet Jms Consumer Reconnects But Fails To Receive Messages (Upgrade)

Description: When Oracle WebLogic Server is restarted, an Applet JMS consumer failed to receive any messages, even though it was reconnected. While the server is down or in the process of restarting, the following exception in Applet JMS consumer output occurs:javax.naming.CommunicationException [Root exception is java.net.ConnectException: t3://host:port: Destination unreachable; nested exception is: java.net.ConnectException: Connection refused: connect; No available router to destination] ...This exception disappears after the server is started. However, no further messages are consumed by this Applet client, even though messages are being sent to ther Topic.This problem, described in Oracle Bug 8121602, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.3.55 Application Deployment Failure When Working Directory Not Set For Local Disk Used By Lvm

Description: If you create a local disk for the Logical Volume Manager (LVM), the current working directory defaults to the /domain directory on the local disk. If the weblogic.RootDirectory refers to another directory, either on an NFS mount or on the local disk, application deployments can fail, particularly if the application contains webservices.

Severity: Warning

Rationale: Development

17.3.56 Application State Hangs With State_Update_Pending After Weblogic.Deployer Runs Redeploy

Description: For Oracle WebLogic Server 9.2 Maintenance Pack 2 or Maintenance Pack 3, an application state can hang with STATE_UPDATE_PENDING status, after the WebLogic.Deployer utility runs redeploy to update files in an application multiple times. This issue happens intermittently.

Severity: Minor Warning

Rationale: Administration

17.3.57 Application With A Web Module Mapped To Different Context Roots Fails To Deploy. (Upgrade)

Description: Applications with Web modules mapped to different context roots can fail to deploy.The following is a sample application.xml configuration file:<?xml version="1.0" encoding="UTF-8"?><application xmlns="http://java.sun.com/xml/ns/j2ee" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://java.sun.com/xml/ns/j2eehttp://java.sun.com/xml/ns/j2ee/application_1_4.xsd" version="1.4"> <display-name>pa</display-name> <module> <web> <web-uri>/web</web-uri> <context-root>pw</context-root> </web> </module> <module> <web> <web-uri>/web</web-uri> <context-root>test</context-root> </web> </module> </application>This problem, described in Oracle Bug 8108005, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.3.58 Applications Must Be Redeployed Upon Any Change Of The Webservicetimestampmbean

Description: Currently, applications must be redeployed after timestamp settings have been configured using Console or WebLogic Scripting Tool. This issue has been fixed.

Severity: Minor Warning

Rationale: Administration

17.3.59 Assertionerror Of Unable To Determine Parent Types For Userlockoutmanage

Description: When using Oracle WebLogic Server 9.2 SNMP Counter monitor, this exception is thrown:ExecuteRequest failed java.lang.AssertionError: Unable to determine parent types for UserLockoutManagerRuntime: while calculating parent for com.bea:ServerRuntime=AdminServer,Name=UserLockoutManager,Type=UserLockoutManagerRuntime,Location=AdminServer,RealmRuntime=myrealm,ServerSecurityRuntime=AdminServer.java.lang.AssertionError: Unable to determine parent types for UserLockoutManagerRuntime: while calculating parent for com.bea:ServerRuntime=AdminServer,Name=UserLockoutManager,Type=UserLockoutManagerRuntime,Location=AdminServer,RealmRuntime=myrealm,ServerSecurityRuntime=AdminServer at weblogic.management.WebLogicObjectName.setParentFromObjectName(WebLogicObjectName.java:900) ...

Severity: Minor Warning

Rationale: Administration

17.3.60 Assertionerror With Ejbs When Multiple Ejbtimerruntimembeans Created With The Same Name

Description: Oracle WebLogic Server was creating multiple EJBTimerRuntimeMBeans with the same name. As a result of the duplicate names, subsequent EJBTimerRuntimeMBeans with the same name failed to register or unregister. The following AssertionError appears in the server logs with message BEA-080004:An error was thrown by the RMI server:weblogic.management.remote.iiop.IIOPServerImpl.newClient(Ljava.lang.Object;) java.lang.AssertionError: Registered more than one instance with the same objectName :com.bea:ServerRuntime=myserver,Name=MedRecSessionBean,ApplicationRuntime=medrecapp, Type=EJBTimerRuntime, EJBComponentRuntime=MedRecSessionBeanWorkaround or Solution:Oracle WebLogic Server now uses unique names for the EJBTimerRuntimeMBean.

Severity: Critical

Rationale: Administration

17.3.61 Async Response Fail To Come Back When Client Cert And Server Cert Are The Same

Description: The receiver service requires inbound/outbound messages to be signed and encrypted. When the sender sends the request, the receiver is able to invoke the Web method; however, when an asynchronous response returns to the sender, an InvocationTargetException is thrown.

Severity: Warning

Rationale: Administration

17.3.62 Attempt To Use Javax.Xml.Soap.Text.Iscomment() Of Saaj 1.1 Results In Unsupportedoperation

Description: The J2EE v1.4 specification shows javax.xml.soap.Text contains the method isComment(). When used in Oracle WebLogic Server 9.1 and Oracle WebLogic Server 9.2, the implementation class of weblogic.Web

service.core.soap.SOAPTextElement (SOAPTextElement.java:43) throws the following exception:java.lang.UnsupportedOperationException: This class does not support SAAJ 1.1The actual class/method in question is javax.xml.soap.Text.isComment(), which appears to be implemented byweblogic.Web service.core.soap.SOAPTextElement.isComment().

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.3.63 Attempt To Use Javax.Xml.Soap.Text.Iscomment() Of Saaj 1.1 Results In Unsupportedoperation (Upgrade)

Description: The J2EE v1.4 specification shows javax.xml.soap.Text contains the method isComment(). When utilized in Oracle WebLogic Server 9.1 and Oracle WebLogic Server 9.2, the implementation class of weblogic.Web service.core.soap.SOAPTextElement (SOAPTextElement.java:43) throws the following exception:java.lang.UnsupportedOperationException: This class does not support SAAJ 1.1The actual class/method in question is javax.xml.soap.Text.isComment(), which appears to be implemented byweblogic.Web service.core.soap.SOAPTextElement.isComment().This problem, described in Oracle Bug 8089633, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.3.64 Attribute Msifilereplicationenabled Is Deprecated In Wls 9.X

Description: In earlier versions of Oracle WebLogic Server, a managed server saved a copy of its configuration data only when Managed Server Independence was enabled by means of the MSIFileReplicationEnabled attribute.In Oracle WebLogic Server 9.X, managed servers automatically maintain a local copy of the domain configuration. In Oracle WebLogic Server 9.X, Managed Server Independence (MSI) mode is enabled by default.

Severity: Minor Warning

Rationale: Administration

17.3.65 Bea06-114.00 - Application Code Installed On A Server May Be Able To Decrypt Passwords

Description: Any site that is running untrusted application code is susceptible to this vulnerability.Application code (for example, EJBs or servlets) can be coded in such a way so as to allow it to decrypt encrypted passwords on the server.This patch resolves the issue by protecting the code to disallow application access. Even after installing this patch, to optimize security Oracle recommends that application code should be inspected for suspicious code before being installed on the server.

Severity: Critical

Rationale: Administration

17.3.66 Bea06-116.00 - Non-Active Security Provider Appears Active

Description: Newly configured security providers appear to be active despite the fact that the server will not use them until after a server restart. After configuring a new security provider, it may appear that the provider is active before a server restart, as

no indication is given that the server is still using the security providers from the last restart. This may lead an administrator to delete or add users, and delete or add security policies to the new provider. The patch for Security Advisory BEA06-116.00 ensures that the WebLogic Administration Console and WebLogic Scripting Tool properly display a warning that the server must be rebooted before a new security provider becomes active. WebLogic Scripting Tool will now display the correct providers in the runtime tree.

Severity: Critical

Rationale: Administration

17.3.67 Bea06-117.00 - Connectionfilters May Leave Server Vulnerable To A Denial-Of-Service Attack

Description: Under certain conditions, connection filters may cause server slowdown, which could make the server vulnerable to a denial-of-service attack.

Severity: Critical

Rationale: Performance

17.3.68 Bea06-119.00 - Vulnerability Of User-Specified Jndi Resources

Description: When using the WebLogic Server Console to set security policies on JNDI resources, the security policies do not properly protect the JNDI resources.

Severity: Critical

Rationale: Server Outage

17.3.69 Bea06-124.00 - Applications Installed On Weblogic Server Can Obtain Private Keys

Description: All sites that allow untrusted applications to be hosted in the server are vulnerable to this issue.An application hosted in the server can obtain the private keys.This patch resolves the issue by restricting access to the private keys.

Severity: Critical

Rationale: Server Outage

17.3.70 Bea06-124.00 - Applications Installed On Weblogic Server Can Obtain Private Keys

Description: All sites that allow untrusted applications to be hosted in the server are vulnerable to this issue.An application hosted in the server can obtain the private keys.This patch resolves the issue by restricting access to the private keys.

Severity: Critical

Rationale: Server Outage

17.3.71 Bea06-126.00 - Console Incorrectly Set Jdbc Policies

Description: All sites where administrators have used the WebLogic Server Administration Console to set custom JDBC security policies are vulnerable to this issue. Sites where the console has not been used to set JDBC security policies are not affected.When setting JDBC security policies, the console was not setting them correctly. This could result in those JDBC resources not being properly secured.This

patch resolves the issue by correcting how the console sets JDBC security policies.After the patch is applied, all JDBC policies will need to be reviewed to ensure correctness.

Severity: Critical

Rationale: Administration

17.3.72 Bea06-127.00 - Weblogic Server Http Handlers Log Username And Password On Failure

Description: All sites that that use WebLogic Server HTTP handlers and that host protected Java Web Service (JWS) or web apps are affected by this issue.If access to a protected JWS or web app fails, the username and password used in the access attempt may be logged to the server log. This can result in the password (either valid or invalid) being visible in clear text in the WebLogic Server log.This patch resolves the issue by ensuring that the username and password are removed from the failure message written to the log.

Severity: Critical

Rationale: Server Outage

17.3.73 Bea06-81.02 - Remote Anonymous Binds Are Possible To The Embedded Ldap Server

Description: All sites are vulnerable to this attack.It is possible for a remote user to bind anonymously to the embedded LDAP server and 1) look at user entries (but not attributes) if the schema can be guessed, or 2) launch a denial-of-service attack against the embedded LDAP server by creating many connections to the LDAP server.The patch for Security Advisory BEA06-81.02 resolves the issue by adding an attribute to restrict anonymous bind. After applying this patch and rebooting, anonymous bind will be restricted by default.

Severity: Critical

Rationale: Administration

17.3.74 Bea07-136.00 - Jdbcdatasourcefactory Mbean Password Field Is Not Encrypted

Description: All sites with JDBCDataSourceFactory MBeans that use the Properties attribute to store a password are vulnerable to this issue.A password entered in the JDBCDataSourceFactory MBean Properties was not being removed and encrypted in the Password attribute. This behavior allowed an administrator to view the password in clear text.This patch resolves the issue by ensuring that a password entered in the JDBCDataSourceFactory MBean Properties attribute is properly protected.

Severity: Critical

Rationale: Administration

17.3.75 Bea07-138.00 - Problem With Certificate Validation On Weblogic Server Web Service Clients

Description: This vulnerability can occur in WebLogic clients using Web Services Security (WSSE). In special circumstances an attacker may be able to mount a man-in-the-middle attack.This patch corrects validation to prevent this attack.

Severity: Critical

Rationale: Non-User Viewable Errors

17.3.76 Bea07-143.00 - Ws-Security Runtime Fails To Enforce Decryption Certificate

Description: The Web Services Security (WSSE) runtime may fail to enforce the use of a credential configured for decrypting messages sent by a client. In specific circumstances a malicious remote client may be able to exploit this vulnerability and bypass the application configured security. Patches are available to enforce proper validation by the WSSE runtime.

Severity: Critical

Rationale: Non-User Viewable Errors

17.3.77 Bea07-144.00 - Ejb Calls Can Be Unintentionally Executed With Administrative Privileges

Description: This vulnerability may occur in a transactional Message Driven Bean (MDB) using EJB container persistence. Some of the persistence operations can be called with an administrative identity. This issue only occurs when using the WebLogic Server 6.1 compatibility realm.This advisory resolves the issue by enforcing the execution of these operations with the proper identity.

Severity: Critical

Rationale: Administration

17.3.78 Bea07-145.00 - Permissions On Ejb Methods With Array Parameters May Not Be Enforced

Description: A vulnerability has been found in WebLogic Server in which a security policy created via the console on an EJB method with array parameters may not be enforced. An attacker could exploit this vulnerability to gain unauthorized access to these particularly defined EJB methods.This advisory resolves the issue by properly enforcing EJB security restrictions.

Severity: Critical

Rationale: Administration

17.3.79 Bea07-146.00 - Denial-Of-Service Vulnerability In The Proxy Plug-In For Apache Web Server

Description: Under certain circumstances, the WebLogic Server proxy plug-in for Apache web server may not properly handle a protocol error. As a result, the proxy plug-in could cause the Apache server to fail or to mark back-end WebLogic servers as unavailable. Open sessions may fail and applications hosted by back-end WebLogic servers may be unreachable. All applications using the WebLogic Server proxy plug-in on an Apache web server are vulnerable to this.

Severity: Critical

Rationale: User Viewable Errors

17.3.80 Bea07-147.00 - Malformed Http Requests May Reveal Data From Previous Requests

Description: An error has been found in the handling of malformed HTTP requests in WebLogic Server. An attacker could exploit this condition to find data involved in previous requests on the server, potentially from other users.This advisory resolves the problem by enforcing proper handling for this type of request.

Severity: Critical

Rationale: Administration

17.3.81 Bea07-149.00 - Security Policy Changes May Not Be Seen By Managed Server

Description: All sites that use admin servers to set security policy for managed servers are vulnerable.In very specific circumstances a policy change made on an admin server for a currently unavailable managed server will never reach the managed server. This is caused by a problem in the handling of the admin server's change log.This would lead to an administrator thinking that the managed server was running with the latest security policies when in fact the managed server might be running with an older set of security policies.This patch resolves the issue by ensuring that security policies will be correctly sent to the managed server.

Severity: Critical

Rationale: Administration

17.3.82 Bea07-150.00 - A Denial Of Service Attack Is Possible On Wls Running On Solaris 9

Description: A client can mount a denial of service attack by manipulating socket connections to a WebLogic Server running on Solaris 9. As a result of this attack, the server may not be able to process other valid requests. This advisory resolves the issue by closing the bad socket connections.

Severity: Critical

Rationale: Administration

17.3.83 Bea07-151.00 - Inadvertent Removal Of Access Restrictions

Description: Any sites that use roles and entitlements to manage WebLogic Portal resources are susceptible to this vulnerability. If an administrative user deletes entitlements for a given role other roles entitlements are inadvertently affected.This patch resolves the issue by enforcing proper access restrictions.

Severity: Critical

Rationale: Administration

17.3.84 Bea07-156.00 - Inadvertent Corruption Of Weblogic Portal Entitlement Policies

Description: Sites that operate in an Oracle WebLogic Server clustered environment and use WebLogic Portal entitlements to manage WebLogic Portal resources are susceptible to this vulnerability. If an administrative user changes a WebLogic Portal entitlement policy on a managed server while the Administrative Server is down, the policy change may not be successfully propagated to the other managed servers in the

cluster.This patch resolves the issue by preventing entitlement policy changes when the Administration server is down.

Severity: Critical

Rationale: Administration

17.3.85 Bea07-161.00 - Weblogic Server Embedded Ldap May Be Susceptible To A Brute Force Attack

Description: On specific configurations, the Oracle WebLogic Server embedded LDAP does not limit or audit failed login attempts, and an attacker, inside the firewall, could mount a trial and error attempt to guess the administrator's password. The attacker can also produce a denial of service condition on the LDAP port with the repeated attempts to logon.This advisory resolves this condition by allowing the definition of quotas limiting the usage of the WebLogic Server embedded LDAP. The quotas limit the maximum number of connections, the maximum number of operations per connection, the maximum number of connections per subject, and the maximum number of connections per IP address. In addition, login attempts and information about exceeded quotas are logged.

Severity: Critical

Rationale: Administration

17.3.86 Bea07-162.00 - Admin Console May Display Sensitive Web Service Attributes In Clear Text

Description: The Administration Console supports the configuration of Web Service security to secure particular web services. Administrators can specify security properties required for a particular web service, including passwords used by credential providers and token handlers. During the creation of the configuration, the console may display these sensitive attributes in clear text. However, these sensitive attributes are correctly encrypted when the configuration is written to disk.A patch is available to correct this issue by updating the Administration Console pages so that Web Service Security credential provider and token handler sensitive properties are not displayed in clear text.

Severity: Critical

Rationale: Administration

17.3.87 Bea07-163.00 - Wlst Script Generated By Configtoscript May Not Encrypt Attributes

Description: The WebLogic configToScript command converts an existing server configuration to an executable WebLogic Scripting Tool script and the resulting script can be used to create a new WebLogic domain. However, the generated script may not encrypt sensitive attributes (in particular, the node manager password) when a new domain is created with the script.A patch is available to allow proper encryption of these sensitive attributes.

Severity: Critical

Rationale: Server Outage

17.3.88 Bea07-164.01 - Security Policy May Not Be Applied To Weblogic Administration Deployers

Description: Security advisory BEA07-164.01 contains the corrected remedy for this vulnerability on Oracle WebLogic Server and WebLogic Express 9.1 and 9.0. This advisory supersedes security advisory BEA07-164.00.

Severity: Critical

Rationale: Server Outage

17.3.89 Bea07-166.00 - Cross-Site Scripting Attacks In The Weblogic Portal Groupspace Application

Description: Rich text content in the WebLogic GroupSpace application is susceptible to cross-site scripting (XSS) attacks. Because rich text content in GroupSpace is actually HTML, it is possible for an authenticated user to add malicious JavaScript code that will execute in another users' environment (e.g., browser) when the HTML is rendered.This patch gives administrators a way to prevent this vulnerability by providing a configurable option to turn off the rich text editor and use a plain text editor instead.

Severity: Critical

Rationale: Administration

17.3.90 Bea07-167.00 - Inadvertent Corruption Of Entitlements Could Result In Unauthorized Access

Description: An authenticated WebLogic Portal administrator or Delegated administrator may cause an inadvertent corruption of a visitor entitlements role when editing the role description if more than 255 characters are entered. This will cause any resources that were protected to no longer be protected. This vulnerability can occur by either editing a role description via the WebLogic Portal Administration Console or through a portal application using the WebLogic Portal APIs.A fix has been provided which prevents the entry of more than 255 characters.

Severity: Critical

Rationale: Administration

17.3.91 Bea07-169.00 - Ssl May Verify Rsa Signatures Incorrectly If The Rsa Key Exponent Is 3

Description: WebLogic SSL may verify incorrectly RSA signatures if the RSA public key exponent is 3. An attacker can create certificates with a forged signature that makes the SSL certificate chain to be improperly verified as valid.This advisory corrects this problem by rejecting RSA certificates with a public key exponent of 3.For additional details about this vulnerability, see the link to Mitre in the For More Information section.

Severity: Critical

Rationale: Administration

17.3.92 Bea07-170.00 - Exposure Of Filenames In Development Mode

Description: The WebLogic Workshop Test View may reveal parent directory information to the WebLogic Workshop Directory (wlwdir) when the application is deployed in an exploded format in a development environment. The WebLogic Workshop Test View console should always be disabled in a production environment.WebLogic Integration 9.2 is only susceptible if the application is deployed explicitly in an exploded form. By default, WebLogic Integration 9.2 does not use the exploded deployment model.This patch resolves this problem by preventing users from navigating beyond the corresponding web application directory.

Severity: Critical

Rationale: Administration

17.3.93 Bea07-171.00 - Non-Trusted Applets May Be Able To Elevate Privileges

Description: The Sun Java Runtime Environment (JRE) contains vulnerabilities that can allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable system.There were two vulnerabilities related to serialization in the Java Runtime Environment. These vulnerabilities would allow a malicious applet or application to elevate its privileges. Earlier BEA JRockit releases supporting applets may be affected by this issue. The latest version of Oracle JRockit JVM cannot be used to run applets, so it is not affected by this issue.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.3.94 Bea07-172.00 - Buffer Overflow In Processing Gif Images

Description: A buffer overflow while processing GIF images in the Java Runtime Environment may allow a malicious applet to elevate its privileges. For example, an applet may grant itself permissions to read and write local files or execute local applications with the privileges of the user running the applet. Earlier versions of BEA JRockit supporting applets may be affected by this issue. Newer versions of BEA JRockit cannot be used to run applets.Under special circumstances, a server running BEA JRockit may also be affected if it can receive (through a web upload) a maliciously crafted image and this image is decoded in the server.

Severity: Critical

Rationale: Administration

17.3.95 Bea07-173.00 - Application Started Through Web Start May Be Able To Elevate Privileges

Description: Java Web Start enables standalone Java applications to be launched from a browser. A vulnerability was reported in Java Web Start that allows a non-trusted application to elevate its privileges. For example, the non-trusted application could read and write local files accessible to the user running the Java Web Start Application. For more information, please contact Oracle Support or visit support.oracle.com.Early releases of BEA JRockit (prior to R26.0) may be affected by this vulnerability and patches are available to correct this problem. The latest releases of BEA JRockit do not ship with Java Web Start and are not affected by this vulnerability.

Severity: Critical

Rationale: Administration

17.3.96 Bea07-174.00 - Non-Trusted Applets May Be Able To Elevate Privileges

Description: The Sun Java Runtime Environment contains vulnerabilities that can allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable system.Two buffer overflow conditions have been identified that may allow non-trusted applets to elevate their privileges. For example, an applet might be able to grant itself permission to read and write local files, or execute local applications that are accessible to the user running the non-trusted applet. Earlier versions of BEA JRockit supporting applets may be affected by these issues.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.3.97 Bea07-175.00 - Ssl Clients May Miss Possible Cipher Suites Resulting In Use Of Null Cipher (Wls V9)

Description: In some circumstances, SSL clients that run outside the server environment may not find all possible ciphers with which to construct the list of potential SSL cipher suites resulting in use of the default null cipher (no encryption).This advisory corrects this issue by supplying jars and instructions to ensure all cipher suites are found.

Severity: Critical

Rationale: Server Outage

17.3.98 Bea07-176.00 - Server May Select Null Cipher Suite For Ssl Communication With Ssl Clients. (Wls V9)

Description: An attacker could obtain and exploit information that is not encrypted when a null cipher suite is in use. Under certain circumstances, when a client does not offer support for any of the cipher suites available in the server, then the server may select a cipher suite that uses a null cipher; this may result in SSL communication that is not encrypted.This advisory corrects this issue by logging a message when null cipher is in use and also provides administrators the ability to disable the use of null ciphers during SSL communications with SSL clients.

Severity: Critical

Rationale: Server Outage

17.3.99 Bea07-177.00 - Multiple Security Vulnerabilities In The Java Runtime Environment

Description: Contact Oracle Support or visit support.oracle.com for the following information:- A JavaDoc defect may lead to the generation of HTML documentation pages with potential cross-site scripting (XSS) vulnerability.- A buffer overflow vulnerability in the JRE image parsing code may allow an untrusted applet or application to elevate its privileges.- A vulnerability in the JRE font parsing code may allow an untrusted applet to elevate its privileges.- The Java XML Digital Signature implementation in JDK and JRE 6 does not securely process XSLT stylesheets in XSLT Transforms in XML Signatures.- A JRE Applet Class Loader security vulnerability may

allow an untrusted applet that is loaded from a remote system to circumvent network access.

Severity: Critical

Rationale: Administration

17.3.100 Bea07-178.00 - Java Secure Socket Extension Does Not Correctly Process Ssl/Tls Handshake

Description: The Java Secure Socket Extension (JSSE) that is included in various releases of the Java Runtime Environment does not correctly process SSL/TLS handshake requests. This vulnerability may be exploited to create a Denial of Service (DoS) condition to the system as a whole on a server that listens for SSL/TLS connections using JSSE for SSL/TLS support. For more information, please contact Oracle Support or visit support.oracle.com.This advisory corrects this issue by supplying patched versions of JRockit.

Severity: Critical

Rationale: Administration

17.3.101 Bea08-159.01 - Requests Served Through Weblogic Proxy Servlets May Acquire More Privileges

Description: WebLogic HttpClusterServlet or HttpProxyServlet, configured with the "SecureProxy" parameter, may serve external requests to back-end WebLogic servers on behalf of a system identity instead of the proxy's own identity. These external requests may be wrongly granted access to certain administrative resources that are only accessible to an administrator.This advisory resolves the problem by enforcing the use of the proxy identity. The configuration of a proxy has also been enhanced to permit connections using two-way SSL.

Severity: Critical

Rationale: Administration

17.3.102 Bea08-191.00 - Tampering Html Request Headers Could Lead To An Elevation Of Privileges (Wls V9)

Description: An attacker can spoof certain information in a request header, which can potentially allow access to application servlets that rely on this information for authentication.This advisory corrects this issue by ensuring that the header information is properly handled before passing it to the servlet.

Severity: Critical

Rationale: Administration

17.3.103 Bea08-193.00 - Non-Authorized User May Be Able To Receive Messages From A Secured Jms (Wls V9)

Description: WebLogic security policies can be configured to restrict the access to a JMS destination. If an application user does not have the "receive" permission to a JMS destination (queue/topic), an attempt of receiving messages from that destination by the application should fail with security errors. By exploiting this vulnerability an unauthorized user may be able to receive messages from a standalone (physical) JMS Topic destination or a member of a secured Distributed Topic member

destination.This advisory resolves this issue by checking permissions before allowing a subscriber to use a durable subscription.

Severity: Critical

Rationale: Administration

17.3.104 Bea08-194.00 - A Non-Authorized User May Be Able To Send Messages To A Protected Queue. (Wls V9)

Description: The distributed queue feature in WebLogic JMS provides higher availability in a clustered environment. If a JMS client sends a message to a distributed queue and encounters a problem with one member of that distributed queue (the member is down, the member exceeds its quota, access denied, etc), internally the JMS subsystem will retry another member of the same distributed destination. In certain configurations, an unauthorized user is able to send messages to a secure distributed queue.This advisory corrects the problem and ensures that the correct user identity is maintained.

Severity: Critical

Rationale: Administration

17.3.105 Bea08-195.00 - Cross-Site Scripting Vulnerability In The Oracle Weblogic Server Administration Console Unexpected Exception Page. (Wls V9)

Description: The WebLogic Server Administration Console uses fields contained in a URL to identify which information should be included when displaying information to a user.An attacker may be able to inject JavaScript into the console output.This advisory corrects the cross site scripting issue by sanitizing the output.

Severity: Critical

Rationale: Administration

17.3.106 Bea08-196.00 - A Session Fixation Exploit Could Result In Elevated Privileges. (Wls V9.2)

Description: In order to exploit this vulnerability, an attacker must have access to the server's console login page and have a non-administrator user account on that server. A session fixation vulnerability exists which can result in elevation of the attacker's privileges. For more information about Session Fixation attacks, see:http://en.wikipedia.org/wiki/Session_fixationThis advisory corrects this issue by always regenerating an auth cookie on login.

Severity: Critical

Rationale: Administration

17.3.107 Bea08-197.00 - Account Lockout Can Be Bypassed, Allowing A Brute-Force Password Attack

Description: In order to avoid brute-force credential attacks, Oracle WebLogic Server has a mechanism that locks the corresponding user account after a certain number of invalid login attempts. By default, the account is locked after 5 invalid login attempts and remains locked for 30 minutes.Even after a user has been locked out, logon requests to certain carefully constructed URLs can still give hints as to whether the password is correct or not. This allows a sophisticated attacker to successfully run a

brute-force password attack, a dictionary attack, or other similar attacks. All sites that use servlets are vulnerable to this problem.The patch associated with this advisory corrects the problem.

Severity: Critical

Rationale: Administration

17.3.108 Bea08-199.00 - A Carefully Constructed Url May Cause Sun, Iis, Or Apache Web Servers To Crash. (Wls V9)

Description: An attacker can use a carefully constructed URL to cause BEA's proxy plugin to crash the Sun, IIS, or Apache web server process. On re-start, this may cause in-flight requests to be lost. This can cause a temporary denial of service. This attack can be exploited remotely, and the attacker does not require authentication.This advisory resolves the issue in the plugin by correctly handling URLs.

Severity: Critical

Rationale: Administration

17.3.109 Bea08-201.00 - Multiple Security Vulnerabilities In The Java Runtime Environment

Description: This is a combined security advisory. These vulnerabilities are fixed in JRockit R27.5.0. Installers, updates, patches and more information are available at support.oracle.com.

Severity: Critical

Rationale: Administration

17.3.110 Bea08-80.04 - Patches Available To Prevent Multiple Cross-Site Scripting Vulnerabilities (Wls V9)

Description: Cross-Site Scripting (XSS) vulnerabilityFor more information, see:http://download.oracle.com/docs/cd/E13222_01/wls/docs81/servlet/progtasks.html#160803Caution About Existing Samples:Our samples are intended to provide a simple tutorial regarding a few specific features. They are not comprehensive guides to best practices. Many of them omit the use of the Utils.encodeXSS() method or other XSS preventative techniques in needed places and are hence vulnerable to XSS attacks.

Severity: Critical

Rationale: Administration

17.3.111 Best Practices For Configuring Outbound Load Balancing Requests

Description: When using Oracle WebLogic Tuxedo Connector, Oracle support recommends the following best practices:For load balancing outbound requests, configure the imported service with multiple entries using a different key. The imported service uses a composite key to determine each record's uniqueness. The composite key is compose of the following:<service name> + <local access point> + <primary route in the remote access point list>

Severity: Minor Warning

Rationale: Performance

17.3.112 Better Way Of Handling Large Log Messages Is Required

Description: The LogBroadcaster fails to broadcast log messages when the log message is large. Messages bigger than 64k fail to be broadcast. This size limitation was introduced in Oracle WebLogic Server 9.x.Error message:<BEA-170011> <The LogBroadcaster on this server failed to broadcast log messages to the admin server. The Admin server may not be running. Message broadcasts to the admin server will be disabled.>

Severity: Warning

Rationale: Administration

17.3.113 Blank Userid Or Password In Username Token Profile Results In Nullpointerexception

Description: When userid and password for username token profile is blank, the server returns NullPointerException, as below:java.lang.NullPointerExceptionat weblogic.xml.crypto.utils.DOMUtils.getText(DOMUtils.java:237)at weblogic.xml.crypto.wss.UsernameTokenImpl.unmarshal(UsernameTokenImpl.java:322)

Severity: Minor Warning

Rationale: Administration

17.3.114 Boxing Conversion Of Small Integer Values Incorrect In Oracle Jrockit R27.2.X And R27.3.X

Description: The following Java class should produce TRUE for Integer values within the range(-128...+127). However, with Oracle JRockit releases R27.2.X and R27.3.X, this may return FALSE.public class Test { public static void main(String[] args) { Integer i1 = 4, i2 = 4; System.out.println(i1 == i2); }}

Severity: Minor Warning

Rationale: Development

17.3.115 Bridge Startup Fails If Connection Url Is Blank For The Bridge Destination (Upgrade)

Description: Oracle WebLogic Server cannot start the JMS bridge if the connection URL was not provided.This problem, described in Oracle Bug 8057089, has been fixed in Oracle WebLogic Server 9.1.

Severity: Minor Warning

Rationale: Subsystem Outage

17.3.116 Corba Strings Encoded In Extended Utf-8 Character Set Are Not Parsed Correctly

Description: CORBA strings encoded in extended UTF-8 character set, wherein a high bit is set, are not correctly parsed by the output stream handler. This is because the IIOPOutputStream.write_string is not correctly handling UTF-8 encoded strings, instead it is parsing them as ASCII.

Severity: Minor Warning

Rationale: Administration

17.3.117 Corba Strings Encoded In Extended Utf-8 Character Set Are Not Parsed Correctly. (Upgrade)

Description: CORBA strings encoded in extended UTF-8 character set, wherein a high bit is set, are not correctly parsed by the output stream handler. This is because the IIOPOutputStream.write_string is not correctly handling UTF-8 encoded strings, instead it is parsing them as ASCII.This problem, described in Oracle Bug 8105677, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.3.118 Cve-2008-1006 - Multiple Security Vulnerabilities In Jrockit

Description: Advisory CVE-2009-1006 refers to all the vulnerability fixes that have been made in JRockit for addressing the applicable issues. The applicable advisories include:CVE 2008-5347CVE 2008-5348CVE 2008-5349CVE 2008-5350CVE 2008-5351CVE 2008-5352CVE 2008-5353CVE 2008-5354CVE 2008-5356CVE 2008-5360xFor more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.3.119 Cve-2008-2576 - Information Disclosure Vulnerability In The Foreignjms Component

Description: Information Disclosure vulnerability in the ForeignJMS component.

Severity: Critical

Rationale: Administration

17.3.120 Cve-2008-2577 - Elevation Of Privilege Vulnerability In The Console/Wlst

Description: Elevation of privilege vulnerability in the Console/WLST.

Severity: Critical

Rationale: Administration

17.3.121 Cve-2008-2578 - Information Disclosure Vulnerability In The Weblogic Console Or Server Log

Description: Information Disclosure vulnerability in the WebLogic console or server log.

Severity: Critical

Rationale: Administration

17.3.122 Cve-2008-2579 - Information Disclosure Vulnerability In Weblogic Plug-Ins For Web Servers (Wls V9)

Description: Information disclosure vulnerability in WebLogic Server plug-ins for Apache, Sun, and IIS Web servers.

Severity: Critical

Rationale: Administration

17.3.123 Cve-2008-2580 - Information Disclosure In Jsp Pages (Wls V9)

Description: Information disclosure in JSP pages.

Severity: Critical

Rationale: Administration

17.3.124 Cve-2008-2581 - Elevation Of Privilege Vulnerabilities In The Uddi Explorer. (Wls V9)

Description: Elevation of privilege vulnerabilities in the UDDI Explorer.

Severity: Critical

Rationale: Administration

17.3.125 Cve-2008-2582 - Denial-Of-Service Vulnerability In Weblogic Server (Oracle Weblogic Server 9.X)

Description: Denial-of-Service vulnerability in WebLogic Server (Oracle WebLogic Server 9.x)

Severity: Critical

Rationale: Server Outage

17.3.126 Cve-2008-3103 - Security Vulnerability In Java Management Extensions (Jmx)

Description: A vulnerability in the Java Management Extensions (JMX) management agent included in the Java Runtime Environment (JRE) may allow a JMX client running on a remote host to perform unauthorized operations on a system running JMX with local monitoring enabled.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.3.127 Cve-2008-3104 - Security Vulnerabilities In Java Runtime Environment Allows Same Origin

Description: Security vulnerabilities in the Java Runtime Environment may allow an untrusted applet that is loaded from a remote system to circumvent network access restrictions and establish socket connections to certain services running on machines other than the one that the applet was downloaded from. This may allow the untrusted remote applet the ability to exploit any security vulnerabilities existing in

the services it has connected to.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.3.128 Cve-2008-3105 - Security Vulnerability In The Java Runtime Environment Related Xml Data

Description: A vulnerability in the Java Runtime Environment related to the processing of XML data may allow unauthorized access to certain URL resources (such as some files and web pages) or a Denial of Service (DoS) condition to be created on the system running the JRE.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.3.129 Cve-2008-3106 - Security Vulnerability In The Java Runtime Environment Related To Xlm Data

Description: A vulnerability in the Java Runtime Environment with processing XML data may allow an untrusted applet or application that is downloaded from a website unauthorized access to certain URL resources (such as some files and web pages).For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.3.130 Cve-2008-3108 - A Security Vulnerability With The Processing Of Fonts In The Java Runtime

Description: A buffer overflow security vulnerability with the processing of fonts in the Java Runtime Environment (JRE) may allow an untrusted applet or application to elevate its privileges. For example, an untrusted applet may grant itself permissions to read and write local files or execute local applications that are accessible to the user running the untrusted applet.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.3.131 Cve-2008-3109 - Security Vulnerability In The Java Runtime Environment Scripting Language

Description: A vulnerability in the Java Runtime Environment relating to scripting language support may allow an untrusted applet or application to elevate its privileges. For example, an untrusted applet may grant itself permissions to read and write local files or execute local applications that are accessible to the user running the untrusted applet.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.3.132 Cve-2008-3110 - Security Vulnerability In The Java Runtime Environment Scripting Language

Description: A vulnerability in the Java Runtime Environment relating to scripting language support may allow an untrusted applet to access information from another applet.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.3.133 Cve-2008-3257 - Security Vulnerability In Oracle Weblogic Server Plug-In For Apache (Wls V9)

Description: Recently an exploit has been made public which may impact the availability, confidentiality or integrity of WebLogic Server applications which use the Apache web server configured with the WebLogic plug-in for Apache. This vulnerability may be remotely exploitable without authentication (that is, it may be exploited over a network without the need for a username and password).

Severity: Critical

Rationale: Server Outage

17.3.134 Cve-2008-4008 - Security Vulnerability In Weblogic Plug-In For Apache

Description: This vulnerability may impact the availability, confidentiality, or integrity of WebLogic Server applications which use the Apache web server configured with the WebLogic plug-in for Apache. This vulnerability may be remotely exploitable without authentication, that is, it may be exploited over a network without the need for a username and password.

Severity: Critical

Rationale: Administration

17.3.135 Cve-2008-4009 - Elevation Of Privilege Vulnerability If More Than One Authorizer Is Used

Description: If you configure more than one authorizer (e.g. an XACMLAuthorizer and a DefaultAuthorizer), certain elevation of privileges may occur for some resources.

Severity: Critical

Rationale: Administration

17.3.136 Cve-2008-4010 - Elevation Of Privilege Vulnerability In Some Netui Tags (Wls V9)

Description: This vulnerability in some NetUI tags may allow an attacker to read unauthorized data.

Severity: Critical

Rationale: Administration

17.3.137 Cve-2008-4011 - Elevation Of Privileges For Some Applications (Wls V9.0)

Description: Under certain conditions, some applications in admin state may be made available to non admin users.

Severity: Critical

Rationale: Administration

17.3.138 Cve-2008-4011 - Elevation Of Privileges For Some Applications (Wls V9.1)

Description: Under certain conditions, some applications in admin state may be made available to non admin users.

Severity: Critical

Rationale: Administration

17.3.139 Cve-2008-4011 - Elevation Of Privileges For Some Applications (Wls V9.2)

Description: Under certain conditions, some applications in admin state may be made available to non admin users.

Severity: Critical

Rationale: Administration

17.3.140 Cve-2008-4013 - Protected Web Applications May Be Displayed Under Certain Conditions. (Wls V9.0)

Description: If you upgrade from Oracle WebLogic Server 8.1 Maintenance Pack 3 to a higher version and use auth-method as CLIENT-CERT, some web apps which were protected in Oracle WebLogic Server 8.1 Maintenance Pack 3 may be made available to an invalid user.

Severity: Critical

Rationale: Administration

17.3.141 Cve-2008-4013 - Protected Web Apps May Be Displayed Under Certain Conditions (Wls V9.1)

Description: If you upgrade from Oracle WebLogic Server 8.1 Maintenance Pack 3 to a higher version and use auth-method as CLIENT-CERT, some Web applications which were protected in Oracle WebLogic Server 8.1 Maintenance Pack 3 may be made available to an invalid user.

Severity: Critical

Rationale: Administration

17.3.142 Cve-2008-4013 - Protected Web Apps May Be Displayed Under Certain Conditions. (Wls V9.2)

Description: If you upgrade from Oracle WebLogic Server 8.1SP3 to a higher version and use auth-method as CLIENT-CERT, some web apps which were protected in Oracle WebLogic Server 8.1SP3 may be made available to an invalid user.

Severity: Critical

Rationale: Administration

17.3.143 Cve-2008-5457 - Security Vulnerability In Oracle Weblogic Server Plug-Ins For Apache, Sun, And Iis Web Servers. (Wls V9)

Description: This vulnerability may impact the availability, confidentiality, or integrity of WebLogic Server applications, which use the Apache, Sun, or IIS Web server configured with the WebLogic plug-in for Apache, Sun, or IIS servers, respectively. This vulnerability may be remotely exploitable without authentication; that is, it may be exploited over a network without the need for a username and password.

Severity: Critical

Rationale: Administration

17.3.144 Cve-2008-5460 - Information Disclosure Vulnerability In Jsp And Servlets (Wls V9)

Description: Certain circumstances may cause some information disclosure in WebLogic Server JSPs and servlets.

Severity: Critical

Rationale: Subsystem Outage

17.3.145 Cve-2008-5461 - Elevation Of Privilege Vulnerability In Weblogic Console

Description: This vulnerability in WebLogic Console may allow information disclosure and elevation of privileges. This may be exploited over a network.

Severity: Critical

Rationale: Administration

17.3.146 Cve-2008-5462 - Elevation Of Privilege Vulnerability In Weblogic Portal (Wls V9.2)

Description: This vulnerability in WebLogic Portal may allow elevation of privileges. This may be exploited over a network.

Severity: Critical

Rationale: Administration

17.3.147 Cve-2009-0217 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle JRockit R27.6.3 JRE/JDK 1.6.0_11. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.3.148 Cve-2009-0217 - Critical Patch Update Notice (Wls V9)

Description: Oracle has released Critical Patch Updates for July 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic 9.0, 9.1 and 9.2. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Server Outage

17.3.149 Cve-2009-1002 - Elevation Of Privilege Vulnerability In Weblogic Server (Wls V9)

Description: This vulnerability in WebLogic Server may allow elevation of privileges. This may be exploited over a network.

Severity: Critical

Rationale: Administration

17.3.150 Cve-2009-1003 - Source Code Access Vulnerability In Web Pages, Weblogic Server (Wls V9)

Description: This vulnerability in Oracle WebLogic Server may allow access to source code of Web pages. This may be exploited over a network.

Severity: Critical

Rationale: Administration

17.3.151 Cve-2009-1012 - Security Vulnerability In Weblogic Plug-In For Apache Web Server

Description: This vulnerability may impact the availability, confidentiality, or integrity of WebLogic Server applications, which use the Apache, Sun, or IIS web server configured with the WebLogic plug-in for Apache, Sun, or IIS servers, respectively. This vulnerability may be remotely exploitable without authentication. That is. it may be exploited over a network without the need for a username and password.

Severity: Critical

Rationale: Administration

17.3.152 Cve-2009-1016 - Security Vulnerability In Oracle Weblogic Server Plug-Ins For Apache, Sun, And Iis Servers

Description: This vulnerability may impact the availability, confidentiality, or integrity of Oracle WebLogic Server applications, which use the Apache, Sun, or IIS web server configured with the WebLogic Server plug-ins for Apache, Sun, or IIS servers, respectively.

Severity: Critical

Rationale: Administration

17.3.153 Cve-2009-1094 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for July 2009 that provide corrective action for potential security vulnerabilities for Oracle JRockit R27.6.3 and earlier JRE and JDK 6, R27.6.3 and earlier JRE and JDK 5.0, R27.6.3 and earlier SDK and JRE 1.4.2. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.3.154 Cve-2009-1974 - Critical Patch Update Notice (Wls V9)

Description: Oracle has released Critical Patch Updates for July 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.0, 9.1, and 9.2.

Severity: Critical

Rationale: Server Outage

17.3.155 Cve-2009-2002 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Portal 10.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.3.156 Cve-2009-2002 - Critical Patch Update Notice (Wls V9.2)

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Portal 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.3.157 Cve-2009-2625 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle JRockit 1.5.0_19 and 1.6.0_14.Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.3.158 Cve-2009-3396 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.0, 9.1, and 9.2. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Server Outage

17.3.159 Cve-2009-3403 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle JRockit 1.6.0_14, 1.5.0_19 and 1.4.2_21. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.3.160 Cve-2009-3555 - Critical Patch Update Notice (Wls V9)

Description: Oracle has released a Critical Patch Update that provides corrective action for a potential security vulnerability for Oracle WebLogic Server 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.3.161 Cve-2010-0068 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.3.162 Cve-2010-0069 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.3.163 Cve-2010-0073 - Critical Patch Update Notice (Wls V9)

Description: Oracle has released a Critical Patch Update that provides corrective action for a potential security vulnerability for Oracle WebLogic Server 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.3.164 Cve-2010-0074 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.3.165 Cve-2010-0078 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.3.166 Cve-2010-0079 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle JRockit 1.6.0_14, 1.5.0_19 and 1.4.2_21. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.3.167 Cve-2010-0849 - Critical Patch Update Notice

Description: Oracle has released a Critical Patch Update that provides corrective action for a potential security vulnerability for Oracle JRockit R27.6.6: JRE/JDK 1.4.2, 5 and 6; R28.0.0, JRE/JDK 5 and 6. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.3.168 Cve-2010-2375 - Critical Patch Update Notice (Wls V9)

Description: Oracle has released a Critical Patch Update that provides corrective action for a potential security vulnerability for Oracle WebLogic Server 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.3.169 Can'T Set The Plug-In Enabled Property On The Administration Console

Description: There is no way to set the WeblogicPluginEnabled attribute of the ClusterMBean from the Administration console.This issue has been resolved by providing a check box for setting ClusterMBean's WeblogicPluginEnabled attribute in the advanced setting of the Cluster - > Configuration - > General tab page.

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.3.170 Can'T Set The Plug-In Enabled Property On The Administration Console. (Upgrade)

Description: There is no way to set the WeblogicPluginEnabled attribute of the ClusterMBean from the Administration console.This issue has been resolved by providing a check box for setting ClusterMBean's WeblogicPluginEnabled attribute in the advanced setting of the Cluster - > Configuration - > General tab page.This problem, described in Oracle Bug 8130511, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.3.171 Cannot Configure Config-Backup-Enabled Via Administration Console

Description: To archive configuration files, you must configure the following two parameters:* archive-configuration-count* config-backup-enabledHowever, for Oracle WebLogic Server 9.x, you cannot configure these parameters from the Administration Console.

Severity: Minor Warning

Rationale: Administration

17.3.172 Cannot Create More Than 100 Wtc Import Services On Administration Console

Description: You cannot create more than 100 WTC (Oracle WebLogic Tuxedo Connector) imported services via the Administration Console. If you attempt to do so, the following type of error appears:Errors must be corrected before proceeding. Bean already exists:"weblogic.management.configuration.WTCImportMBeanImpl@13f4e919([C720485]/WTCServers[wtc_zt5]/WTCImports[WTCImportedService-99])"

Severity: Minor Warning

Rationale: Administration

17.3.173 Cannot Create More Than 100 Wtc Import Services On Administration Console. (Upgrade)

Description: You cannot create more than 100 Oracle WebLogic Tuxedo Connector imported services via the Administration Console. If you attempt to do so, the following type of error appears:Errors must be corrected before proceeding. Bean already exists:"weblogic.management.configuration.WTCImportMBeanImpl@13f4e919([C720485]/WTCServers[wtc_zt5]/WTCImports[WTCImportedService-99])"This problem, described in Oracle Bug 8122138, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Administration

17.3.174 Cannot Deploy Web Service When Wsdl Xsd Referenced Is Not Accessible

Description: When deploying a Web Service Definition Language (WSDL) that references a schema from a URI that is not accessible, the Web Service fails to be deployed and is not available to service requests.

Severity: Warning

Rationale: Subsystem Outage

17.3.175 Cannot Detach Webservice Policies

Description: In the console, Policy attachments for Web Services can be specified for "inbound", "outbound" and "both" directions. Any new policies or changes to the direction of the policies get updated to the deployment plan but policies detached from operations are not removed from the deployment plan.

Severity: Minor Warning

Rationale: User Viewable Errors

17.3.176 Cannot Display More Than 50 Ldap Users In The Administration Console

Description: Only 50 of the LDAP users are displayed on the Oracle WebLogic Server Admin console even if the actual number is greater than 50. Need capability to list more than 50 users or groups from an external LDAP or database in the console

Severity: Minor Warning

Rationale: Administration

17.3.177 Cannot Dynamically Change Cookie Name Of Administration Console

Description: In Oracle WebLogic Server versions prior to 10.3, there is no way to dynamically change the cookie name of an Oracle WebLogic Server Administration Console. The workaround is to modify the CookieName in the weblogic.xml file in the console.war.

Severity: Minor Warning

Rationale: Administration

17.3.178 Cannot Manage The Jolt Connection Through Monitoring Tab

Description: The Oracle WebLogic Server Administration Console does not provide the ability to monitor connection details for a Jolt Connection Pool. This feature was present in previous versions of Oracle WebLogic Server.On Oracle WebLogic Server 8.1, the column Jolt connection is a hyperlink. It is a static HTML on Oracle WebLogic Server 9.1, and there is no other possibility to have Jolt connection info in the console.

Severity: Minor Warning

Rationale: Administration

17.3.179 Cannot Overwrite From Field When Sending From Business Service With Dummy Email Address

Description: If you have a Business Service with a dummy email address and you use a payload to overwrite the "To" and "From" portions of the transport header, the "From" portion may not be overwritten. For example, using the following payload:<test:sendMyMail xmlns:test="http://test"> <test:body>string</test:body> <test:from>someone@bea.com</test:from> <test:to>someoneelse@bea.com</ test:to></test:sendMyMail>The email arrives at the address defined in the "To" portion, and the "From" address remains the address defined in the Business Service. In other words, the "From" address is not overwritten. Setting "Pass all Headers through Pipeline" does not influence the result.

Severity: Warning

Rationale: Subsystem Outage

17.3.180 Cannot Set Plug-In Enabled Property On Administration Console

Description: In the Admin Console the selection for setting ClusterMBean's WeblogicPluginEnabled attribute is missing in the Cluster - Configuration - General tab page.

Severity: Minor Warning

Rationale: Administration

17.3.181 Cannot Set Plug-In Enabled Property On Administration Console. (Upgrade)

Description: In the Admin Console the selection for setting ClusterMBean's WeblogicPluginEnabled attribute is missing in the Cluster - Configuration - General tab page.This problem, described in Oracle Bug 8130511, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Administration

17.3.182 Cannot Update The Application With Adminconsole In Japanese Environment

Description: Applications deployed using the Administration Console Japanese edition cannot be updated because the Active Changes button is missing.

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.3.183 Cannot Use Javabean Which Has Multidimensional Array Property

Description: When building Web services, if you have a JavaBean that has multidimensional array property for parameter and result, the JWSC task fails with the following message: [jwsc] [SEVERE] Multidimensional arrays NYI [jwsc] on Java element 'test.ws.multidimensionalarrays.Data.StrArr'

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.3.184 Cannot Use Javabean Which Has Multidimensional Array Property. (Upgrade)

Description: When building Web services, if you have a JavaBean that has multidimensional array property for parameter and result, the JWSC task fails with the following message: [jwsc] [SEVERE] Multidimensional arrays NYI [jwsc] on Java element 'test.ws.multidimensionalarrays.Data.StrArr'This problem, described in Oracle Bug 8131580, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.3.185 Chainentityresolver Exception While Calling A Webservice (Wls V9.2)

Description: While invoking a Web Services Application based on Apache AXIS version 1.3, the following exception is logged:[[ACTIVE] ExecuteThread: '0' for queue:'weblogic.kernel.Default (self-tuning)'] DEBUG [TXID:]org.apache.axis.utils.XMLUtils - Failed to set EntityResolver on DocumentBuilderjava.lang.NullPointerException at weblogic.xml.jaxp.ChainingEntityResolver.popEntityResolver(ChainingEntityResolver.java:61) at weblogic.xml.jaxp.RegistryDocumentBuilder.setEntityResolver(RegistryDocumentBuilder.java:169) ...

Severity: Minor Warning

Rationale: User Viewable Errors

17.3.186 Changes In Dst Definitions Cause Issues With Basic Date Handling In Oracle Jrockit Jdk

Description: The recent change to the definition of US timezones to remove Daylight Savings Time (DST) awareness has broken basic functionality in date handling in multiple vendor JVMs, including Oracle JRockit 1.4.2_12. This issue affects sites using the three letter abbreviations for the deprecated DST timezone denotations, when using any affected JVM.The DateFormat parser uses the contents of String zoneStrings[][] in class DateFormatSymbols to identify the timezone based on the zone value in the input date string. For example, the zoneStrings[][] array defines "EST" before "America/New_York" and so sets the timezone for the parser to the EST zone, which is now unaware of DST.

Severity: Warning

Rationale: Not Complying with Specifications

17.3.187 Changes In Dst Definitions Cause Issues With Basic Date Handling In Oracle Jrockit Jdk

Description: The recent change to the definition of US timezones to remove Daylight Savings Time (DST) awareness has broken basic functionality in date handling in multiple vendor JVMs, including Oracle JRockit 1.5.0_08. This issue only affects sites using three-letter abbreviations of DST times zones denotations, which have been deprecated, and any affected JVM.The DateFormat parser uses the contents of String zoneStrings[][] in class DateFormatSymbols to identify the timezone based on the zone value in the input date string.The bug will only have an impact if and only if the application is using the deprecated denotation of three-letter abbreviations for US timezones (for example, EST, MST, or HST).

Severity: Warning

Rationale: Not Complying with Specifications

17.3.188 Changing Ssl Option Through Admin Console Is Hardcoded To Return To Port 7001

Description: If you use the Administration Console to enable/disable the SSL option against a server, and the server is accessed through a proxy server, when the changes are activated the accessed URL is hard-coded and redirects to port 7001.IMPACT:If you access the Administration Console through a proxy server, the connection to the Admin Server will be lost, since the URL is redirected to port 7001, which does not access the Console from the client side.

Severity: Minor Warning

Rationale: Administration

17.3.189 Changing Ssl Option Through Admin Console Is Hardcoded To Return To Port 7001 (Upgrade)

Description: If you use the Administration Console to enable/disable the SSL option against a server and the server is accessed through a proxy server, the accessed URL is hard-coded and redirects to port 7001 when the changes are activated.IMPACT:If you access the Administration Console through a proxy server, the connection to the Admin Server will be lost, since the URL is redirected to port 7001, which does not

access the Console from the client side.This problem, described in Oracle Bug 8166113, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3.

Severity: Minor Warning

Rationale: Administration

17.3.190 Characters With Different Character Sets Not Displaying Properly On Linux

Description: Special characters are not displayed correctly on the browser. The problem occurs only on Linux (Windows is not affected).Workaround: Add "-Dfile.encoding=ISO8859_1" to the server start params.

Severity: Minor Warning

Rationale: User Viewable Errors

17.3.191 Class-Level Generic Ejbs Are Not Supported

Description: Class-level Generics for EJBs are not supported. EJBs using class-level generics compile successfully in Oracle WebLogic Server 9.1. However, in Oracle WebLogic Server 9.2, the same appc compiler fails and an exception occurs with the following stack trace:location: interface com.rtn.template.ejb.Template_siqdx8_Intfpublic java.util.Collection<T> returnSomething() throwsjava.rmi.RemoteException;

Severity: Warning

Rationale: Not Complying with Specifications

17.3.192 Class-Level Generic Ejbs Are Not Supported (Upgrade)

Description: Class-level Generics for EJBS are not supported. EJBs using class-level generics compile successfully in Oracle WebLogic Server 9.1. However, in Oracle WebLogic Server 9.2, the same appc compiler fails and an exception occurs with the following stack trace:location: interface com.rtn.template.ejb.Template_siqdx8_Intfpublic java.util.Collection<T> returnSomething() throwsjava.rmi.RemoteException;This problem, described in Oracle Bug 8031049, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.3.193 Classcastexception Involving Custom Jndi Object And Cluster Synchronization (Wls V9.2)

Description: When creating a custom object and binding the object to the JNDI tree of a managed server of a two-node cluster, after the custom object is bound, the server log in the managed server shows a ClassCastException.

Severity: Minor Warning

Rationale: Administration

17.3.194 Classcastexception Involving Custom Jndi Object And Cluster Synchronization. (Wls V9.2, Upgrade)

Description: When creating a custom object and binding the object to the JNDI tree of a managed server of a 2 node cluster, after the custom object is bound, the server log in

the managed server shows a ClassCastException.This problem, described in Oracle Bug 8141074, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3.

Severity: Minor Warning

Rationale: Administration

17.3.195 Classcastexception Occurs When Deploying An Application

Description: A ClassCastException occurs when deploying an Oracle WebLogic Portal 9.2 application that has been upgraded from Oracle WebLogic Portal 8.1 SP4.When using the "prefer-web-inf-classes" feature, be careful not to mix instances created from the Web application class definition with instances created from the server definition. If you mix such instances, an exception results:<Warning> <Deployer> <BEA-149078> <Stack trace for message 149004weblogic.application.ModuleException: at weblogic.servlet.internal.WebAppModule.prepare(WebAppModule.java:295) ...

Severity: Warning

Rationale: Development

17.3.196 Classcastexception When Binding A Dynamic Proxy That Is Facade To Remote Object

Description: If an application has dynamic proxies as a facade to remote objects, and these dynamic proxies are bound to JNDI for lookup, the application seems to fail with the following ClassCastException:java.lang.ClassCastException: $Proxy0 atweblogic.rmi.extensions.server.ServerHelper.replaceAndResolveRemoteObject(ServerHelper.java:388)...

Severity: Minor Warning

Rationale: User Viewable Errors

17.3.197 Classcastexception When Binding A Dynamic Proxy That Is Facade To Remote Object (Upgrade)

Description: If an application has dynamic proxies as a facade to remote objects, and these dynamic proxies are bound to JNDI for lookup, the application seems to fail with the following ClassCastException:java.lang.ClassCastException: $Proxy0 atweblogic.rmi.extensions.server.ServerHelper.replaceAndResolveRemoteObject(ServerHelper.java:388) atweblogic.jndi.internal.WLEventContextImpl.copyObject(WLEventContextImpl.java:388)...This problem, described in Oracle Bug 8083730, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 1.

Severity: Minor Warning

Rationale: User Viewable Errors

17.3.198 Classcastexception When Deploying Application Containing Stax Classes (Upgrade)

Description: Deployment fails and the following ClassCastException is thrown when attempting to deploy an application containing StAX classes:java.lang.ClassCastException: com.ctc.wstx.stax.WstxInputFactoryat javax.xml.stream.XMLInputFactory.newInstance(XMLInputFactory.java:136)at weblogic.servlet.internal.WebAppHelper.addListenerElements(WebAppHelper.java:

244)at weblogic.servlet.internal.WebAppHelper $IOHelperImpl.parseXML(WebAppHelper.java:224)...This problem, described in Oracle Bug 8129805, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: User Viewable Errors

17.3.199 Classloader Leak When Using Side-By-Side Deployment

Description: Memory leak occurs in the ClassLoader when using side-by-side deployment.

Severity: Minor Warning

Rationale: Administration

17.3.200 Classloader Leak When Using Side-By-Side Deployment (Upgrade)

Description: Memory leak occurs in the ClassLoader when using side-by-side deployment.This problem, described in Oracle Bug 8152096, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3.

Severity: Minor Warning

Rationale: Administration

17.3.201 Classnotfoundexception For Jsp When Url Path Contains Spaces

Description: Attempting to access JSP pages located in a directory caused ClassNotFoundException - if the directory name included included space(s).This problem has been resolved. JSP pages located in a directory whose name includes spaces can now be accessed.

Severity: Warning

Rationale: Development

17.3.202 Classnotfoundexception For Jsp When Url Path Contains Spaces (Upgrade)

Description: Attempting to access JSP pages located in a directory caused ClassNotFoundException - if the directory name included included space(s).This problem has been resolved. JSP pages located in a directory whose name includes spaces can now be accessed.This problem has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 1

Severity: Minor Warning

Rationale: Development

17.3.203 Classnotfoundexception Thrown While Monitoring The Performance Of The Servers

Description: When monitoring the performance of either the managed or administrative server, errors get logged every ten seconds, which happens to be the time that it takes the performance screen to refresh.

Severity: Minor Warning

Rationale: Administration

17.3.204 Classnotfoundexception Thrown While Monitoring The Performance Of The Servers (Upgrade)

Description: When monitoring the performance of either the managed or administrative server, errors are logged every 10 seconds, which happens to be the time that it takes the performance screen to refresh.This problem, described in Oracle Bug 8109123, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.3.205 Classnotfoundexception With Httprequest For Replicated Webapp With Versioning

Description: Under load, an HTTPRequest lands on a Server that holds neither the Primary nor the Secondary HTTPSession, which results in a ClassNotFoundException (see below). This also causes end user issues in the environment.The following exception occurs:java.rmi.UnmarshalException: failed to unmarshal classweblogic.cluster.replication.ReplicationManager$ROObject; nested exceptionis: java.lang.ClassNotFoundException: Failed to load classuk.co.igindex.core.common.user.AnonymousUser ...

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.3.206 Classnotfoundexception With Httprequest For Replicated Webapp With Versioning (Upgrade)

Description: Under load, an HTTPRequest lands on a Server that holds neither the Primary nor the Secondary HTTPSession, which results in a ClassNotFoundException (see below). This also causes end user issues in the environment.The following exception occurs:java.rmi.UnmarshalException: failed to unmarshal classweblogic.cluster.replication.ReplicationManager$ROObject; nested exceptionis: java.lang.ClassNotFoundException: Failed to load classuk.co.igindex.core.common.user.AnonymousUserThis problem, described in Oracle Bug 8163071, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3.

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.3.207 Clicking Customize This Table And Proceeding Causes A Dialog Box To Pop Up

Description: When you click on "Customize this table" then navigate to another area in the console without making any changes, you get the "Do you want to save changes" dialog. This appears to be happening in the following pages:JDBC - DataSourceFactoryJDBC - Data SourcesJDBC - Multi Data Sources

Severity: Minor Warning

Rationale: Administration

17.3.208 Clientgen/Wsdlc Does Not Generate A Wrapped Doc/Literal Service

Description: Oracle WebLogic Server Web services ANT tasks clientgen/wsdlc do not generate a WRAPPED style Document/literal service. The generated interface is always BARE style. Per the original definition, wrapped array is not part of the wrapped element convention. Support is required for a wrapped array to be recognized as a wrapped element.

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.3.209 Clientgen/Wsdlc Does Not Generate A Wrapped Doc/Literal Service. (Upgrade)

Description: Oracle WebLogic Server webservices Ant tasks clientgen/wsdlc do not generate a WRAPPED style Document/literal service. The generated interface is always BARE style. Per the original definition, wrapped Array is not part of the wrapped Element convention. There needs to support for wrapped array to be recognized as a wrapped element using a flag.This problem, described in Oracle Bug 8135751, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.3.210 Cloning Of Server Through Console Does Not Clone The Custom Keystore/Ssl Settings

Description: When a server is cloned, all of its settings should be copied to the new server, including the custom keystore and SSL settings. In Oracle WebLogic Server 9.1, the custom keystore and SSL settings are not copied over during the cloning process. As a result, the keystore and SSL settings must be manually configured.

Severity: Minor Warning

Rationale: Administration

17.3.211 Cluster Hangs In Muxer Threads Under Load

Description: Cluster hangs under load. Thread dumps show Muxer threads are blocked when attempting to get the secondary session.

Severity: Minor Warning

Rationale: Administration

17.3.212 Cluster Hangs In Muxer Threads Under Load

Description: During high load tests, Muxer threads can become stuck in both managed servers. Thread dumps report stack similar to the following:'ExecuteThread: '2' for queue: 'weblogic.socket.Muxer'' daemon prio=10 tid=00a1eb68 nid=26 lwp_id=332127 in Object.wait() [4fae8000..4fae76f8] at java.lang.Object.wait(Native Method) - waiting on <6df388f8> (a java.lang.Object) at java.lang.Object.wait(Object.java:474) at weblogic.rjvm.RJVMImpl.ensureConnectionEstablished(RJVMImpl.java:317) - locked <6df388f8> (a java.lang.Object) at weblogic.rjvm.RJVMImpl.getOutputStream(RJVMImpl.java:340) ...This issue occurs due to an issue in the servlet code.

Severity: Critical

Rationale: Administration

17.3.213 Cluster Hangs In Muxer Threads Under Load. (Upgrade)

Description: During high load tests, Muxer threads can become stuck in both managed servers. Thread dumps report stack similar to the following:'ExecuteThread: '2' for queue: 'weblogic.socket.Muxer'' daemon prio=10 tid=00a1eb68 nid=26 lwp_id=332127 in Object.wait() [4fae8000..4fae76f8] at java.lang.Object.wait(Native Method) - waiting on <6df388f8> (a java.lang.Object) at java.lang.Object.wait(Object.java:474) at weblogic.rjvm.RJVMImpl.ensureConnectionEstablished(RJVMImpl.java:317) - locked <6df388f8> (a java.lang.Object) ...This issue occurs due to an issue in the servlet code.This problem, described in Oracle Bug 8107157, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3.

Severity: Minor Warning

Rationale: Administration

17.3.214 Cluster Has No Frontendhost Server Specified

Description: A cluster has the Oracle WebLogic Plugin enabled, but the FrontEndHost server setting has not been specified. Oracle WebLogic Server uses this setting to specify the host for HTTP responses. If no FrontEndHost server has been specified, Oracle WebLogic Server uses the hostname of the server that processed the request.

Severity: Warning

Rationale: Non-User Viewable Errors

17.3.215 Clusters Using In-Memory Session Replication May Experience Session Loss

Description: When in-memory session replication is used during failover, there is a possibility of a session loss. This session loss happens because when the primary server goes down, the secondary server detects this event and attempts to promote the session to become primary. However, the thread does not have the correct context ClassLoader. As a result, the session is lost.

Severity: Warning

Rationale: Subsystem Outage

17.3.216 Clusters Using In-Memory Session Replication May Experience Session Loss. (Upgrade)

Description: When in-memory session replication is used during failover, there is a possibility of a session loss. This session loss happens because when the primary server goes down, the secondary server detects this event and attempts to promote the session to become primary. However, the thread does not have the correct context ClassLoader. As a result, the session is lost.This problem, described in Oracle Bug 8051482, has been fixed in Oracle WebLogic Server 9.2.

Severity: Minor Warning

Rationale: Subsystem Outage

17.3.217 Comma-Separated List In Authentication Method Of Web.Xml Does Not Deploy Successfully. (Upgrade)

Description: The Oracle WebLogic Server documentation states that, according to the Servlet 2.4 specifications, you can use a comma separated list of authentication methods in the <login-config> element of a web.xml file. However, when this is implemented, an exception occurs.The exception is as follows:"Invalid auth-method list - CLIENT-CERT,FORM as the auth-method in web.xml, which is not valid. Valid values are BASIC (default), FORM and CLIENT-CERT."This problem, described in Oracle Bug 8115612, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.3.218 Compaction(S) Aborted Due To Counters Do Not Reset Between Each Garbage Collection

Description: Compaction of objects is the process of moving objects closer to each other in the heap, thus reducing the fragmentation and making object allocation easier for the JVM. Oracle JRockit compacts a part of the heap at each garbage collection (or old collection, if the garbage collector is generational).It has been observed in Oracle JRockit releases R27.3.1 and R27.4.0 that the compaction is being aborted when it should not be aborted due to the counter not being set to 0 between Garbage Collections.In some cases, the counter will continue to increase until it grows too large, leading to an aborted compaction. Since it is not set to 0, all the following Garbage Collections will be aborted as well.

Severity: Warning

Rationale: Performance

17.3.219 Compilation Of Jsp 2.0 Tag File Fragment Attribute Fails With A Compilationexception

Description: When creating a JSP 2.0 custom tag as a tag file (for example, WEB-INF/tags/test.tagx), if you exclude jsp:attribute, then the test tag is resolved normally. However, if you use jsp:attribute, the following exception occurs:weblogic.servlet.jsp.CompilationException: Failed to compile JSP /WEB-INF/jsp/root.jsproot.jsp:14:6: This tag can only appear as a subelement of a standard or custom action. Exceptions are: jsp:body, jsp:attribute, jsp:expression, jsp:scriptlet, and jsp:declaration. <jsp:attribute name='fragment'> ^ - - - - - -^ at weblogic.servlet.jsp.JavelinxJSPStub.compilePage(JavelinxJSPStub.java:296) at weblogic.servlet.jsp.JspStub.prepareServlet(JspStub.java:200)... >

Severity: Minor Warning

Rationale: Development

17.3.220 Compilation With Weblogic.Appc Is Slow

Description: Webapp compilation with weblogic.appc takes more time, with 100% CPU usage, as compared with Tomcat (Jasper).

Severity: Warning

Rationale: Performance

17.3.221 Compliance To Rfc3515 Broken, Sending Sip 481 Response On Notify (100 Or 200 Ok)

Description: In a SIP proxy scenario, client A sends a SIP REFER request to client B, which replies with a SIP 202 message, followed by two NOTIFY (100 trying and 200OK) SIP responses.Oracle WebLogic SIP Server, a proxy between client A and client B, sends a '481 Subscription does not exists' response back to client B, which is not compliant to RFC3515.Instead the NOTIFY or 202 response should be forwarded to client A by the proxy.

Severity: Warning

Rationale: Not Complying with Specifications

17.3.222 Concurrentmodification Exception When Accessing An External Authentication Provider. (Upgrade)

Description: Oracle WebLogic Server Administration Console raises a ConcurrentModification exception when accessing a users list or a groups list, if there are too many matches of users or groups for the specified filter.This problem, described in Oracle Bug 8093424, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 1.

Severity: Minor Warning

Rationale: User Viewable Errors

17.3.223 Concurrentmodification Exception When Accessing External Authentication Provider

Description: Oracle WebLogic Server Administration Console raises a ConcurrentModification exception when accessing a users list or a groups list, if there are too many matches of users or groups for the specified filter.

Severity: Minor Warning

Rationale: User Viewable Errors

17.3.224 Concurrentmodificationexception During Concurrent Lazy Enlist

Description: The connector's ConnectionPool class had unsynchronized access to a shared data object. Thus, when multiple threads attempt to update/access the same data object, ConcurrentModificationException is thrown.

Severity: Minor Warning

Rationale: User Viewable Errors

17.3.225 Concurrentmodificationexception During Concurrent Lazy Enlist (Upgrade)

Description: The connector's ConnectionPool class had unsynchronized access to a shared data object. Thus when multiple threads attempt to update/access the same data object, ConcurrentModificationException is thrown.This problem, described in Oracle Bug 8081433, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: User Viewable Errors

17.3.226 Connecting A 8.1 Client To A 9.X Server Leads To A Classcastexception Error

Description: Consider the following scenario: * Oracle WebLogic Server 9.0 Server * Oracle WebLogic Server 8.1 SP3 Java client repeated performing the following: - InitialContext creation using security credentials - Lookup using the ContextUnder the scenario above, a call may fail - new InitialContext(hashtable) - fails with java.lang.NullPointerException - Context.lookup(objLookup) - fails with java.lang.ClassCastExceptionThe issue could only be caused if both the following were present: - Use of security credentials - Performing a JNDI lookupThis issue is more apparent when the client and server are on different machines.

Severity: Minor Warning

Rationale: User Viewable Errors

17.3.227 Connecting A 8.1 Client To A 9.X Server Leads To A Classcastexception Error (Upgrade)

Description: Consider the following scenario: * Oracle WebLogic Server 9.0 Server * Oracle WebLogic Server 8.1 SP3 Java client repeated performing the following: - InitialContext creation using security credentials - Lookup using the ContextSome calls fail with: * new InitialContext(hashtable) - fails with java.lang.NullPointerException * Context.lookup(objLookup) - fails with java.lang.ClassCastExceptionThe issue could only be caused if both the following were present: * Use of security credentials * Performing a JNDI lookupThis issue is more apparent when the client and server are on different machines.This problem, described in Oracle Bug 8078111, has been fixed in Oracle WebLogic Server 9.2.

Severity: Minor Warning

Rationale: User Viewable Errors

17.3.228 Connection Pool Performance May Be Degraded Due To The Test Settings That Are Specified

Description: A connection pool has been set up to perform all of the following tests:* TestOnCreate* TestOnReserve* TestOnReleaseAs a result of enabling all three of these settings, the connection will be tested when it is retrieved from the pool and then again when it is put back into the pool. This can lead to performance issues in JDBC access code.

Severity: Minor Warning

Rationale: Performance

17.3.229 Console Cannot Display Jolt Connection Pool Details

Description: Could not manage the Jolt connection through the monitoring tab of the JoltConnectionPool in the Oracle WebLogic Server(tm) Administration console.This has been resolved by providing the ability to manage the Jolt connection through the hyperlinks in the Pool Name and Connection columns of the Jolt connection pools monitoring table.

Severity: Minor Warning

Rationale: Administration

17.3.230 Console Cannot Display Jolt Connection Pool Details (Upgrade)

Description: Could not manage the Jolt connection through the monitoring tab of the JoltConnectionPool in the Oracle WebLogic Server(tm) Administration console.This has been resolved by providing the ability to manage the Jolt connection through the hyperlinks in the Pool Name and Connection columns of the Jolt connection pools monitoring table.This problem, described in Oracle Bug 8114080, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.3.231 Console Does Not Show Image Creation Tasks In The Task Table

Description: It appears that console is not showing the tasks created for capturing diagnostic image.

Severity: Minor Warning

Rationale: Administration

17.3.232 Console Hangs When Two(Multiple) Users Try To Get The Lock On The Same Config

Description: Go into the console and start an edit session.Click on the Domain wide configuration settings link. Enable the flag "Production Mode" and "Activate" your changes.Now start another edit session, disable this flag, and activate your settings.The console now gives an error and does not allow this change to take place.

Severity: Minor Warning

Rationale: Administration

17.3.233 Console Is Too Slow

Description: Oracle WebLogic Server 9.2 console is too slow.

Severity: Minor Warning

Rationale: Administration

17.3.234 Console Is Too Slow (Upgrade)

Description: Oracle WebLogic Server 9.2 console is too slow.This problem, described in Oracle Bug 8128522, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.3.235 Console Mode Multi-Byte Characters Display Alignment Issue

Description: Localized version of config wizard console mode screen cannot display multi-byte characters correctly in 3 portions.1. TitlesIf titles contain multi-byte characters, the titles exceed the length of underline. This happens if a title has multi-byte characters.2. TablesIf fields in a table contain multi-byte characters, the lattice

breaks. This happens if a field has multi-byte characters.3. StringsIf strings contains multi-byte characters, Line Feed (return) is inserted in incorrect position.

Severity: Minor Warning

Rationale: User Viewable Errors

17.3.236 Console Shows Wrong Config Values If Production Mode Is Enabled/Disabled From Command Line

Description: When Production Mode is enabled or disabled with the command line option "-Dweblogic.ProductionModeEnabled=[true

Severity: false]" but the setting does not agree with the config.xml "ProductionMode" setting, the Adminstration Console may show incorrect values for some configuration options. This can occur for any configuration options for which the default values for production mode differ from the default values for development mode.Note: Command line overrides are not persisted in config.xml. The Administration Console shows the configuration attribute values and defaults that correspond to the persisted version in the config.xml file.

Rationale: Warning

17.3.237 Console Throws Ddbeancreateexception When Clicking On Applications In A Clustered Domain

Description: Customers receive the following exception when clicking on applications in the Oracle WebLogic Server console in a clustered domain:####<Apr 19, 2007 8:06:02 AM EDT> <Error> <Console> <devapp1.rfiddev.isdtpa.labs.att.com> <AdminServer> <[ACTIVE] ExecuteThread: '11' for queue: 'weblogic.kernel.Default (self-tuning)'> <rfidweblogic> <> <> <1176984362305> <BEA-240003> <Console encountered the following error com.bea.console.exceptions.ManagementException: javax.enterprise.deploy.model.exceptions.DDBeanCreateException: [J2EE Deployment SPI:260142]The descriptor ...Installers, updates, patches and more information are available at support.oracle.com.

Severity: Minor Warning

Rationale: Administration

17.3.238 Console Will Not Open If Server Is Started With -Dweblogic.Jsp.Windows.Casesensitive=True

Description: When the server is started with the option "-Dweblogic.jsp.windows.caseSensitive=true", the console will not open and a "ClassNotFoundException" error is thrown. This error occurs because the LoginForm.jsp file cannot find the LoginForm class in the console.war file, because the compiled class of LoginForm is "loginform" in all lowercase characters.

Severity: Minor Warning

Rationale: Administration

17.3.239 Console Will Not Open If Server Is Started With -Dweblogic.Jsp.Windows.Casesensitive=True (Upgrade)

Description: When the server is started with the option "-Dweblogic.jsp.windows.caseSensitive=true", the console will not open and a

ClassNotFoundException is thrown. This error occurs because the LoginForm.jsp file cannot find the LoginForm class in the console.war file, because the compiled class of LoginForm is "loginform" in all lowercase characters.This problem, described in Oracle Bug 8056225, has been fixed in Oracle WebLogic Server 9.2.

Severity: Minor Warning

Rationale: Administration

17.3.240 Consumers Not Recreated After Server Is Rebooted

Description: When a Message Driven Bean (MDB) is deployed on a multiserver domain and is listening on a distributed queue, and the MDB is configured to connect to all of the distributed queue members. However, if a remote distributed queue member server is restarted, the deployed MDB server does not reconnect with the remote distributed queue member server.

Severity: Warning

Rationale: Subsystem Outage

17.3.241 Container Throwing Nullpointerexception For Any Empty Via Headers In Message

Description: If Oracle WebLogic SIP Server receives a message with an empty "Via" header, then a java.lang.NullPointerException can occur, as follows:[ACTIVE] ExecuteThread: '3' for queue: 'weblogic.kernel.Default (self-tuning)'> <<WLS Kernel>> <> <> <1186999006009> <BEA-330608> <Socket error java.lang.NullPointerException at com.bea.wcp.sip.engine.connector.transport.UdpTransportModule $UdpWorker.setViaHeader(UdpTransportModule.java:696) at com.bea.wcp.sip.engine.connector.transport.UdpTransportModule $UdpWorker.run(UdpTransportModule.java:597) ...The container should not throw a java.lang.NullPointerException. Instead, it should warn with a meaningful message after necessary validation for the above 'Via' header in the response.

Severity: Warning

Rationale: Development

17.3.242 Content Of Exported Jms Text Message May Be Changed When Imported Via Administration Console

Description: The content of an exported JMS text message may be changed when using the Oracle WebLogic Server Administration Console to import the exported message.

Severity: Minor Warning

Rationale: User Viewable Errors

17.3.243 Content Of Exported Jms Text Message May Be Changed When Imported Via Administration Console. (Upgrade)

Description: The content of an exported JMS text message may be changed when using the Oracle WebLogic Server Administration Console to import the exported message.This problem, described in Oracle Bug 8162695, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3.

Severity: Minor Warning

Rationale: User Viewable Errors

17.3.244 Content-Type Header For Soap Messages Does Not Contain Type Field

Description: The Oracle WebLogic Server SAAJ implementation does not create a value of "type="text/xml"" as a parameter of the Content-Type header for a SOAP Message.The expected value for Content-Type is as follows:Content-Type: Multipart/Related; boundary="example-1"; type="text/xml"; start=soapPartHowever, the "type="text/xml";" portion of the string is not printed to the header.

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.3.245 Content-Type Header For Soap Messages Does Not Contain Type Field. (Upgrade)

Description: The Oracle WebLogic Server SAAJ implementation does not create a value of "type="text/xml"" as a parameter of the Content-Type header for a SOAP Message.The expected value for Content-Type is as follows:Content-Type: Multipart/Related; boundary="example-1"; type="text/xml"; start=soapPartHowever, the "type="text/xml";" portion of the string is not printed to the header.This problem, described in Oracle Bug 8085390, has been fixed in Oracle WebLogic Server 10.0.

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.3.246 Context.Getrealpath Method Returns A Null When Called Per The Servlet Specification

Description: If you deploy a Web application as an archived Web Application Archive (WAR) file, context.getRealPath() returns a NULL when called, as specified by the servlet specification. This can lead to failures if the Web application is dependent on the path value.Resolution: Use the getrealpath() method in Oracle WebLogic Server 9.2, and use the flag <show-archived-real-path-enabled>true</show-archived-real-path-enabled>.This is fixed in Oracle WebLogic Server 10, but you must apply the patch in Oracle WebLogic Server 9.2, 9.2.1, 9.2.2, and 9.2.3 to use this flag.

Severity: Minor Warning

Rationale: Administration

17.3.247 Context.Getrealpath Method Returns A Null When Called Per The Servlet Specification (Upgrade)

Description: If you deploy a Web application as an archived Web Application Archive (WAR) file, context.getRealPath() returns a NULL when called per the servlet specification. This can lead to failures if the Web application is dependent on the path value.Resolution:Use the getrealpath() method in Oracle WebLogic Server 9.2, you must use the flag show-archived-real-path-enabled. This is fixed in Oracle WebLogic Server 10, but you must apply the patch in Oracle WebLogic Server 9.2, 9.2.1, 9.2.2, and 9.2.3 to use this flag.This problem, described in Oracle Bug 8107008, has been fixed in Oracle WebLogic Server 10.0.

Severity: Minor Warning

Rationale: Administration

17.3.248 Context.Getrealpath Method Returns A Null When Called Per The Servlet Specification (Upgrade)

Description: If you deploy a Web application as an archived Web Application Archive (WAR) file, context.getRealPath() returns NULL when called per the servlet specification. This can lead to failures if the Web application is dependent on the path value.Resolution:Use the getrealpath() method in Oracle WebLogic Server 9.2, you must use the flag show-archived-real-path-enabled. This is fixed in Oracle WebLogic Server 10, but you must apply the patch in Oracle WebLogic Server 9.2, 9.2.1, 9.2.2, and 9.2.3 to use this flag.This problem, described in Oracle Bug 9181232, has been fixed in Oracle WebLogic Server 10.0.

Severity: Minor Warning

Rationale: Administration

17.3.249 Crashes In Conjunction With A Native Library

Description: If you are using Oracle JRockit in conjunction with a native library that relies on OS signals you may experience crashes due to a signal handling conflict between Oracle JRockit and the native library.Dump stack matches known issue:Thread Stack Trace: at pthread_kill+62()@0xb75c00ee at ptSendSignal +34()@0xb71aedc6 at trapiConvertToDeferredSigsegv+199()@0xb719d207 at trapiSigSegvHandler+40()@0xb719d23c at xehInterpretSavedSigaction +219(amqxerrx.c)@0xb72f276b at xehExceptionHandler+543()@0xb72f2b3f at __libc_sigaction+272()@0xb75c2f80Oracle Engineering found this conflict using IBM's MQSeries native drivers, and it may be present in other libraries that rely on native code.

Severity: Critical

Rationale: Server Outage

17.3.250 Create Columns Correctly As Null And Non Null In Sybase And Db2 Using Autocreate

Description: Using automatic table creation to deploy EJBs for Sybase results in every column in every table being non-null. As a result, if the EJB create method only takes a few of the Container-Managed Persistence (CMP) fields, creating EJBs fails with the following error:column does not allow nullsThe only column created as NOT NULL should be the primary key column.

Severity: Warning

Rationale: Subsystem Outage

17.3.251 Credentials Specified For Foreign Jms Are Not Picked Up Properly By Mdb

Description: Message-Driven Beans (MDB) that use a local foreign JMS server configuration, fail to use the credentials provided by the foreign JMS server configuration.

Severity: Warning

Rationale: Subsystem Outage

17.3.252 Credentials Specified For Foreign Jms Are Not Picked Up Properly By Mdb (Upgrade)

Description: Message-driven beans (MDBs) that use a local foreign JMS server configuration, fail to use the credentials provided by the foreign JMS server configuration.This problem, described in Oracle Bug 8117048, has been fixed in Oracle WebLogic Server 9.1.

Severity: Minor Warning

Rationale: Subsystem Outage

17.3.253 Current Capacity Exceeds Max Capacity If Testconnectionsonrelease=True

Description: During periodic test of a pool, or if a pool is test on release, the pool temporarily removes a connection from any list where it would be counted in the current capacity of the pool. If a pool is stressed with many threads making and releasing connections, the connection count might fail to include one or two of these connections, allowing the pool to create more than the maximum connections allowed.

Severity: Minor Warning

Rationale: Administration

17.3.254 Current Capacity Exceeds Max Capacity If Testconnectionsonrelease=True (Upgrade)

Description: During periodic test of a pool or if a pool is test-on-release, the pool temporarily removes a connection from any list where it would be counted in the current capacity of the pool. If a pool is stressed with many threads making and releasing connections, the connection count might fail to include one or two of these connections, allowing the pool to create more than the maximum connections allowed.This problem, described in Oracle Bug 8113591, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.3.255 Custom Work Manager Cannot Be Named 'Default' Because Of System-Wide Default Work Manager

Description: A custom global Work Manager defined with the name "default" will not override the system-wide default Work Manager. This results in runtime MBean registration errors.

Severity: Minor Warning

Rationale: Administration

17.3.256 Custom Work Manager Cannot Be Named 'Default' Because Of System-Wide Default Work Manager. (Upgrade)

Description: When defining a custom, global Work Manager with the name "default," will not override the system-wide default Work Manager; it causes runtime MBean registration errors.This problem, described in Oracle Bug 8088410, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Administration

17.3.257 Dtd Mapping Using Weblogic-Application.Xml Throws Runtimeexception: Can'T Read Zip Entry

Description: The application has a DTD mapping using weblogic-application.xml. When the application is deployed as an archive, it fails with the following error:weblogic.xml.registry.XMLRegistryException: Can't read zip entry: dtd/eventRegister.dtd in zip: D:\646827\91app.ear at com.sun.org.apache.xerces.internal.parsers.DOMParser.parse(DOMParser.java:286) at...The application is a regression from Oracle WebLogic Server 8.1, which works fine in both archive and exploded format. In Oracle WebLogic Server 9.x, the same application works in exploded format, but fails as an archive.

Severity: Minor Warning

Rationale: Administration

17.3.258 Datasource Test Frequency Seconds Does Not Work After Shutdown And Start

Description: Shutting down a pool also kills the associated asynchronous connection testing process. When the pool is restarted, the asynchronous testing job does not restart, and the DataSource cannot detect database failures by test frequency until the Oracle WebLogic Server is rebooted.

Severity: Minor Warning

Rationale: Administration

17.3.259 Datasource'S Shutdown Operation Has Failed With Javax.Transaction.Systemexception

Description: When you shutdown a DataSource from the Administration Console, the operation fails with javax.transaction.SystemException. This behavior occurs when using an XA driver.Workaround or Solution:Use untarget/target instead of shutdown/start operation.

Severity: Minor Warning

Rationale: Administration

17.3.260 Datasource'S Shutdown Operation Has Failed With Javax.Transaction.Systemexception (Upgrade)

Description: When you shutdown a DataSource from the Administration Console, the operation fails with javax.transaction.SystemException. This behavior occurs when using an XA driver.Workaround or Solution:Use untarget/target instead of shutdown/start operation.This problem, described in Oracle Bug 8164163, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3.

Severity: Minor Warning

Rationale: Administration

17.3.261 Dates For Connections, Reservations, And Creations Are Displaying As Dec 31 1969

Description: The date displayed for date of connections, date of creation, date of reservation, and reserved since date are displaying as "Dec 31, 1969" instead of as "Never."

Severity: Minor Warning

Rationale: User Viewable Errors

17.3.262 Deadlock In Feconnection.Close And Feconnectionruntimedelegate.Getsessionscurren (Wls V9.2)

Description: A deadlock occurs in FEConnection and FEConnectionRuntimeDelegate class when sending a message to JMS Server using thin client.The following is the thread stack for the deadlock:"[STANDBY] ExecuteThread: '5' for queue: 'weblogic.kernel.Default(self-tuning)'": at weblogic.management.runtime.RuntimeMBeanDelegate.unregisterChildren(RuntimeMBeanDelegate.java:336) - waiting to lock <0x03ae0028> (a weblogic.jms.frontend.FEConnectionRuntimeDelegate) ..."[ACTIVE] ExecuteThread: '0' for queue: 'weblogic.kernel.Default(self-tuning)'": at weblogic.jms.frontend.FEConnection.getSessionMap(FEConnection.java:1278) - waiting to lock <0x03ae0098> (a weblogic.jms.frontend.FEConnection)

Severity: Warning

Rationale: Administration

17.3.263 Deadlock Occurs At Weblogic.Jms.Client.Jmsxaconnection

Description: Deadlock/stuck thread occurs at weblogic.jms.client.JMSConnection.stateChangeListener with the following error: A deadlock has been detected regarding the following object: - weblogic.jms.client.JMSXAConnectionThis error can also occur after a while in production or on heavy load. For example, some stuck threads with the following stack may appear:[STUCK] ExecuteThread: '4' for queue: 'weblogic.kernel.Default (self-tuning)' has been busy for "700" seconds working on the request "weblogic.work.ServerWorkManagerImpl$WorkAdapterImpl@1827d10", which is more than the configured time (StuckThreadMaxTime) of "600" seconds. Stack trace: weblogic.jms.common.CDS.makeChangeEvent(CDS.java:602) weblogic.jms.common.CDS.access$000(CDS.java:25) ...

Severity: Warning

Rationale: Subsystem Outage

17.3.264 Deadlock Occurs At Weblogic.Jms.Client.Jmsxaconnection (Upgrade)

Description: A deadlock/stuck thread occurs at weblogic.jms.client.JMSConnection.stateChangeListener, with the following error: A deadlock has been detected regarding the object: - weblogic.jms.client.JMSXAConnectionThis can also occur when running under heavy load. Stuck threads may occur with the following stack:[STUCK] ExecuteThread: '4' for queue: 'weblogic.kernel.Default (self-tuning)' has been busy for "700" seconds working on the request "weblogic.work.ServerWorkManagerImpl $WorkAdapterImpl@1827d10", which is more than the configured time

(StuckThreadMaxTime) of "600" seconds. Stack trace: weblogic.jms.common.CDS.makeChangeEvent(CDS.java:602) ...This problem, described in Oracle Bug 8129087, is fixed in Oracle WebLogic Server 9.2 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Subsystem Outage

17.3.265 Deadlock Occurs At Weblogic.Jms.Client.Jmsxaconnection (Upgrade)

Description: Deadlock/stuck thread at weblogic.jms.client.JMSConnection.stateChangeListener: A deadlock has been detected regarding the object: - weblogic.jms.client.JMSXAConnection[STUCK] ExecuteThread: '4' for queue: 'weblogic.kernel.Default (self-tuning)' has been busy for "700" seconds working on the request "weblogic.work.ServerWorkManagerImpl $WorkAdapterImpl@1827d10", which is more than the configured time (StuckThreadMaxTime) of "600" seconds.This problem, Oracle Bug 8138174, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Subsystem Outage

17.3.266 Deadlock Occurs In Oracle Weblogic Server (Wls V9.2)

Description: Java level deadlock between weblogic.deployment.jms.JMSSessionPoolTester and weblogic.deployment.jms.JMSSessionPool reveal in Oracle WebLogic Server Thread dump.

Severity: Critical

Rationale: Server Outage

17.3.267 Deadlock Occurs In Oracle Weblogic Server (Wls V9.2, Upgrade)

Description: Java level deadlock between weblogic.deployment.jms.JMSSessionPoolTester and weblogic.deployment.jms.JMSSessionPool reveal in Oracle WebLogic Server Thread dump.

Severity: Minor Warning

Rationale: Server Outage

17.3.268 Deadlock On Weblogic.Rmi.Extensions.Abstractdisconnectmonitordelegate.Remove

Description: In a cluster configuration, some clients (about 100) connect as subscriber/publisher for one JMS topic, with each client having its own topic. On another client, C2 is connected as subscriber/publisher to all JMS topics. The C2 client is multithreaded, and each thread opens a connection to one JMS topic. All clients use the T3 protocol, and wlclient.jar and wljmsclient.jar.When delivering disconnect notices, the RMI subsystem obtains a coarse lock on the disconnect listeners set, and then invokes a callback for the disconnect event. The lock is held throughout. The patch to Oracle Bug 8088961 changes the behavior so that the lock is held only for the time required to remove the listener set, and then the callback is invoked. As a result, the deadlock no longer occurs.

Severity: Warning

Rationale: Subsystem Outage

17.3.269 Deadlock On Weblogic.Rmi.Extensions.Abstractdisconnectmonitordelegate.Remove (Upgrade)

Description: In a cluster configuration, some clients (about 100) connect as subscriber/publisher for one JMS topic, and each client has its own topic. On another client, C2 is connected as subscriber/publisher to all JMS topics. The C2 client is multithreaded, and each thread opens a connection to one JMS topic.All of the clients use T3 protocol and wlclient.jar and wljmsclient.jar. Running a failover test by killing the Oracle WebLogic Server instance where the connections with the C2 client are established, causes a deadlock.The patch to Oracle Bug 8088961 changes the behavior so that the lock is held only for the time required to remove the listener set, and then the callback is invoked. As a result the deadlock no longer occurs.

Severity: Minor Warning

Rationale: Subsystem Outage

17.3.270 Deleting A Filestore Associated With A Jmsserver Throws Exception In Console

Description: Deleting a FileStore associated with a JMSServer relates throws the following exception on the console.Unexpected ExceptionAn unexpected exception has occurred processing your requestMessage: Beanweblogic.management.configuration.FileStoreMBeanImpl@6d099267([mydomain]/FileStores[FileStore@CS1])references [FileStore@CS1 by[mydomain]/JMSServers[JmsServer@CS1]/PersistentStore, FileStore@CS1 by[mydomain]/PathServices[myPathService]/PersistentStore]

Severity: Minor Warning

Rationale: Administration

17.3.271 Deleting An Application From The Autodeploy Directory Leads To An Out-Of-Sync Domain

Description: If you delete a web application from the autodeploy folder when the server is inactive, the config.xml file incorrectly retains an entry for the web application as follows and results in an out-of-sync domain: <app-deployment> <name>_appsdir_Good_webApp_dir</name> <target>AdminServer</target> <module-type>war</module-type> <source-path>autodeploy\Good_webApp</source-path> <security-dd-model>DDOnly</security-dd-model> <staging-mode>nostage</staging-mode> </app-deployment>deleted the cache folder for the admin server.'C:\bea92\user_projects\domains\wls\servers\AdminServer\tmp 'restarted the weblogic server. The webapp still remains deployed.

Severity: Minor Warning

Rationale: Administration

17.3.272 Deleting Channel Used By Rdbms Event Generator Can Cause Deadlock In Server

Description: Deleting a channel used by an RDBMS Event Generator can cause a deadlock in the server.

Severity: Critical

Rationale: Administration

17.3.273 Deployer Does Not Use Previous Targets When Redeploying Newer Version Of Application

Description: weblogic.Deployer does not use previous targets when deploying newer version of the application:1.When using weblogic.Deployer to redeploy a new version of the application,it fails.2.According to the output, because there is not specified a target, it attempts to use the admin instance as a default.Getting the following exceptions:weblogic.management.ManagementException: [Deployer:149119]You cannot specify different targets when deploying a new version 'Newer_v920.beta' of application 'SimpleEAR'. The target(s) specified, '[AdminServer]', is/are different from those of the previous version, '[MS1]'. at weblogic.deploy.internal.adminserver.operations.OperationHelper.validateVersionTargets(OperationHelper.java:535) ...

Severity: Warning

Rationale: Administration

17.3.274 Deployer Does Not Use Previous Targets When Redeploying Newer Version Of Application (Upgrade)

Description: weblogic.Deployer does not use previous targets when deploying newer version of the application:* When using weblogic.Deployer to redeploy a new version of the application,it fails.* According to the output, because there is not specified a target, it attempts to use the admin instance (AdminServer) as a default.* This is contrary to both the documentation for weblogic.Deployer as well as previous version (Oracle WebLogic Server 8.1) in which the existing targets are used when no target is specified.This problem, described in Oracle Bug 8146267, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3

Severity: Minor Warning

Rationale: Administration

17.3.275 Deploying Jar For Custom Http Log Field In Domain/Lib Directory Results In Exception

Description: If a custom ELF (Extensible and Linkable Format) field is defined for an HTTP log and the JAR is copied to the $DOMAIN/lib folder, the server startup fails with an exception.

Severity: Minor Warning

Rationale: Development

17.3.276 Deploying Jar For Custom Http Log Field In Domain/Lib Directory Results In Exception (Upgrade)

Description: If a custom ELF (Extensible and Linkable Format) field is defined for an HTTP Log, and the JAR is copied to the $DOMAIN/lib folder, the server startup fails with an exception.This problem, described in Oracle Bug 8101714, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Development

17.3.277 Deploying A Service Fails With Classnotfoundexception When Soap Array Is Used As Out Param

Description: When a SOAP array is used as an OUT parameter in a Web service method, deploying a service fails with a ClassNotFoundException because the holder class cannot be found.

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.3.278 Deploying An Ejb With Large Cmp Deployment Descriptors Fails

Description: The Oracle WebLogic Server's EJB container is not able to handle Oracle WebLogic Server Container-Managed Persistence (CMP) deployment descriptors larger than one MB (for example, the weblogic-cmp-rdbms-jar.xml file is larger than one MB). Deploying an EJB JAR file with large deployment descriptors fails with the following exception:Exception preparing module: EJBModule(abac-entity) Unable to deploy EJB: CommitmentEnvelopeLinkCountryRW from abac-entity.jar: [EJB: 011017]Error while reading 'META-INF/weblogic-cmp-rdbms-jar.xml'. The error was: weblogic.ejb20.cmp.rdbms.RDBMSException: java.io.IOException: Resetting to invalid mark at java.io.BufferedInputStream.reset(BufferedInputStream.java:408) at weblogic.ejb.container.cmp.rdbms.Deployer.parseXMLFile(Deployer.java:1006) ...

Severity: Warning

Rationale: Administration

17.3.279 Deploying An Ejb With Large Cmp Deployment Descriptors Fails. (Upgrade)

Description: Oracle WebLogic Server's EJB container is not able to handle Container-Managed Persistence (CMP) deployment descriptors larger than one MB, such as the weblogic-cmp-rdbms-jar.xml file. Deploying an EJB JAR file with such large deployment descriptors fails with the following exception:Exception preparing module: EJBModule(abac-entity) Unable to deploy EJB: CommitmentEnvelopeLinkCountryRW from abac-entity.jar: [EJB:011017]Error while reading 'META-INF/weblogic-cmp-rdbms-jar.xml'. The error was: weblogic.ejb20.cmp.rdbms.RDBMSException: java.io.IOException: Resetting to invalid mark ...This problem, described in Oracle Bug 8104252, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Administration

17.3.280 Deploying Applications From The Console Is Slow Using Solaris

Description: When deploying a very large application on Solaris 8 (or 9) using the Oracle WebLogic Server 9.2 console, you find that the deployment time is three times slower than on Oracle WebLogic Server 8.1.

Severity: Warning

Rationale: Development

17.3.281 Deploying Applications From The Console Is Slow Using Solaris. (Upgrade)

Description: When deploying a very large application on Solaris 8 (or 9) using the Oracle WebLogic Server 9.2 console, you find that the deployment time is three times slower than on Oracle WebLogic Server 8.1.This problem, described in Oracle Bug 8114093, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Development

17.3.282 Deploying The Application, But Targeting Modules Individually, Causes The Application Not To Start.

Description: When deploying an application, but targeting the modules individually, the application does not get started properly.

Severity: Warning

Rationale: Administration

17.3.283 Deploying The Application, But Targeting Modules Individually, Causes The Application Not To Start. (Upgrade)

Description: When deploying an application, but targeting the modules individually, the application does not get started properly.This problem, described in Oracle Bug 8095694, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Administration

17.3.284 Deploying The Application, But Targeting Modules Individually, Causes The Application Not To Start. (Upgrade)

Description: When deploying an application, but targeting the modules individually, the application does not get started properly.This problem, described in Oracle Bug 8095694, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Administration

17.3.285 Deployment Fails During Compilation With Complianceexception Occurring In Weblogic Appc

Description: Deployment fails during compilation, with a ComplianceException occurring in wlappc, as follows:"weblogic.servlet.internal.dd.compliance.ComplianceException: Required file WEB-INF/web.xml not found at weblogic.servlet.jsp.JspcInvoker.compile(JspcInvoker.java:183) at weblogic.application.compiler.AppcUtils.compileWAR(AppcUtils.java:348) at weblogic.application.compiler.WARModule.compile(WARModule.java:78) at weblogic.application.compiler.flow.CompileModuleFlow.compileModules(CompileModuleFlow.java:104) ..."

Severity: Minor Warning

Rationale: Administration

17.3.286 Deployment Fails During Compilation With Complianceexception Occurring In Wlappc (Upgrade)

Description: Deployment fails during compilation, with a ComplianceException occurring in wlappc, as follows:"weblogic.servlet.internal.dd.compliance.ComplianceException: Required file WEB-INF/web.xml not found at weblogic.servlet.jsp.JspcInvoker.compile(JspcInvoker.java:183) at weblogic.application.compiler.AppcUtils.compileWAR(AppcUtils.java:348) at weblogic.application.compiler.WARModule.compile(WARModule.java:78) at weblogic.application.compiler.flow.CompileModuleFlow.compileModules(CompileModuleFlow.java:104) ..."This problem, described in Oracle Bug 8086108, has been fixed in Oracle WebLogic Server 9.2.

Severity: Minor Warning

Rationale: Administration

17.3.287 Deployment Fails When Using The Oracle Weblogic Server 8.1 Deployer

Description: Oracle WebLogic Server 9.1 should be backward compatible with the Oracle WebLogic Server 8.1 deployer. However, the Oracle WebLogic Server 8.1 weblogic.Deployer running on a 1.4.2 JVM cannot deploy to Oracle WebLogic Server 9.1 running on 1.5 JVM. When you configure this type of deployment and test it, the test results in an exception.

Severity: Minor Warning

Rationale: Administration

17.3.288 Deployment Fails When Using The Oracle Weblogic Server 8.1 Deployer (Upgrade)

Description: Oracle WebLogic Server 9.1 should be backward compatible with the Oracle WebLogic Server 8.1 deployer. However, the Oracle WebLogic Server 8.1 weblogic.Deployer running on a 1.4.2 JVM cannot deploy to Oracle WebLogic Server 9.1 running on 1.5 JVM. When you configure this type of deployment and test it, the test results in an exception.This problem, described in Oracle Bug 8086846, has been fixed in Oracle WebLogic Server 9.2.

Severity: Minor Warning

Rationale: Administration

17.3.289 Deployment Fails When Using The Oracle Weblogic Server 8.1 Installer. (Upgrade)

Description: Oracle WebLogic Server 9.1 should be backward compatible with the Oracle WebLogic Server 8.1 deployer. However, the Oracle WebLogic Server 8.1 weblogic.Deployer running on a 1.4.2 JVM cannot deploy to Oracle WebLogic Server 9.1 running on 1.5 JVM. When you configure and test this type of deployment, the test results in an exception.This problem, described in Oracle Bug 8086846, has been fixed in Oracle WebLogic Server 9.2.

Severity: Minor Warning

Rationale: Administration

17.3.290 Deployment Fails With Timeout When Webapp With Lots Of Servlet Mappings

Description: When deploying a large Web application that has a large number of servlet mappings, the deployment hangs while trying to add the servlet mappings.

Severity: Minor Warning

Rationale: Administration

17.3.291 Deployment Fails With Timeout When Webapp With Lots Of Servlet Mappings (Upgrade)

Description: When deploying a large Web application that has a large number of servlet mappings, the deployment hangs while trying to add the servlet mappings.This problem, described in Oracle Bug 8148113, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3.

Severity: Minor Warning

Rationale: Administration

17.3.292 Deployment Order Of Startup Classes Ignored

Description: The Deployment order for the startup classes is not taken into account while loading them.

Severity: Minor Warning

Rationale: Administration

17.3.293 Deployment Order Of Startup Classes Ignored (Upgrade)

Description: The Deployment order for the startup classes is not taken into account while loading them.This problem, described in Oracle Bug 8111459, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.3.294 Deployment To One Target Server In A Cluster Deploys Application To All Servers In Cluster

Description: When you deploy an application to one target server in a cluster, the application incorrectly gets deployed to all of the servers in the cluster. This error occurs because the JavaScript that selects the appropriate user selection is currently computing the incorrect HTML element that represents the cluster.

Severity: Minor Warning

Rationale: Administration

17.3.295 Deployment Unable To Resolve Symbolic Links On Unix

Description: When an application is deployed using the Administration Console from a symbolic link, the path is resolved to the actual path instead.

Severity: Minor Warning

Rationale: Administration

17.3.296 Deploymentexception Occurring During Startup Of A Managed Server In Msi Mode

Description: Oracle WebLogic Server fails to deploy libraries with an exception having the following key items when a managed server tries to start with Managed Server Independence (MSI) mode:BEA-149205Failed to initialize the application 'beehive-controls-1.0 [LibSpecVersion=1.0,LibImplVersion=1.0]' due to errorweblogic.management.DeploymentException: Exception occured while downloading files.

Severity: Minor Warning

Rationale: Administration

17.3.297 Deploymentexception Occurring During Startup Of A Managed Server In Msi Mode. (Upgrade)

Description: Oracle WebLogic Server fails to deploy libraries with an exception having the following key items when a Managed server tries to start with Managed Server Independence (MSI) mode:BEA-149205Failed to initialize the application 'beehive-controls-1.0 [LibSpecVersion=1.0,LibImplVersion=1.0]' due to errorweblogic.management.DeploymentException: Exception occured while downloading files.This problem, described in Oracle Bug 8106942, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.3.298 Diagnostic Archive Data Keeps Increasing

Description: Diagnostic Archive data keeps increasing, which will result in a disk full condition.

Severity: Minor Warning

Rationale: Administration

17.3.299 Diagnostic Image File Growing Rapidly (WIs V9)

Description: When JDBC profiling is turned on, it periodically dumps profiling information in the diagnostic store. Enabling it for extended time can cause the diagnostic store to grow. Several customers have run into this issue in production.This looks like the JDBC profiling flags were enabled and this might be one of the causes.The setting the following parameters and disabling the JDBC profile flags have resolved the issue:-Dcom.bea.wlw.netui.disableInstrumentation=true-D_Offline_FileDataArchive=true

Severity: Warning

Rationale: Performance

17.3.300 Diagnostic Images Cannot Be Captured On Managed Servers

Description: When trying to capture a diagnostic image on a Managed Server, Oracle WebLogic Server fails with an ImageSourceCreationException error as follows:<BEA-320127> <An error occurred while generating Image Source

configuration as part of the diagnostic image zip file:weblogic.diagnostics.image.ImageSourceCreationException: java.lang.NullPointerException at weblogic.management.provider.internal.ConfigImageSource.createDiagnosticImage(ConfigImageSource.java:105)

Severity: Warning

Rationale: Administration

17.3.301 Diagnostic Images Cannot Be Captured On Managed Servers. (Upgrade)

Description: When trying to capture a diagnostic image on a Managed Server, Oracle WebLogic Server fails with an ImageSourceCreationException error as follows:<BEA-320127> <An error occurred while generating Image Source configuration as part of the diagnostic image zip file:weblogic.diagnostics.image.ImageSourceCreationException: java.lang.NullPointerException at weblogic.management.provider.internal.ConfigImageSource.createDiagnosticImage(ConfigImageSource.java:105)This problem, described in Oracle Bug 8088096, has been fixed in Oracle WebLogic Server 10.0.

Severity: Minor Warning

Rationale: Administration

17.3.302 Direct Use Of Sun'S Internal Classes Causes Jaxb Functionality To Break On Aix

Description: The following Sun internal classes are used in our JAXB code:import com.sun.org.apache.xerces.internal.dom.DocumentImpl;import com.sun.org.apache.xerces.internal.dom.ElementNSImpl;import com.sun.org.apache.xerces.internal.dom.TextImpl;import com.sun.org.apache.xerces.internal.jaxp.datatype.XMLGregorianCalendarImpl;This causes those portions of Enterprise Server that use our JAXB classes (JMS capture, HTTP capture) to break on AIX, which uses IBM's implementation of Java.

Severity: Warning

Rationale: Subsystem Outage

17.3.303 Domain > Ws Security > Token Handler> Configuration Page Not Showing Javadoc Comments

Description: The Domain > Web service Security pages have issues:1. The assistant page has incorrect labels and no screen title.2. The assistant page does not autofill the Name field as it should.3. It is not possible to delete a Web service Security Configuration, and there are no error messages to notify you that the deletion does not work.

Severity: Minor Warning

Rationale: Administration

17.3.304 Domain > Ws Security > Token Handler> Configuration Page Not Showing Javadoc Comments

Description: When you create a new Web service security configuration, then create a new token handler, the token handler configuration page displays the name of a key (for example, webservice.webservicesecurity.tokenhandler.config.className.label.inlinehelp) instead of the Javadoc from the MBeans to the right of the fields. Note that the corresponding pagehelp file, pagehelp\webservice\webservicesecurity\tokenhandler \ConfigureTokenHandler.xml, correctly references the MBean. This indicates that there is a mismatch in what the JSP is looking for and the actual keys in the pagehelp file.

Severity: Minor Warning

Rationale: Administration

17.3.305 Domain Template Builder Generates Config.Xml Files Incorrectly

Description: When using Config Builder (config_builder.cmd) with the "Create Extension Template" option to generate a template JAR from configurations containing JMS resources, the following issues are observed after the JAR has been generated:(1) The JMS configuration file in the generated template JAR contains duplicatedJMS topic details.(2) Two config.xml files are generated, one in the root directory of the JAR, and one in the /config directory of the JAR. The file generated in the root directory is correct, but the file in the /config directory is missing several details, including the <target> info. Consequently, when the template JAR is used, the incorrect /config/config.xml file is then used.

Severity: Minor Warning

Rationale: Administration

17.3.306 Drop In Performance Shortly After Enterprise Server Start

Description: Under load, RFID Enterprise Server 2.0 experiences bad performance issues, specifically a drop in performance shortly after the 10-minute mark, and a long-term degradation in performance over time.

Severity: Warning

Rationale: Administration

17.3.307 Duplicate Global Type Error Thrown In A Web Service When <Xs:Include> Is Used (Upgrade)

Description: When a Oracle WebLogic Server Webservice has two operations in it and each operation takes one XMLBean, and these XSDs include an XML type via <xs:include> statement, it results in the following error when publishing the Web service to the server:weblogic.wsee.ws.WsException: Failed to create binding providersch-props-correct.2: Duplicate global type: Item@http://www.sample.org/ model (Original global type found in file:URI_SHA_1_26F162A02C0B8E453B3528125B8B9A9E38A76D2C/SaleService.wsdl) at weblogic.wsee.ws.WsBuilder.createRuntimeBindingProvider(WsBuilder.java: 355)This problem, described in Oracle Bug 8192827, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3.

Severity: Minor Warning

Rationale: Development

17.3.308 During Automatic Migration Managed Server Startup Delayed For 15 Minutes

Description: During automatic migration when the managed server starts if its administration server is not running it may take a long time for the managed server to start.To minimize the time of the managed server startup set theweblogic.security.embeddedLDAPConnectTimeout property on the managed server to specify an appropriate duration for the connection timeout. The value for this property represents seconds.This problem, described in Oracle Bug 8129103, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Warning

Rationale: Performance

17.3.309 During Automatic Migration Managed Server Startup Delayed For 15 Minutes. (Upgrade)

Description: During automatic migration when the managed server starts if its administration server is not running it may take a long time for the managed server to start.To minimize the time of the managed server startup set the:weblogic.security.embeddedLDAPConnectTimeout property on the managed server to specify an appropriate duration for the connection timeout. The value for this property represents seconds.This problem, described in Oracle Bug 8129103, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Performance

17.3.310 During Heavy Load After Transport Overload, Nullpointerexception Occurs In Messagehandler

Description: In Oracle WebLogic SIP Server 3.0:Under heavy load after a transport overload ends, a java.lang.NullPointerException occurs, as follows:<Nov 15, 2006 1:21:03 PM PST> <Notice> <WLSS.Transport> <BEA-330637> <Transport overload protection has ended.><Aug 23, 2007 3:53:57 PM CEST> <Error> <WLSS.Engine> <BEA-330101> <Exception while processing messages for call id: 29425-17908@111.222.33.44 java.lang.NullPointerException atcom.bea.wcp.sip.engine.server.MessageHandler $MessageQueue.processMessages(MessageHandler.java:212)...

Severity: Warning

Rationale: Development

17.3.311 Dweblogic.Management.Nologsystemproperties=True Has No Effect

Description: In Oracle WebLogic Server 8.1 Maintenance Pack 5, it was possible to disable the writing of system properties to the Oracle WebLogic Server log file by using the -Dweblogic.management.noLogSystemProperties=true parameter.However, after upgrading to Oracle WebLogic Server 9.x, this setting no longer has any effect.

Severity: Minor Warning

Rationale: Performance

17.3.312 Dynamic Wsdl Host Address Incorrect When Deployed In A Cluster

Description: An incorrect dynamic Web Service Definition Language (WSDL) location address is generated when a Web service is deployed on a cluster with multiple front-end hosts and ports. A new property, weblogic.wsee.useRequestHost, has been introduced in Oracle WebLogic Server 9.2.1 that allows generation of the WSDL location address either from the host header or by following the topology design.

Severity: Minor Warning

Rationale: Administration

17.3.313 Dynamic Wsdl Host Address Is Incorrect When A Web Service Is Deployed In A Cluster

Description: An incorrect dynamic WSDL location address is generated when a Web Service is deployed in a cluster with multiple front-end hosts and ports.

Severity: Warning

Rationale: Administration

17.3.314 Dynamic Wsdl Host Address Is Incorrect When A Web Service Is Deployed In A Cluster (Upgrade)

Description: An incorrect dynamic Web Service Definition Language (WSDL) location address is generated when a Web Service is deployed in a cluster with multiple front-end hosts and ports.This problem, described in Oracle Bug 8103127, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Administration

17.3.315 Ejb Client Stuck Rmi Call Over T3

Description: In Oracle WebLogic Server 9.2, a stuck situation can occur between a client and an EJB session. The problem happens if the client application and the EJB are deployed on different JVMs. For a standalone Java the issue can be resolved by using the wlclient.jar on the first order in the Application Classpath. However, for a client application that is running on a different JVM, the Stuck behavior still persists.You could see the following exception:java.rmi.UnmarshalException: Method not found: 'newMethod(Ljava.lang.String;)' at @ weblogic.rmi.internal.MethodDescriptor.getCanonical(MethodDescriptor.....

Severity: Critical

Rationale: Server Outage

17.3.316 Ejb Ql Case-Insensitive Feature Does Not Work For Order By And Group By Clauses

Description: The EJB QL parser does not allow the use of the UPPER and LOWER functions in the ORDER BY and GROUP BY clauses in an EJB QL query.

Severity: Warning

Rationale: Subsystem Outage

17.3.317 Ejb Aftercompletion Error Of Primary Key Could Not Be Found In The Lock Manager

Description: An EJB error is reported in afterCompletion, with the server log error similar to the following, even though the primary key is in place:[EJB:010108]The EJB Lock Manager has received an unlock request from EJB:sims.ejb.GridSetupLEB with primary key:CCM. However, this primary key could not be found in the Lock Manager.This indicates either an EJB container bug, or the equals and hashCode methods for the primary key class:com.sims.ejb.user.UserPK are implemented incorrectly. Please check the equals and hashCode implementations.javax.ejb.EJBException: [EJB:010108]The EJB Lock Manager has received an unlock request from EJB:sims.ejb.GridSetupLEB with primary key:CCM. ...

Severity: Minor Warning

Rationale: Administration

17.3.318 Ejb Aftercompletion Error Of Primary Key Could Not Be Found In The Lock Manager (Upgrade)

Description: An EJB error is reported in afterCompletion, even though the primary key is properly in place. The server log contains errors similar to the following:Ignoring error in afterCompletion. Object=weblogic.ejb.container.internal.TxManager$TxListener@17022f6, Exception=javax.ejb.EJBException: [EJB:010108]The EJB Lock Manager has received an unlock request from EJB:sims.ejb.GridSetupLEB with primary key:CCM. However, this primary key could not be found in the Lock Manager.This indicates either an EJB container bug, or the equals and hashCode methods for the primary key class:com.sims.ejb.user.UserPK are implemented incorrectly ...This problem, described in Oracle Bug 8099609, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3.

Severity: Minor Warning

Rationale: Administration

17.3.319 Ejb Client Compatibility Issue Between Mp1 And Mp2

Description: After migrating Oracle WebLogic Servers to version 9.2 Maintenance Pack 2, some standalone clients that use the 9.2 Maintenance Pack 1 version of the weblogic.jar are unable to access EJBs located on the 9.2 Maintenance Pack 2 Server.This applies only to some remote EJB methods that have methods containing generic list arguments.The issue does not occur with wlclient.jar on the client side.

Severity: Warning

Rationale: Development

17.3.320 Ejb-Based Web Service Leaks Ejb Beans When Message Handler Throws An Exception

Description: EJB-based Web Service leaks EJB beans when the message handler throws an exception. If the SOAP message handler encounters any exception, it fails to release the associated service bean from the cache, which will lead to the leak.

Severity: Critical

Rationale: Subsystem Outage

17.3.321 Ejb-Based Web Service Leaks Ejb Beans When Message Handler Throws An Exception. (Upgrade)

Description: The EJBs in EJB-based Web services leak when the message handler throws an exception. If the SOAP message handler encounters an exception, it fails to release the associated service bean from the cache, which will lead to the leak.This problem, described in Oracle Bug 8102108, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Subsystem Outage

17.3.322 Epoll Is Absent In Red Hat Linux Version 3.0

Description: The main reason of this error "java.io.IOException: Failed in epoll_wait: Function not implemented" is the absence of EPOLL in Red Hat Linux version 3.0.EPOLL does not exist in Red Hat Enterprise Linux version 3.0. This is a feature of the 2.6 kernel. Red Hat Enterprise Linux version 3 is based on the 2.4 Linux kernel. The EPOLL functionality was unable to be back ported to the 2.4 kernel due to issues with maintenance of the Application Binary Interface (ABI).EPOLL should be available in versions of Red Hat Enterprise Linux that use the 2.6 kernel or later, such as Red Hat Enterprise Linux 4. The Red Hat Enterprise Linux 4 ISO files are available to download to subscribers from Red Hat Network (RHN).

Severity: Warning

Rationale: Administration

17.3.323 Ejbhomequery Causes Nullpointerexception In Cachekey

Description: ejbHomeQuery causes NullPointerException in the EJB container.

Severity: Minor Warning

Rationale: Administration

17.3.324 Ejbhomequery Causes Nullpointerexception In Cachekey (Upgrade)

Description: ejbHomeQuery causes NullPointerException in the EJB container.This problem, described in Oracle Bug 8115318, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3.

Severity: Minor Warning

Rationale: Administration

17.3.325 Email Transport Is Not Handling Incoming Email Attachments In Various Email Formats

Description: When an email with an attachment is received by Oracle Service Bus, the email may not be handled properly. Instead, a NullPointerException similar to the following may be thrown:<Apr 12, 2007 5:02:44 PM EDT> <Error> <WliSbTransports> <machine> <AdminServer> <[ACTIVE] ExecuteThread: '2' for queue: 'weblogic.kernel.Default (self-tuning)'> <<WLS Kernel>> <> <> <1176411764962> <BEA-381014> <Error occurred for endpoint ProxyService$EmailProcessor

$ProxyServices$InboundEmailProcessor java.lang.NullPointerExceptionThe Oracle Bug 8116727 patch fixes this issue.

Severity: Warning

Rationale: Administration

17.3.326 Embedded Ldap Server Data Files Are Not Backed Up

Description: Embedded LDAP server data files are not backed up at the configured time.Backup of LDAP files is performed as a scheduled activity. However, after the first scheduled backup, the timer that triggers the next backup fails to be set, so the next scheduled backup activity does not take place. This behavior occurs in Oracle WebLogic Server 9.0, 9.1, and 9.2.

Severity: Warning

Rationale: Administration

17.3.327 Embedded Ldap Server Data Files Are Not Backed Up (Upgrade)

Description: Embedded LDAP server data files are not backed up at the configured time.Backup of LDAP files is performed as a scheduled activity. However, after the first scheduled backup, the timer that triggers the next backup fails to be set, so the next scheduled backup activity does not take place. This behavior occurs in Oracle WebLogic Server 9.0, 9.1, and 9.2.This problem, described in Oracle Bug 8066295, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Administration

17.3.328 Empty Host Listen Address For Node Manager Results In Illegalargumentexception

Description: In the Domain Configuration Wizard of the Oracle WebLogic Server Adminstration Console, you can select "All Local Addresses" for the NodeManager listen address. However, with that configuration, the Configuration Wizard generates the following field, in which the listen address can be empty:<node-manager><name>new_Machine_1</name><listen-address/></node-manager>With an empty host name specified for the Node Manager, if you open the Admin Console and select [Environment] -> [Servers], an error stack is shown in the server log. According to the error message, an empty host name is not allowed for the Node Manager.

Severity: Minor Warning

Rationale: Administration

17.3.329 Encrypted Data With Special Characters Cause Failure Of The Signature Reference Validation

Description: Signature reference validation fails if encrypted data contains special characters (for example, '&').

Severity: Warning

Rationale: Subsystem Outage

17.3.330 End-Of-Support Announcement For Microsoft Windows 2000 Server

Description: As of June 30, 2005, Microsoft has announced the end of mainstream support for the following platforms:* Windows 2000 Server* Advanced Server* Datacenter ServerOracle will continue supporting Oracle applications (for example Oracle JRockit on these platforms) at least through December 2006. A final notice of the end of support for Oracle JRockit on Windows 2000 will appear at least 12 months before the actual end of support.Note: Support for any Windows-specific issues must addressed by Microsoft via their extended support services.

Severity: Warning

Rationale: Not Complying with Specifications

17.3.331 End-Of-Support Announcement For Red Hat Enterprise Linux 2.1

Description: Oracle stopped supporting Red Hat Linux 2.1 on April 30, 2006.

Severity: Warning

Rationale: Not Complying with Specifications

17.3.332 Enhancement To Disable Passivation/Activation During Sfsb Replication In Cluster

Description: Enhancement to add deployment descriptor to turn off passivation/activation during replication of Stateful Session Bean (SFSB) in cluster.A new flag <passivate-during-replication> is added to weblogic-ejb-jar.xml. This flag is part of <stateful-session-descriptor> as below:<!ELEMENT stateful-session-clustering (home-is-clusterable?, home-load-algorithm?, home-call-router-class-name?, use-serverside-stubs?, replication-type?, passivate-during-replication?)>Set the flag to 'false' to avoid passivation/activation during SFSB replication. The default value for the flag is 'true'.

Severity: Minor Warning

Rationale: Administration

17.3.333 Entitlements Not Working For Visitor Tools Search Tab

Description: When using the portal visitor tools, portlets residing in entitled portlet categories are still visible to non-entitled users when initially viewing and arranging the portlets. This occurs prior to selecting the "add content" button within the visitor tools.

Severity: Critical

Rationale: Administration

17.3.334 Entitlements Not Working For Visitor Tools Search Tab (Upgrade)

Description: When using the portal visitor tools, portlets residing in entitled portlet categories are still visible to nonentitled users when initially viewing and arranging the portlets. This occurs prior to selecting the "add content" button within the visitor tools.This problem, described in Oracle Bug 8114802, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Administration

17.3.335 Entity Relationships Deployment Warnings And Runtime Npe

Description: EJBs with many-to-many unidirectional relationships in Oracle WebLogic Server 9.0 throws a warning to the server. The equivalent (barring annotation differences) application in Oracle WebLogic Server 8.1 produces no warning or a NullPointerException error.

Severity: Warning

Rationale: Administration

17.3.336 Error Adding Fd To Epoll Is Encountered During Server Startup (Upgrade)

Description: An error, Error adding FD to epoll, occurs while starting the Oracle WebLogic Server on Oracle JRockit with any 2.6 Linux Kernel version. The error you will see is similar to:####<10:44:04 AM EDT> <Error> <Socket> <XXXXXXX> <AdminServer> <ExecuteThread: '0' for queue: 'weblogic.socket.Muxer'> <<Oracle WebLogic Server Kernel>> <> <> <1146494644744> <BEA-000405> <Uncaught Throwable in processSockets weblogic.utils.NestedError: Error adding FD to epoll.weblogic.utils.NestedError: Error adding FD to epoll...This problem, described in Oracle Bug 8082331, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3.

Severity: Minor Warning

Rationale: User Viewable Errors

17.3.337 Error Adding Fd To Epoll Is Encountered During Server Startup

Description: An error, Error adding FD to EPOLL, occurs while starting the Oracle WebLogic Server on Oracle JRockit with any 2.6 Linux Kernel version. The error you will see is similar to:####<10:44:04 AM EDT> <Error> <Socket> <XXXXXXX> <AdminServer> <ExecuteThread: '0' for queue: 'weblogic.socket.Muxer'> <<WLS Kernel>> <> <> <1146494644744> <BEA-000405> <Uncaught Throwable in processSockets weblogic.utils.NestedError: Error adding FD to epoll.weblogic.utils.NestedError: Error adding FD to epoll...

Severity: Warning

Rationale: User Viewable Errors

17.3.338 Error Adding Fd To Epoll Is Encountered During Server Startup (Upgrade)

Description: An error, Error adding FD to epoll, occurs while starting the Oracle WebLogic Server on Oracle JRockit with any 2.6 Linux Kernel version. The error is similar to:####<10:44:04 AM EDT> <Error> <Socket> <XXXXXXX> <AdminServer> <ExecuteThread: '0' for queue: 'weblogic.socket.Muxer'> <<Oracle WebLogic Server Kernel>> <> <> <1146494644744> <BEA-000405> <Uncaught Throwable in processSockets weblogic.utils.NestedError: Error adding FD to epoll.weblogic.utils.NestedError: Error adding FD to epoll...This problem, described in Oracle Bug 8189643, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3.

Severity: Minor Warning

Rationale: User Viewable Errors

17.3.339 Error Occurs In Oracle Service Bus 2.6 During Xquery Transformation

Description: Oracle Service Bus Service proxy runs an XQuery transformation. During performance testing, after a period of time or of load or both, one proxy fails, with

error code BEA-382513. The underlying exception is:java.lang.IllegalStateException at weblogic.xml.query.compiler.Variable.createRTVariables(Variable.java:151) at weblogic.xml.query.compiler.Expression.createRunTimeVariables(Expression.java:570) at weblogic.xml.query.compiler.Expression.codeGen(Expression.java:392)

Severity: Warning

Rationale: Subsystem Outage

17.3.340 Error Occurs When Weblogic.Rootdirectory Is Specified As A Unc Path

Description: When the domain files are stored in a shared network location, and the domain root directory is specified using the UNC format(i.e., -Dweblogic.RootDirectory=\\machinename\foldername\domain), the server starts as expected. However, when attempting to navigate in the Administration Console, the following exception occurs:java.util.zip.ZipException: The system cannot find the path specified at java.util.zip.ZipFile.open(Native Method) at java.util.zip.ZipFile.<init>(ZipFile.java:204) at java.util.zip.ZipFile.<init>(ZipFile.java:235) .....

Severity: Minor Warning

Rationale: User Viewable Errors

17.3.341 Error Occurs When Weblogic.Rootdirectory Is Specified As A Unc Path (Upgrade)

Description: When the domain files are stored in a shared network location, and the domain root directory is specified using the UNC format(i.e., -Dweblogic.RootDirectory=\\machinename\foldername\domain), the server starts as expected. However, when attempting to navigate in the Administration Console, the following exception occurs:java.util.zip.ZipException: The system cannot find the path specified at java.util.zip.ZipFile.open(Native Method) at java.util.zip.ZipFile.<init>(ZipFile.java:204) at java.util.zip.ZipFile.<init>(ZipFile.java:235) .....This problem, described in Oracle Bug 8109928, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: User Viewable Errors

17.3.342 Error With Signature Verification When The Cr/Lf Is Inserted Between Tags

Description: While using Oracle WebLogic Server Web service stack and attempting to take advantage of the SAML assertion as signed by SOATest, an error occurs when Oracle WebLogic Server validates the signature. The problem occurs regardless if the client and Oracle WebLogic Server are running on Windows XP or Solaris 9. The SAML standard used is V1.1.There is a CR/LF inserted by the client between the SignatureValue end tag and the Signature tag:</ds:SignatureValue></ds:Signature>If the CR/LF is removed, there is no problem. SOATest version 5.1 is able to sign SAML assertions and this is the version used for the testing. Prior SOATest versions could not sign SAML.

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.3.343 Error With Signature Verification When The Cr/Lf Is Inserted Between Tags (Upgrade)

Description: While using Oracle WebLogic Server Web Service stack, and attempting to take advantage of the SAML assertion as signed by SOATest, an error occurs when Oracle WebLogic Server validates the signature. The problem occurs regardless if the client and Oracle WebLogic Server are running on Windows XP or Solaris 9. The SAML standard used is V1.1.There is a CR/LF inserted by the client between the SignatureValue end tag and the Signature tag:</ds:SignatureValue></ds:Signature>If the CR/LF is removed, there is no problem.

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.3.344 Errors Occur When Using Jax-Rpc Type Classes Generated By Oracle Workshop For Weblogic

Description: Schema enumeration types are not handled properly in the XBeans used by Oracle WebLogic Integration when generating JAX-RPC style objects from a Web Service Definition Language (WSDL) file. Per the JAX-RPC specifications, the generated JAVA types should not have a default constructor that is public. Since XBeans validate that Java Type objects have a default public constructor before binding them with the XML Schema objects, these special type JAX-RPC Java Objects fail to validate, causing the build error in Oracle WebLogic Integration.Example of a build error:'Type com.frk.middleware.xmlschemas.contactmodifyprofile.v100.ActionType has no default constructor and cannot be unmarshalled from XML.'

Severity: Critical

Rationale: Not Complying with Specifications

17.3.345 Errors Occur When Using Jax-Rpc Type Classes Generated By Oracle Workshop For Weblogic (Upgrade)

Description: Schema enumeration types are not handled properly in XBeans implementation (used by Oracle WebLogic Integration) when generating JAX-RPC style objects from a Web Service Definition Language (WSDL) file. Oracle Bug 8144075 has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3.

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.3.346 Errors Occur When Using Jre Instead Of Jdk For Running Oracle Weblogic Server

Description: eDocs for Oracle WebLogic Server 9.1 (http://download.oracle.com/docs/cd/E13222_01/wls/docs91/lockdown/secure.html) suggest running Oracle WebLogic Server with the JRE instead of the Java SDK.Following the advice, if we remove the JDK and start Oracle WebLogic Server 9.1 or 9.2 using theJRE, and when a simple precompiled JSP is deployed and accessed the following error is logged:java.lang.NoClassDefFoundError: com/sun/mirror/declaration/DeclarationThis missing class is actually contained in the "tools.jar" from JDK 1.5, and

is not available in the JRE.If tools.jar is included, then there will be no difference in using the Oracle WebLogic Server with Java SDK or not.

Severity: Minor Warning

Rationale: Administration

17.3.347 Errors Occur When Using Jre Instead Of Jdk For Running Oracle Weblogic Server. (Upgrade)

Description: The eDocs for Oracle WebLogic Server 9.1 (http://download.oracle.com/docs/cd/E13222_01/wls/docs91/lockdown/secure.html) suggest running Oracle WebLogic Server with the JRE instead of the Java SDK.When a simple precompiled JSP is deployed and accessed the following error is logged :java.lang.NoClassDefFoundError: com/sun/mirror/declaration/DeclarationThis problem, described in Oracle Bug 8094051, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.3.348 Errors Occur When Using Cached Remote Home Of New Redeployed Stateless Ejbs

Description: Errors occur when using cached remote home of new redeployed Stateless EJBs.The following is an example scenario in which this can occur:1. Two Oracle WebLogic Server 9.2 Maintenance Pack 1 domains are created.2. Business services implemented as Stateless EJBs are deployed on domain1.3. Other business services using those of domain1 are implemented on domain2.Business services on domain2 place the Remote Home EJB object from domain1 into the cache, so that domain2 does not look up home objects needlessly. Unfortunately, when redeploying business services on domain1, services on domain2 no longer work for the first call, but do work for the second call.

Severity: Warning

Rationale: Performance

17.3.349 Eventgeneratorutils Should Not Use Localhost

Description: If you specify the listen address explicitly, creating or viewing the Event Generator tab in the Oracle WebLogic Integration Console causes a ManagementException and a ConnectException to be thrown. This occurs because the server listens only at the specified address, while the console uses "localhost" to access the server.

Severity: Critical

Rationale: Development

17.3.350 Eventgeneratorutils Should Not Use Localhost (Upgrade)

Description: If you specify the listen address explicitly, creating or viewing the Event Generator tab in the Oracle WebLogic Integration Console causes a ManagementException and a ConnectException to be thrown. This occurs because the server listens only at the specified address, while the console uses "localhost" to access the server.This problem, described in Oracle Bug 8120430, has been fixed in Oracle WebLogic Server 10.3.

Severity: Minor Warning

Rationale: Development

17.3.351 Exception Java.Lang.Nullpointerexception Occurs When Using Consoleformatter

Description: The java.lang.NullPointerException occurs if an application tries to log a message using weblogic.logging.ConsolFormatter that was instantiated using the default constructor.

Severity: Minor Warning

Rationale: Administration

17.3.352 Exception Java.Lang.Nullpointerexception Occurs When Using Consoleformatter (Upgrade)

Description: The java.lang.NullPointerException occurs if an application tries to log a message using weblogic.logging.ConsolFormatter that was instantiated using the default constructor.This problem, described in Oracle Bug 8140586, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3.

Severity: Minor Warning

Rationale: Administration

17.3.353 Exception Results When Omitting Cluster Members From Server-Debug

Description: Enabling server-debug for only some members of a cluster results in the following Multicast socket receive error from the HeartbeatMessages: java.io.EOFException

Severity: Minor Warning

Rationale: Administration

17.3.354 Excessive Logging Of Ejb Exceptions In Logs

Description: Per the EJB specification, any business exception thrown from business methods needs to be handled at the client end (that is, the business exception propagates to the client end without any intervention from the server).However, when implementing a Web service using an EJB, with a business exception thrown from the exposed methods, the business exception thrown is propagated to client; but, an exception stack trace is also getting generated in the server log.This results in unneccessary growth of server logs.NOTE: The following flag suppresses the error message from the logs:-Dweblogic.wsee.component.exception=false

Severity: Minor Warning

Rationale: Administration

17.3.355 Expanding An Enterprise Application In Console Causes Loss Of Navigation Capabilities

Description: The Deployment Control page in the Oracle WebLogic Server Administration Console supports navigating into the modules, Web Services, and EJBs within a deployment. When a deployment is expanded, the ability to navigate to

previous or next pages in the deployment control table is disabled and the page number information is incorrect.

Severity: Warning

Rationale: Administration

17.3.356 Exporting Ws-Securitypolicy To Wsdl Needs To Explicitly Set The Default Assertions

Description: Microsoft explicitly spells out the default value of the assertion whenadvertising the policy (export).Arguments: One of the following policy intersect problems may occur if the value is not specified: false positive, unable to distinguish cases of 'no policy defined' and 'default value'.

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.3.357 Expression Language Variables Exposed By The Tagx Cause Jspx Compilation Failure

Description: Expression language variables exposed by the TAGX caused JSPX compilation to fail.

Severity: Warning

Rationale: Development

17.3.358 Expression Language Variables Exposed By The Tagx Cause Jspx Compilation Failure (Upgrade)

Description: Expression language variables exposed by the TAGX caused JSPX compilation to fail.This problem has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Development

17.3.359 Failed Deployment: Workshop Fails To Publish

Description: During deployment using DynamicUpdateOperation, Application MBeans are nulled out.Replication Steps:1. After four or five partial builds, Workshop fails to publish. Usually, but not always, the error is related to the fact that the root web application could not be deployed.2. While building the publishing fails.3. Then, as an attempted workaround, the following steps were taken: a. Shutdown server. b. Close Workshop. c. Delete the domain "tmp" folder on the admin server. d. Delete both the apt_src and build folder for the projects. e. Restart Workshop. f. Perform a complete clean up. g. Perform a complete build. h. Restart the server.However, this procedure works sometimes. When it fails, you must repeat steps 3.f and 3.g multiple times.

Severity: Critical

Rationale: Development

17.3.360 Failed Deployment: Workshop Fails To Publish (Upgrade)

Description: During deployment using DynamicUpdateOperation, Application MBeans are nulled out.Replication Steps:1. After four or five partial builds, Workshop fails to publish. Usually, but not always, the error is related to the fact that the root web application could not be deployed.2. While building the publishing fails.3. Then, as an attempted workaround, the following steps were taken: a. Shutdown server. b. Close workshop. c. Delete the domain "tmp" folder on the admin server. d. Delete both the apt_src and build folder for the projects. e. Restart Workshop. f. Perform a complete clean up. g. Perform a complete build. h. Restart the server.However, this procedure works sometimes. When it fails, you must repeat steps 3.f and 3.g multiple times.

Severity: Minor Warning

Rationale: Development

17.3.361 Fails To Deploy Libraries When Managed Server Tries To Start With Msi Mode

Description: Oracle WebLogic Server Managed Server fails to load the earlier deployed libraries with the following exception when it is being started in MSI (Managed Server Independence) mode:####<Oct 30, 2006 5:49:17 PM JST> <Error> <Deployer> <XXXXXX> <XXXXXXX> <[ACTIVE] ExecuteThread: '0' for queue: 'weblogic.kernel.Default (self-tuning)'> <<Oracle WebLogic Server Kernel>> <> <> <1162198157203> <BEA-149205> <Failed to initialize the application 'XXXXXX' due to error weblogic.management.DeploymentException: Exception occured while downloading files.weblogic.management.DeploymentException: Exception occured while downloading files at weblogic.deploy.internal.targetserver.datamanagement.AppDataUpdate.doDownload(AppDataUpdate.java:43) .....

Severity: Minor Warning

Rationale: Administration

17.3.362 Failure In A Class Preprocessing Recursive Calls In Oracle Jrockit R27.X

Description: In Oracle JRockit R27.1, the class bytes preprocessing facility was changed to allow for recursive preprocessing. This meant that a class preprocessor instance that was currently doing class preprocessing and through this caused a new class to be loaded would be recursively called with the new class bytes. This caused failures in some existing preprocessor implementations that relied on the old behavior of JRockit R27.1. In Oracle JRockit R27.5, this has been reverted. A thread doing class preprocessing will now silently refuse to preprocess any types created by executing the preprocessor itself.For example, in Oracle SOA Manager (ALSM), the error "Nanoagents not loading" occurs when used with Oracle JRockit R27.3.1.

Severity: Warning

Rationale: Subsystem Outage

17.3.363 Failure In Heartbeat Trigger For Rjvm When T3 Outbound Channel Is Configured

Description: Repeated occurrence of missed RJVM heartbeat errors in Admin Server logs as shown below, when managed server(s) have an outbound channel enabled and configured with t3/t3s protocol.Missed heartbeat RJVM error in AdminServer

log(managed server running healthy):.....Failure in heartbeat trigger for RJVM: -1397576259334623576S:111.222.333.444: [7030,7030,-1,-1,-1,-1,-1]:tf7domain:TF701_1java.io.IOException: The connection manager to ConnectionManager for: 'weblogic.rjvm.RJVMImpl@149d226 - id: '-1397576259334623576S:111.222.333.444:[7030,7030,-1,-1,-1,-1,-1]:tf7domain:TF701_1' connect time: 'Tue May 22 16:53:57 CEST 2007'' has already been shut down. at weblogic.rjvm.ConnectionManager.getOutputStream(ConnectionManager.java: 1663) ...

Severity: Warning

Rationale: User Viewable Errors

17.3.364 Failure In Heartbeat Trigger For Rjvm When T3 Outbound Channel Is Configured (Upgrade)

Description: Repeated occurrence of missed RJVM heartbeat errors in Admin Server logs, when managed server(s) have an outbound channel enabled and configured with t3/t3s protocol.This problem, described in Oracle Bug 8065523, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3.

Severity: Minor Warning

Rationale: User Viewable Errors

17.3.365 Failure In Heartbeat Trigger For Rjvm When T3 Outbound Channel Is Configured. (Upgrade)

Description: Repeated occurrence of missed RJVM heartbeat errors in Admin Server logs, when managed server(s) have an outbound channel enabled and configured with t3/t3s protocol.This problem, described in 8065523, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3.

Severity: Minor Warning

Rationale: User Viewable Errors

17.3.366 Failure To Deploy A Jms Connection Factory Due To Weblogic.Application.Moduleexception

Description: Error when starting server (sample server log excerpt is shown below), thus preventing initialisation of the JMS server:weblogic.application.ModuleException: [Management:141213]An attempt to initialize property FlowMinimum failed because of java.lang.IllegalArgumentException: FlowMinimum has to be less than FlowMaximum at weblogic.jms.frontend.FEConnectionFactory.initialize(FEConnectionFactory.java:370) at weblogic.jms.frontend.FEConnectionFactory.prepare(FEConnectionFactory.java: 1530) ...

Severity: Minor Warning

Rationale: Subsystem Outage

17.3.367 Failure To Deploy A Jms Connection Factory Due To Weblogic.Application.Moduleexception (Upgrade)

Description: Error when starting server prevents initialisation of the JMS server:Failed to deploy a JMS connection factory "dfpSystemModule\!dfpConnectionFactory" due to weblogic.application.ModuleException: [Management:141213]An attempt to initialize property FlowMinimum failed because of java.lang.IllegalArgumentException: FlowMinimum has to be less than FlowMaximum.weblogic.application.ModuleException: [Management:141213]An attempt to initialize property FlowMinimum failed because of java.lang.IllegalArgumentException: FlowMinimum has to be less than FlowMaximum at weblogic.jms.frontend.FEConnectionFactory.initialize(FEConnectionFactory.java:370)...This problem, described in Oracle Bug 8119451, has been fixed in Oracle WebLogic Server 10.0.

Severity: Minor Warning

Rationale: Subsystem Outage

17.3.368 Failure To Deploy Libraries When A Managed Server Tries To Start In Msi Mode. (Upgrade)

Description: Oracle WebLogic Server Managed Server fails to load the earlier deployed libraries with the following exception when it is being started in Managed Server Independence (MSI) mode:[ACTIVE] ExecuteThread: '0' for queue: 'weblogic.kernel.Default (self-tuning)'> <<WLS Kernel>> <> <> <1162198157203> <BEA-149205> <Failed to initialize the application 'XXXXXX' due to error weblogic.management.DeploymentException: Exception occured while downloading files.weblogic.management.DeploymentException: Exception occured while downloading files at weblogic.deploy.internal.targetserver.datamanagement.AppDataUpdate.doDownload(AppDataUpdate.java:43) .....This problem, described in Oracle Bug 8106942, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.3.369 Field To Configure Unitoforderrouting For Distributed Destinations Missing

Description: The page Module -> Distributed Destination -> General should contain a field to configure the UnitOfOrder Routing policy. The relevant Bean and attributes are DistributedDestinationBean.setUnitOfOrderRouting().

Severity: Minor Warning

Rationale: Administration

17.3.370 File Event Generator May Generate Event Before File Has Been Completely Uploaded

Description: When a File Event Generator has been configured to poll a directory at a regular interval, it is possible that it may attempt to process that file while it is being updated.This can happen if the polling interval is set to less time than it takes to complete a file upload to the polling directory. As a result, the file will be archived to

the polling directory with incomplete data and processes will be invoked using this incomplete data.

Severity: Warning

Rationale: Subsystem Outage

17.3.371 File Event Generator May Generate Event Before File Has Been Completely Uploaded. (Upgrade)

Description: When a File Event Generator has been configured to poll a directory at a regular interval, it is possible that it may attempt to process that file while it is being updated.This can happen if the polling interval is set to less time than it takes to complete a file upload to the polling directory. As a result, the file will be archived to the polling directory with incomplete data and processes will be invoked using this incomplete data.This problem, described in Oracle Bug 8189304, has been fixed in Oracle WebLogic Server 10.0 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Subsystem Outage

17.3.372 File Name Is Corrupted When Uploading Application With Non-Ascii File Name

Description: When uploading an application with a non-ASCII name in the Oracle WebLogic Server Administration Console, the file name appears garbled.

Severity: Minor Warning

Rationale: Administration

17.3.373 File Name Not Honored When Set As A Header In The Ftp Transport

Description: The file name set as a header in the FTP transport is not honored by Oracle Service Bus 2.5/2.6. Instead, the file name uses the format: Prefix + "-" + GUID + "-" + filename + SuffixHere, the prefix and suffix are required, while the filename is optional.The patch to Oracle Bug 8123250 changes this behavior so that the FTP transport now works in the following way:- Prefix and Suffix are now optional- GUID (message id) is used in filename only if filename header is not set in the pipeline at runtime.- The filename generated is either:<prefix>+<filename from header> +<suffix>or<prefix>+<GUID>+<suffix>- A file that exists in the FTP server with the same generated filename is overwritten.On applying the patch, users are advised to clear the server cache.

Severity: Warning

Rationale: Administration

17.3.374 Fmlxmlcnv.Xmltofml32 Method Cannot Handle A Buffer That Includes '&'

Description: When using Oracle WebLogic Tuxedo Connector with Oracle WebLogic Server 9.2, the FmlXmlCnv.XMLtoFML32 method fails to convert the XML to FML32 if an element of the VIEW32 buffer includes an ampersand ("&").

Severity: Warning

Rationale: Development

17.3.375 Foreign Jndi Connection Fails On Startup When Using A Cluster

Description: When a Foreign JNDI connection between two Oracle WebLogic Server domains in a cluster is attempted, the server in the calling domain fails to start with following exception. This is due to the Foreign JNDI Manager service being started prior to cluster services starting.Server subsystem failed. Reason: java.lang.NullPointerExceptionjava.lang.NullPointerExceptionat weblogic.cluster.ServiceAdvertiser.announceOffer(ServiceAdvertiser.java:117)at weblogic.cluster.ServiceAdvertiser.offerService(ServiceAdvertiser.java:70)...

Severity: Warning

Rationale: Administration

17.3.376 Foreign Jndi Connection Fails On Startup When Using A Cluster. (Upgrade)

Description: When a Foreign JNDI connection between two Oracle WebLogic Server domains in a cluster is attempted, the server in the calling domain fails to start with following exception. This is due to the Foreign JNDI Manager service being started prior to cluster services starting.####<Jun 1, 2006 2:45:59 PM MEST> <Critical> <WebLogicServer> <BEA-000386> <Server subsystem failed. Reason: java.lang.NullPointerExceptionjava.lang.NullPointerExceptionat weblogic.cluster.ServiceAdvertiser.announceOffer(ServiceAdvertiser.java:117).....This problem, described in Oracle Bug 8051204, has been fixed in Oracle WebLogic Server 9.2.

Severity: Minor Warning

Rationale: Administration

17.3.377 Foreign Jndi Link Causes The Server Jndi Tree To Be Incorrectly Displayed In The Administration Console

Description: If a configuration contains foreign JNDI links, the Oracle WebLogic Server Administration Console fails to display the JNDI tree. There are no exceptions, and the Administration Console displays a blank page. This makes it impossible to browse the JNDI tree for debugging purposes or to administer the JNDI security policies.

Severity: Minor Warning

Rationale: Administration

17.3.378 Foreign-Connection-Factory Credentials Are Not Taken To Account If Provider-Url Specified

Description: JMS proxy using local foreign JMS server configuration with credentials given is not able to connect to the remote system.

Severity: Warning

Rationale: Subsystem Outage

17.3.379 Get More Than 10 Applications Displayed In Console Deployments Page

Description: The Admin Console Deployments Table displays only 10 deployments per page.

Severity: Minor Warning

Rationale: Administration

17.3.380 Get More Than 10 Applications Displayed In Console Deployments Page (Upgrade)

Description: The Admin Console Deployments Table displays only 10 deployments per page.This problem, described in Oracle Bug 8110216, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3.

Severity: Minor Warning

Rationale: Administration

17.3.381 Getting *Sys-Package-Mgr*: Can'T Write Cache File While Running Wls Tools

Description: When multiple users run Domain Provisioning tools like the Configuration Wizard, Domain Stop Server Script, or WebLogic Scripting Tool Offline Scripting, it is possible that subsequent users of the tool might encounter error messages like the following:*sys-package-mgr*: can't write cache file for '/Oracle_HOME/jrockit90_150_06/lib/tools.jar'*sys-package-mgr*: can't write cache file for '/WLS_HOME/server/lib/weblogic.jar'*sys-package-mgr*: can't write cache file for '/WLS_HOME/server/lib/webservices.jar'*sys-package-mgr*: can't write cache file for '/WLS_HOME/common/eval/pointbase/lib/pbclient51.jar'*sys-package-mgr*: can't write cache file for '/Oracle_HOME/jrockit90_150_06/jre/lib/managementapi.jar'...

Severity: Minor Warning

Rationale: Administration

17.3.382 Global Multicast Address Has Cluster Jndi Replication Issues

Description: Using global multicast addresses between 230.0.0.1 and 239.192.0.0 causes cluster issues. For example, the JMS destination may not replicate to all members of the cluster although the JNDINameReplicated attribute is set to "true."

Severity: Warning

Rationale: Administration

17.3.383 Group Circular Reference In External Authenticator Causes Ldap To Hang

Description: By default, Oracle WebLogic Server does not check for Group circularity for any externally configured LDAP Authenticators (iPlanet, Active Directory, Novell, Open LDAP, etc.).Circular reference:Group A is a member of Group BGroup B is a member of Group AWhen a group circularity exists in the backend LDAP, so many LDAP connections are created (due to the backend LDAP group having itself as a member), that a server crash can result.

Severity: Minor Warning

Rationale: Subsystem Outage

17.3.384 Http Head Request Throws Servletexception (Wls V9)

Description: If a servlet calls RequestDispatcher.forward(), the following error occurs for a HEAD request: javax.servlet.ServletException: Original response not available.

Severity: Warning

Rationale: Administration

17.3.385 Http Head Request Throws Servletexception (Wls V9, Upgrade)

Description: If a servlet calls RequestDispatcher.forward(), the following error occurs for a HEAD request: javax.servlet.ServletException: Original response not available.This problem, described in Oracle Bug 8103455, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.3.386 Http Post Method Can Be Tuned Via Maxpostsize To Harden Security

Description: A denial-of-service attack is a malicious attempt to overload a server by sending more requests than it can handle, preventing access to a service. Attackers may overload the server by sending huge amounts of data in an HTTP POST method. The client can get an HTTP error code 413 (Request Entity Too Large) or the connection may be broken.Prevent this type of attack by setting the MaxPostSize parameter. This limits the number of bytes of data that can be received in a POST from a single request. (By default, the value for MaxPostSize is -1, i.e. unlimited.) If an attacker sends an HTTP POST that exceeds the limit you specify, it triggers a MaxPostSizeExceeded exception and the server logs a "POST size exceeded the parameter MaxPostSize" message.

Severity: Critical

Rationale: Server Outage

17.3.387 Http Connection Is Closed After Receiving Options Query With No Content-Length Header

Description: HTTP connection is closed after receiving OPTIONS query with no Content-Length header.

Severity: Minor Warning

Rationale: Administration

17.3.388 Http Connection Is Closed After Receiving Options Query With No Content-Length Header. (Upgrade)

Description: HTTP connection is closed after receiving OPTIONS query with no content-length header.This problem, described in Oracle Bug 8091366, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Administration

17.3.389 Http Tunneling Protocol Exception When Managed Server Are Run Through The Node Manager

Description: On a UNIX-like system, if you start your managed servers from a Node Manager, the Administration Server can throw frequent Protocol Exceptions with the message, "HTTP tunneling is disabled."

Severity: Minor Warning

Rationale: Administration

17.3.390 Httpclusterservlet Uses Non-Ssl Port When Secureproxy Is On

Description: HTTPCluster proxy tries to connect with the non-SSL ports even when the SecureProxy is set to ON. There are two issues regarding this:(1) When SecureProxy is ON, the proxy should not contact non-SSL ports.(2) Due to a problem with the session stickiness, the dynamic servlet list is not updated correctly.

Severity: Warning

Rationale: Non-User Viewable Errors

17.3.391 Handling Of Unavailableexception Does Not Comply With Servlet 2.4 Spec. (Upgrade)

Description: UnavailableException does not comply with Servlet 2.4 Specifications for permanent and temporary unavailability. When a servlet throws temporary UnavailableException with the time period of the temporary unavailability, Oracle WebLogic Server still returns SC_NOT_FOUND (404) response. For Oracle WebLogic Server to comply with the specification, Oracle WebLogic Server would return 503 with Retry-After header OR treat it completely the same as permanent unavailability.This problem, described in Oracle Bug 8109719, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.3.392 Hibernate And Ehcache Cache Locking Problem With Multiple Managed Servers On Same Server

Description: When Hibernate and ehcache are used with Oracle WebLogic Server, the ehcache component writes cached objects to the file system defined by the property java.io.tmpDir. This, in itself, is not an issue. However, when there are two or more managed servers running on each physical server, these managed servers write to the same directory in the file system using the same file names. Consequently, the servers are sharing resources that require explicit locks in order to modify the files, which can result in a deadlock condition.

Severity: Critical

Rationale: Administration

17.3.393 High Memory Consumption When Using Expression Language In Jsp

Description: The symptom is a high number of garbage collections happening when using JSP with Expressions Language.Memory is reclaimed by the garbage collection so this is not a memory leak, but a high usage of memory (high rate of object creation).Using JSP without Expressions Language has a pattern of not using memory that much.

Severity: Warning

Rationale: Performance

17.3.394 High Memory Consumption When Using Expression Language In Jsp (Upgrade)

Description: The symptom is a high number of garbage collections happening when using JSP with Expressions Language.Memory is reclaimed by the garbage collection (GC). So, this is not a memory leak, but a high usage of memory (high rate of object creation).Using JSP without Expressions Language has a pattern of not using memory that much.This problem, described in Oracle Bug 8059776, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3.

Severity: Minor Warning

Rationale: Performance

17.3.395 How Do You Persist Enabling Library Services After Removing Application In Dev Mode?

Description: Removing an application causes the associated deployment plan files to be discarded. A new deployment no longers carries any plan changes you may have made (such as enabling library services).

Severity: Minor Warning

Rationale: Development

17.3.396 Httpproxyservlet Keeps Reading Response From Backend After Client Closes Connect

Description: When using HttpProxyServlet in Oracle WebLogic Server 9.2 as Reversed Proxy Server (RPS), the socket is to be closed when the browser is closed or navigated to some other site. However, the connection is found to be kept alive, and it keeps reading from the socket.Symptom can be verified in server thread dumps.

Severity: Minor Warning

Rationale: Administration

17.3.397 Httpproxyservlet Keeps Reading Response From Backend After Client Closes Connect. (Upgrade)

Description: When using HttpProxyServlet in Oracle WebLogic Server 9.2 as Reversed Proxy Server (RPS), the socket is to be closed when the browser is closed or navigated to some other site. However, the connection is found to be kept alive, and it keeps reading from the socket.Symptom can be verified in server thread dumps. This problem, described in Oracle Bug 8118037, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Administration

17.3.398 Httpservletrequest.Getremoteuser() Returns Null (Wls V9.2)

Description: After upgrading to Oracle WebLogic Server 9.2 Maintenance Pack 2 or Maintenance Pack 3, the call request.getRemoteUser() returns null because Oracle WebLogic Server is not authenticating the user.Workaround: Change the source code to request.getHeader('REMOTE_USER') to get the remote user.

Severity: Minor Warning

Rationale: Administration

17.3.399 Httpurlconnection Causes A Socket Leak That Goes To Close_Wait State

Description: HttpURLConnection is not closing the sockets that go to CLOSE_WAIT state, resulting in a socket leak.

Severity: Warning

Rationale: User Viewable Errors

17.3.400 Httpurlconnection Causes A Socket Leak That Goes To Close_Wait State. (Upgrade)

Description: HttpURLConnection is not closing the sockets that go to CLOSE_WAIT state, resulting in a socket leak.This problem, described in Oracle Bug 8114063, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: User Viewable Errors

17.3.401 Httpurlconnection Fails To Post On Retry

Description: When using weblogic.net.HttpURLConnection to connect to an external system, POST requests to the system fail on retry.

Severity: Warning

Rationale: Subsystem Outage

17.3.402 Httpurlconnection Fails To Post On Retry. (Upgrade)

Description: When using weblogic.net.HttpURLConnection to connect to an external system, POST requests to the system fail on retry.This problem, described in Oracle Bug 8125047, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: Subsystem Outage

17.3.403 Ibm Jdk 64 Bit Is Not Supported By All Versions Of Oracle Weblogic Server

Description: IBM JDK 64 bit is not supported for all versions of Oracle WebLogic Server. Oracle will provide support to the best of its ability. You may be advised to revert to a supported JVM configuration if you encounter an Oracle issue that appears to be JVM-related.

Severity: Warning

Rationale: Administration

17.3.404 Idl Repository Id Of Array Is Incompatible With Sun Jdk Rmic

Description: When generating IDL files, there are compatibility issues with the java.lang.String[] repository ID as follows:* Sun JDK rmic generates: "RMI:Ljava.lang.String;:071DA8BE7F971128:A0F0A4387A3BB342"* Oracle WebLogic Server IIOP/CORBA Impl generates: "RMI:[Ljava.lang.String;:071DA8BE7F971128:ADD256E7E91D7B47"

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.3.405 Idl Repository Id Of Array Is Incompatible With Sun Jdk Rmic (Upgrade)

Description: When generating IDL files, there are compatibility issues with the java.lang.String[] repository ID as follows:* Sun JDK rmic generates: "RMI:Ljava.lang.String;:071DA8BE7F971128:A0F0A4387A3BB342"* Oracle WebLogic Server IIOP/CORBA Impl generates: "RMI:[Ljava.lang.String;: 071DA8BE7F971128:ADD256E7E91D7B47"This problem, described in Oracle Bug 8086027, has been fixed in Oracle WebLogic Server 9.2.

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.3.406 Ioexception Invoking Web Service Method Through Jms Using Default Charset (Wls V9.2.1, Upgrade)

Description: An IOException occurs when invoking a Web Service method through JMS that uses the default charset.For example, see Russian characters with code 0418H in UTF8.This problem, described in Oracle Bug 8124232, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3.

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.3.407 Ioexception Invoking Web Service Method Through Jms Using Default Charset (Wls V9.2.2, Upgrade)

Description: An IOException occurs when invoking a Web service method through JMS that uses the default charset.As an example, see the Russian characters with code 0418H in UTF8.This problem, described in Oracle Bug 8124232, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3.

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.3.408 Ioexception Invoking A Web Service Method Through Jms Using Default Charset

Description: An IOException occurs when invoking a Web service method through JMS that uses the default charset.For example, see Russian characters with code 0418H in UTF8.

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.3.409 Ioexception Occurs When Resource-Reload-Check-Secs Is Disabled

Description: When resource-reload-check-secs is disabled (set to -1), if a browser attempts to access with Cache Control: no-cache header, and if static files are modified to a small size, Oracle WebLogic Server throws the following exception:<2006/06/12 15??15??34?b JST> <Error> <HTTP> <BEA-101019><[weblogic.servlet.internal.WebAppServletContext@168fa45 -name:

'DefaultWebApp', context-path: '/DefaultWebApp'] Servlet failed with IOExceptionjava.io.IOException: failed to read '2' bytes from InputStream; clen: 39remaining: 2 count: 37 atweblogic.servlet.internal.ChunkOutput.writeStream(ChunkOutput.java:411) atweblogic.servlet.internal.ChunkOutputWrapper.writeStream(ChunkOutputWrapper.java:168)...>

Severity: Warning

Rationale: Not Complying with Specifications

17.3.410 Ipv6 Is Not Available On Windows Xp With Any Available Jvms

Description: The IPv6 implemented by Microsoft Windows XP does not support dual mode sockets and cannot be used with any available JVMs. If SIP traffic is enabled by configuring a network channel with an IPv6 address on Windows XP with either the Sun or Oracle JRockit JVMs, the following exception occurs:com.bea.wcp.sip.engine.connector.transport.TransportException: Address family not supported by protocol family: bind at com.bea.wcp.sip.engine.connector.transport.UdpTransportModule.start(UdpTransportModule.java:166) ...

Severity: Minor Warning

Rationale: Development

17.3.411 If Record-Route Header Enabled, External Listen Port Set To 5060 Instead Of Specified Port

Description: If you use the Administration Console to configure SIP channels with "External Listen Address" and "External Listen Port," the following occurs, as expected:* Oracle WebLogic SIP Server (WLSS) replaces the Via header of the WLSS IP address with the IP address specified for "External Listen Address."* WLSS replaces the WLSS port number with the port number specified for "External Listen Port."However, if you enable the Record-Route header in your application (setRecordRoute(true)), the following occurs:* WLSS correctly sets the IP address of the Record-Route header to the address specified for "External listen address."* WLSS incorrectly sets the Record-Route header port number to 5060, instead of the port specified for "External Listen Port."

Severity: Warning

Rationale: Administration

17.3.412 If Connection Fails, Server Attempts To Reconnect To Target Host Via Httpurlconnection

Description: In Oracle WebLogic Server 9.0.x and earlier releases, if a connection fails, the server does not attempt to reconnect. This behavior changed for Oracle WebLogic Server 9.1 and later releases. In Oracle WebLogic Server 9.1.x, if a connection fails, the server tries to reconnect to a target host. If the target host is down, Oracle WebLogic Server continues to wait for the response until double the amount of the specified TCP timeout has lapsed.For example, if the TCP timeout is set to 3 minutes, Oracle WebLogic Server 9.0 waits for a response for 3 minutes, while Oracle WebLogic Server 9.1 waits for 6 minutes. This has an impact on performance when the target system is down.

Severity: Minor Warning

Rationale: Performance

17.3.413 If Weblogic_Patch.Jar Is After Weblogic.Jar The Installed Patches Have No Effect

Description: Some customers write their own startup and environment scripts. Sometimes they invert the CLASSPATH order. When this occurs, patches applied with BSU are not active even if Oracle Enterprise Manager detects them. The weblogic_patch.jar must always come before weblogic_sp.jar and weblogic.jar in the classpath.

Severity: Critical

Rationale: Administration

17.3.414 If You Use Wls Admin Console To Enable Wtc Debug, Tpcall Returns A Tpesystem Error

Description: When you use the Oracle WebLogic Server Administration Console to enable the debugWTCUdata flag, an atpesystem error occurs on the second tpcall.

Severity: Warning

Rationale: User Viewable Errors

17.3.415 If You Use Wls Admin Console To Enable Wtc Debug, Tpcall Returns A Tpesystem Error (Upgrade)

Description: When you use the Oracle WebLogic Server Administration Console to enable the debugWTCUdata flag, an atpesystem error occurs on the second tpcall.This problem, described in Oracle Bug 8122871, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 2.

Severity: Minor Warning

Rationale: User Viewable Errors

17.3.416 Illegalargumentexception Can Occur When Accessing Ws-Policy Tab In Console

Description: The following exception can occur when you attempt to access the "WS-Policy" configuration tab in the Oracle WebLogic Server Administration Console:java.lang.IllegalArgumentException: The property you provided 'contents' of form 'deploymentPlanForm' must not be set to null.

Severity: Minor Warning

Rationale: Administration

17.3.417 Illegalargumentexception When Empty Array Is Received From Web Service (Upgrade)

Description: Web services with a single dimension SOAP array and variable length are not handled properly. The Web Services fail when processing empty arrays.java.lang.IllegalArgumentException: Illegal Capacity: -1at java.util.ArrayList.<init>(ArrayList.java:111)at com.bea.staxb.runtime.internal.util.collections.ArrayListBasedObjectAccumulator.createNewStore(ArrayListBasedObjectAccumulator.java:42)at

com.bea.staxb.runtime.internal.util.collections.ObjectAccumulator.<init>(ObjectAccumulator.java:39)This problem, described in Oracle Bug 8122845, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 3.

Severity: Minor Warning

Rationale: Administration

17.3.418 Illegalargumentexception When Empty Array Is Received From Web Service

Description: Web services with a single dimension SOAP array and variable length are not handled properly. The Web services fail when processing for empty arrays.java.lang.IllegalArgumentException: Illegal Capacity: -1at java.util.ArrayList.<init>(ArrayList.java:111)at com.bea.staxb.runtime.internal.util.collections.ArrayListBasedObjectAccumulator.createNewStore(ArrayListBasedObjectAccumulator.java:42)at com.bea.staxb.runtime.internal.util.collections.ObjectAccumulator.<init>(ObjectAccumulator.java:39)

Severity: Warning

Rationale: Administration

17.3.419 In Weblogic Sip Server 3.1, Sip Session Is Not Destroyed When Setexpires() Is Invoked

Description: In Oracle WebLogic SIP Server 3.1, SIP sessions never expire, when "setExpires()" is called on SipApplicationSession.

Severity: Warning

Rationale: Not Complying with Specifications

17.3.420 In A Forking Proxy Scenario Under High Load, A Java.Lang.Illegalstateexception Is Raised

Description: In a forking proxy scenario under high load, noAckReceived after IllegalStateException as follows:<Oct 16, 2007 3:19:53 PM CEST> <Error> <WLSS.Transport> <BEA-330608> <Socket errorjava.lang.IllegalStateException: This transaction has been completed already. at com.bea.wcp.sip.engine.server.SipServletResponseImpl.<init>(SipServletResponseImpl.java:75) at com.bea.wcp.sip.engine.server.SipServletRequestImpl.createResponse(SipServletRequestImpl.java:1013) at com.bea.wcp.sip.engine.server.SipServletRequestImpl.createResponse(SipServletRequestImpl.java:994) at com.bea.wcp.sip.engine.server.ServerTransaction.rcvCancel(ServerTransaction.java:632) at com.bea.wcp.sip.engine.server.TransactionManager.receiveContinuationRequest(TransactionManager.java:1235)

Severity: Warning

Rationale: Performance

17.3.421 In A Forking Proxy Scenario, Oracle Weblogic Sip Server Forwards All The Responses

Description: Based on the SIP Servlet API version 1.0 Chapter 8.2.3, the container should notify a forking application only when the "best" response is received; that is, when final responses have been received from all destinations except "200 OK." However, when an application forks two or more destinations, Oracle WebLogic SIP Server 3.0 informs the application about all responses.Resolution:The patch to Oracle Bug 8119447 fixes the forking proxy issues described above. However, a memory leak can occur under heavy load conditions. Therefore, Oracle recommends applying the the patch to Oracle Bug 8113068 along with the patch to Oracle Bug 8119447.

Severity: Warning

Rationale: Not Complying with Specifications

17.3.422 In Forking Proxy, Wlss Sends Ack To To Tag Of 183 Instead Of To Tag Of Final Response

Description: A forking proxy returns to Oracle WebLogic SIP Server UAS different "To:" header tags in the "183 Session Progress" and "200 OK."When SipServletResponse.createAck() is invoked on the 200 OK, the ACK request has the "To:" header tag of the 183 response, instead of the 200 response.Use case:The following typical call flow illustrates the issue: -> UAS1UAC->WLSS-B2BUA-> Forking Proxy -> UAS2The 183 is coming from the UAS1 session, and the 200 from the UAS2 session (different "To:" tag). When ACK is generated for the 200 OK response, the container creates the ACK with 183 "To:" tag.Resolution:The issue is fixed by the patch to Oracle Bug 8118703.

Severity: Warning

Rationale: Development

17.3.423 Incorrect Failedmessagestotalcount For Saf In Admin Console When Jms Messages Expire

Description: The Administration Console is not showing the correct value for FailedMessagesTotalCount for SAF agents even though the messages expire after the configured TimeToLive value. However, this value is getting updated if the messages are manually expired using the Expire all tab of the console.

Severity: Minor Warning

Rationale: Administration

17.3.424 Incorrect Info Message In Logs: Java.Net.Protocolexception: Http Tunneling Is Disabled

Description: Under certain conditions, an inaccurate Info message (see below) is written to the server logs continuously, every few seconds. This happens during a particular sequence of starting the Oracle WebLogic Server Administration and managed servers.Example:1. The Administration Server Listen Address is set to something other than "localhost."2. "TunnelingEnabled" is set to "false" (this is the default setting).The following error then occurs:'weblogic.kernel.Default (self-tuning)'> <<anonymous>> <> <> <1215144474983> <000000> <HTTPClntLogin: Login rejected with code: 'Failed', reason: java.net.ProtocolException: HTTP tunneling

is disabled at weblogic.rjvm.http.HTTPServerJVMConnection.acceptJVMConnection(HTTPServerJVMConnection.java:88)

Severity: Minor Warning

Rationale: Administration

17.3.425 Incorrect Jmsexception For Jmsserver Does Not Exist In Activate() Of Wlst

Description: Oracle WebLogic Scripting Tool (WLST) running a script generated by execToscript fails on activate():WLSTException: 'Error occured while performing activate :Error while Activating changes.[JMSExceptions:045032]While attempting to create destination WSInternaljms.internal.queue.WSStoreForwardQueuemyserver in module interop-jms the JMSServer of name WSStoreForwardInternalJMSServermyserver could not be found. Use dumpStack() to view the full stacktrace'

Severity: Minor Warning

Rationale: Administration

17.3.426 Incorrect Xml Escaping In Jspx Document

Description: When creating a JSPX document with a content type of "text/html" the parser incorrectly escapes the template characters, whereas if it is changed to "text/xml" it works as expected.

Severity: Minor Warning

Rationale: Administration

17.3.427 Incorrect Xml Escaping In Jspx Document (Upgrade)

Description: When creating a JSPX document with a content type of "text/html," the parser incorrectly escapes the template characters. If it is changed to "text/xml," the parser processes the file correctly.This problem, described in Oracle Bug 8099960, has been fixed in Oracle WebLogic Server 9.2 Maintenance Pack 1.

Severity: Minor Warning

Rationale: Administration

17.3.428 Incorrect Help Page For Jta -> Monitoring -> Migration Tab

Description: Incorrect help page is showing up for JTA -> monitoring -> Migration tab. A page of "The WebLogic Server Administrative Console" is shown instead of help page for Migration tab of JTA Monitoring.

Severity: Minor Warning

Rationale: Administration

17.3.429 Incorrect Scope For Getdebugsaf*

Description: The debugging scope values for SAF debug APIs are incorrectly defined in Oracle WebLogic Server 9.0. Consequently setting the corresponding DebugSAF* flags on the Administration Console does not produce the desired result.Workaround or Solution:In Oracle WebLogic Server 9.1 and later, the debugging scope values for SAF debug APIs are correct and the flags work as expected.

Severity: Minor Warning

Rationale: Administration

17.3.430 Increased Garbage Collection Time In Oracle Jrockit R27.1.X And R27.2.X

Description: In rare cases, external compaction can cause very long pause times when attempting to move a large object from the highest heap parts, if the heap is fragmented.

Severity: Warning

Rationale: Performance

17.3.431 Initial Complete Route Header Is Fetched Before Oracle Weblogic Sip Server Reduces It

Description: Certain applications require the ability to retrieve the complete Route Header of a SIP request before Oracle WebLogic Server SIP Server reduces it. JSR 116 does not define a way of retrieving it; however, this is addressed in JSR 289.Oracle WebLogic Server SIP Server versions (2.2, 3.0, and 3.1) support JSR 116 and subsequent releases JSR 289.Use case:As described in JSR 116, the Oracle WebLogic Server SIP Server reduces the Route Header before sending the message to the deployed SIP servlet application.Some applications will not work with the reduced header. Oracle Bug 8132205 fixes this limitation of JSR 116. A patch is available for Oracle WebLogic Server SIP Server 3.0.

Severity: Minor Warning

Rationale: Development

17.3.432 Inner Java Class As A Param/Return Type In A Webmethod Causes The Web Service Not To Deploy

Description: An inner Java class as a parameter/return type in a Web method causes the Webservice not to deploy.

Severity: Minor Warning

Rationale: Not Complying with Specifications

17.4 Rules For Potential WLS V10 Problems Which May Result In System Outages Or Downtime (Deprecated)

The compliance rules for the Rules For Potential Wls V10 Problems Which May Result In System Outages Or Downtime standard follow.

17.4.1 Administration Console Hangs During Restart Of A Remote Managed Server

Description: Cannot display the JNDI tree on the Oracle WebLogic Server console on a managed server. It seems that the problem is caused by an empty <jndi-name> tag, which was accidentally added in the datasource configuration file.<jdbc-data-source-params> <jndi-name>dsGestionRepresentations</jndi-name> <jndi-name></jndi-name><global-transactions-protocol>TwoPhaseCommit</global-transactions-protocol></jdbc-data-source-params>Will see a StackOverflowError in the logs as a symptom of this problem.

Severity: Critical

Rationale: Server Outage

17.4.2 An Org.Hibernate.Lazyinitializationexception Occurs For Calls Over Iiop (Wls V10.0)

Description: When using the -Dweblogic.iiop.useJavaSerialization flag in a call over IIOP, an org.hibernate.LazyInitializationException can occur.

Severity: Critical

Rationale: Server Outage

17.4.3 Annotation Does Not Work With Unchecked Exceptions

Description: For Oracle WebLogic Server 10.0 with EJB3.0, an ApplicationException occurs. Annotation does not work with unchecked exceptions.

Severity: Critical

Rationale: Server Outage

17.4.4 Bea07-175.00 - Ssl Clients May Miss Possible Cipher Suites Resulting In Use Of Null Cipher (Wls V10)

Description: In some circumstances, SSL clients that run outside the server environment may not find all possible ciphers with which to construct the list of potential SSL cipher suites resulting in use of the default null cipher (no encryption).This advisory corrects this issue by supplying jars and instructions to ensure all cipher suites are found.

Severity: Critical

Rationale: Server Outage

17.4.5 Bea07-176.00 - Server May Select Null Cipher Suite For Ssl Communication With Ssl Clients (Wls V10.0.0)

Description: An attacker could obtain and exploit information that is not encrypted when a null cipher suite is in use. Under certain circumstances, when a client does not offer support for any of the cipher suites available in the server, then the server may select a cipher suite that uses a null cipher; this may result in SSL communication that is not encrypted.This advisory corrects this issue by logging a message when null cipher is in use and also provides administrators the ability to disable the use of null ciphers during SSL communications with SSL clients.

Severity: Critical

Rationale: Server Outage

17.4.6 Bea07-177.00 - Multiple Security Vulnerabilities In The Java Runtime Environment

Description: Contact Oracle Support or visit support.oracle.com for the following information:- A JavaDoc defect may lead to the generation of HTML documentation pages with potential cross-site scripting (XSS) vulnerability.- A buffer overflow vulnerability in the JRE image parsing code may allow an untrusted applet or application to elevate its privileges.- A vulnerability in the JRE font parsing code may allow an untrusted applet to elevate its privileges.- The Java XML Digital Signature

implementation in JDK and JRE 6 does not securely process XSLT stylesheets in XSLT Transforms in XML Signatures.- A JRE Applet Class Loader security vulnerability may allow an untrusted applet that is loaded from a remote system to circumvent network access.

Severity: Critical

Rationale: Administration

17.4.7 Bea07-178.00 - Java Secure Socket Extension Does Not Correctly Process Ssl/Tls Handshake

Description: The Java Secure Socket Extension (JSSE) that is included in various releases of the Java Runtime Environment does not correctly process SSL/TLS handshake requests. This vulnerability may be exploited to create a Denial of Service (DoS) condition to the system as a whole on a server that listens for SSL/TLS connections using JSSE for SSL/TLS support. For more information, please contact Oracle Support or visit support.oracle.com.This advisory corrects this issue by supplying patched versions of JRockit.

Severity: Critical

Rationale: Administration

17.4.8 Bea08-191.00 - Tampering Html Request Headers Could Lead To An Elevation Of Privileges (Wls V10.0)

Description: An attacker can spoof certain information in a request header that can lead to possibly getting access to application servlets that rely on this information for authentication.This advisory corrects this issue by ensuring that the header information is properly handled before passing it to the servlet.

Severity: Critical

Rationale: Administration

17.4.9 Bea08-193.00 - Non-Authorized User May Be Able To Receive Messages From A Secured Jms (Wls V10)

Description: WebLogic security policies can be configured to restrict the access to a JMS destination. If an application user does not have the "receive" permission to a JMS destination (queue/topic), an attempt to receive messages from that destination by the application should fail with security errors. By exploiting this vulnerability, an unauthorized user may be able to receive messages from a standalone (physical) JMS Topic destination or a member of a secured Distributed Topic member destination.This advisory resolves this issue by checking permissions before allowing a subscriber to use a durable subscription.

Severity: Critical

Rationale: Administration

17.4.10 Bea08-194.00 - A Non-Authorized User May Be Able To Send Messages To A Protected Queue (Wls V10)

Description: The distributed queue feature in Oracle WebLogic Server JMS provides higher availability in a clustered environment. If a JMS client sends a message to a distributed queue and encounters a problem with one member of that distributed

queue (the member is down, the member exceeds its quota, access denied, etc), internally the JMS subsystem will retry another member of the same distributed destination. In certain configurations, an unauthorized user is able to send messages to a secure distributed queue.This advisory corrects the problem and ensures that the correct user identity is maintained.

Severity: Critical

Rationale: Administration

17.4.11 Bea08-195.00 - Cross-Site Scripting Vulnerability In Console'S Unexpected Exception Page (Wls V10)

Description: Cross-Site Scripting (XSS) vulnerabilityFor more information, see:http://download.oracle.com/docs/cd/E13222_01/wls/docs81/servlet/progtasks.html#160803Background: Cross-Site Scripting (XSS) vulnerabilities are well documented in the industry. An XSS vulnerability requires three parties:Installers, updates, patches and more information are available at support.oracle.com.

Severity: Critical

Rationale: Administration

17.4.12 Bea08-196.00 - A Session Fixation Exploit Could Result In Elevated Privileges. (Wls V10.0)

Description: In order to exploit this vulnerability, an attacker must have access to the server's console login page and have a non-administrator user account on that server. A session fixation vulnerability exists which can result in elevation of the attacker's privileges. For more information about Session Fixation attacks, see:http://en.wikipedia.org/wiki/Session_fixationThis advisory corrects this issue by always regenerating an auth cookie on login.

Severity: Critical

Rationale: Administration

17.4.13 Bea08-197.00 - Account Lockout Can Be Bypassed, Exposing The Account To Brute-Force Attack

Description: In order to avoid brute-force credential attacks, Oracle WebLogic Server has a mechanism that locks the corresponding user account after a certain number of invalid login attempts. By default, the account is locked after 5 invalid login attempts and remains locked for 30 minutes.Even after a user has been locked out, logon requests to certain carefully constructed URLs can still give hints as to whether the password is correct or not. This allows a sophisticated attacker to successfully run a brute-force password attack, a dictionary attack, or other similar attacks.The patch associated with this advisory corrects the problem. All sites that use servlets are vulnerable to this problem.

Severity: Critical

Rationale: Administration

17.4.14 Bea08-199.00 - A Carefully Constructed Url May Cause Sun, Iis, Or Apache Webserver To Crash. (Wls V10)

Description: An attacker can use a carefully constructed URL to cause BEA's proxy plugin to crash the Sun, IIS or Apache web server process. On re-start, this may cause in-flight requests to be lost. This can cause a temporary denial of service. This attack can be exploited remotely, and the attacker does not need any authentication.This advisory resolves the issue in the plugin by correctly handling URLs.

Severity: Critical

Rationale: Administration

17.4.15 Bea08-201.00 - Multiple Security Vulnerabilities In The Java Runtime Environment

Description: This is a combined security advisory. These vulnerabilities are fixed in JRockit R27.5.0. Installers, updates, patches and more information are available at support.oracle.com.

Severity: Critical

Rationale: Administration

17.4.16 Bea08-80.04 - Patches Available To Prevent Multiple Cross-Site Scripting Vulnerabilities. (Wls V10)

Description: Cross-Site Scripting (XSS) vulnerabilityFor more information, see:http://download.oracle.com/docs/cd/E13222_01/wls/docs81/servlet/progtasks.html#160803Caution About Existing Samples:Our samples are intended to provide a simple tutorial regarding a few specific features. They are not comprehensive guides to best practices. Many of them omit the use of the Utils.encodeXSS() method or other XSS preventative techniques in needed places and are hence vulnerable to XSS attacks.

Severity: Critical

Rationale: Administration

17.4.17 Cve-2008-1006 - Multiple Security Vulnerabilities In Jrockit

Description: Advisory CVE-2009-1006 refers to all the vulnerability fixes that have been made in JRockit for addressing the applicable issues. The applicable advisories include:CVE 2008-5347CVE 2008-5348CVE 2008-5349CVE 2008-5350CVE 2008-5351CVE 2008-5352CVE 2008-5353CVE 2008-5354CVE 2008-5356CVE 2008-5360xFor more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.4.18 Cve-2008-2578 - Information Disclosure Vulnerability In The Weblogic Console Or Server Log

Description: Information Disclosure vulnerability in the WebLogic console or server log.

Severity: Critical

Rationale: Administration

17.4.19 Cve-2008-2579 - Information Disclosure Vulnerability In Weblogic Plug-Ins For Web Servers (Wls V10)

Description: Information disclosure vulnerability in WebLogic Server plug-ins for Apache, Sun, and IIS Web servers.

Severity: Critical

Rationale: Administration

17.4.20 Cve-2008-2580 - Information Disclosure In Jsp Pages (Wls V10.0)

Description: Information disclosure in JSP pages.

Severity: Critical

Rationale: Administration

17.4.21 Cve-2008-2581 - Elevation Of Privilege Vulnerabilities In The Uddi Explorer (Wls V10)

Description: Elevation of privilege vulnerabilities in the UDDI Explorer.

Severity: Critical

Rationale: Administration

17.4.22 Cve-2008-2582 - Denial-Of-Service Vulnerability In Weblogic Server

Description: Denial-of-Service vulnerability in WebLogic Server.

Severity: Critical

Rationale: Server Outage

17.4.23 Cve-2008-3103 - Security Vulnerability In Java Management Extensions (Jmx)

Description: A vulnerability in the Java Management Extensions (JMX) management agent included in the Java Runtime Environment (JRE) may allow a JMX client running on a remote host to perform unauthorized operations on a system running JMX with local monitoring enabled.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.4.24 Cve-2008-3104 - Security Vulnerabilities In Java Runtime Environment Allows Same Origin

Description: Security vulnerabilities in the Java Runtime Environment may allow an untrusted applet that is loaded from a remote system to circumvent network access restrictions and establish socket connections to certain services running on machines other than the one that the applet was downloaded from. This may allow the untrusted remote applet the ability to exploit any security vulnerabilities existing in

the services it has connected to.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.4.25 Cve-2008-3105 - Security Vulnerability In The Java Runtime Environment Related Xml Data

Description: A vulnerability in the Java Runtime Environment related to the processing of XML data may allow unauthorized access to certain URL resources (such as some files and web pages) or a Denial of Service (DoS) condition to be created on the system running the JRE.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.4.26 Cve-2008-3106 - Security Vulnerability In The Java Runtime Environment Related To Xlm Data

Description: A vulnerability in the Java Runtime Environment with processing XML data may allow an untrusted applet or application that is downloaded from a website unauthorized access to certain URL resources (such as some files and web pages).For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.4.27 Cve-2008-3108 - A Security Vulnerability With The Processing Of Fonts In The Java Runtime

Description: A buffer overflow security vulnerability with the processing of fonts in the Java Runtime Environment (JRE) may allow an untrusted applet or application to elevate its privileges. For example, an untrusted applet may grant itself permissions to read and write local files or execute local applications that are accessible to the user running the untrusted applet.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.4.28 Cve-2008-3109 - Security Vulnerability In The Java Runtime Environment Scripting Language

Description: A vulnerability in the Java Runtime Environment relating to scripting language support may allow an untrusted applet or application to elevate its privileges. For example, an untrusted applet may grant itself permissions to read and write local files or execute local applications that are accessible to the user running the untrusted applet.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.4.29 Cve-2008-3110 - Security Vulnerability In The Java Runtime Environment Scripting Language

Description: A vulnerability in the Java Runtime Environment relating to scripting language support may allow an untrusted applet to access information from another applet.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.4.30 Cve-2008-3257 - Security Vulnerability In Weblogic Plug-In For Apache (Wls V10)

Description: Recently, an exploit has been made public which may impact the availability, confidentiality, or integrity of WebLogic Server applications that use the Apache web server configured with the WebLogic plug-in for Apache. This vulnerability may be remotely exploitable without authentication (that is, it may be exploited over a network without the need for a username and password).

Severity: Critical

Rationale: Server Outage

17.4.31 Cve-2008-4008 - Security Vulnerability In Weblogic Plug-In For Apache

Description: This vulnerability may impact the availability, confidentiality, or integrity of WebLogic Server applications which use the Apache web server configured with the WebLogic plug-in for Apache. This vulnerability may be remotely exploitable without authentication, that is, it may be exploited over a network without the need for a username and password.

Severity: Critical

Rationale: Administration

17.4.32 Cve-2008-4010 - Elevation Of Privilege Vulnerability In Some Netui Tags (Wls V10)

Description: This vulnerability in some NetUI tags may allow an attacker to read unauthorized data. This may be exploited over a network.

Severity: Critical

Rationale: Administration

17.4.33 Cve-2008-4011 - Elevation Of Privileges For Some Applications (Wls V10.0)

Description: Under certain conditions, some applications in admin state may be made available to non admin users.

Severity: Critical

Rationale: Administration

17.4.34 Cve-2008-4013 - Protected Web Apps May Be Displayed Under Certain Conditions. (Wls V10)

Description: If you upgrade from Oracle WebLogic Server 8.1SP3 to a higher version and use auth-method as CLIENT-CERT, some web apps which were protected in Oracle WebLogic Server 8.1SP3 may be made available to an invalid user.

Severity: Critical

Rationale: Administration

17.4.35 Cve-2008-5457 - Security Vulnerability In Wls Plug-Ins For Apache, Sun, And Iis Web Server (Wls V10)

Description: This vulnerability may impact the availability, confidentiality or integrity of WebLogic Server applications, which use the Apache, Sun, or IIS web server configured with the WebLogic plug-in for Apache, Sun, or IIS, respectively. This vulnerability may be remotely exploitable without authentication, that is, it may be exploited over a network without the need for a username and password.

Severity: Critical

Rationale: Administration

17.4.36 Cve-2008-5460 - Information Disclosure Vulnerability In Jsp And Servlets (Wls V10)

Description: Certain circumstances may cause some information disclosure in WebLogic Server JSPs and servlets.

Severity: Critical

Rationale: Subsystem Outage

17.4.37 Cve-2008-5461 - Elevation Of Privilege Vulnerability In Oracle Weblogic Console

Description: This vulnerability in Oracle WebLogic Console may allow information disclosure and elevation of privileges. This may be exploited over a network.

Severity: Critical

Rationale: Subsystem Outage

17.4.38 Cve-2008-5462 - Elevation Of Privilege Vulnerability In Weblogic Portal (Wls V10)

Description: This vulnerability in WebLogic Portal may allow elevation of privileges. This may be exploited over a network.

Severity: Critical

Rationale: Administration

17.4.39 Cve-2009-0217 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle JRockit R27.6.3 JRE/JDK 1.6.0_11. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.4.40 Cve-2009-0217 - Critical Patch Update Notice (Wls V10.0)

Description: Oracle has released Critical Patch Updates for July 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 10.0. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Server Outage

17.4.41 Cve-2009-1002 - Elevation Of Privilege Vulnerability In Weblogic Server (Wls V10)

Description: This vulnerability in WebLogic Server may allow elevation of privileges. This may be exploited over a network.

Severity: Critical

Rationale: Administration

17.4.42 Cve-2009-1003 - Source Code Access Vulnerability In Web Pages, Weblogic Server (Wls V10)

Description: This vulnerability in WebLogic Server may allow access to source code of web pages. This may be exploited over a network.

Severity: Critical

Rationale: Administration

17.4.43 Cve-2009-1012 - Security Vulnerability In Weblogic Plug-In For Apache Web Server

Description: This vulnerability may impact the availability, confidentiality, or integrity of WebLogic Server applications, which use the Apache, Sun, or IIS web server configured with the WebLogic plug-in for Apache, Sun, or IIS servers, respectively. This vulnerability may be remotely exploitable without authentication. That is. it may be exploited over a network without the need for a username and password.

Severity: Critical

Rationale: Administration

17.4.44 Cve-2009-1016 - Security Vulnerability In Oracle Weblogic Server Plug-Ins For Apache, Sun, And Iis Servers

Description: This vulnerability may impact the availability, confidentiality, or integrity of Oracle WebLogic Server applications, which use the Apache, Sun, or IIS web server configured with the WebLogic Server plug-ins for Apache, Sun, or IIS servers, respectively.

Severity: Critical

Rationale: Administration

17.4.45 Cve-2009-1094 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for July 2009 that provide corrective action for potential security vulnerabilities for Oracle JRockit R27.6.3 and earlier JRE and JDK 6, R27.6.3 and earlier JRE and JDK 5.0, R27.6.3 and earlier SDK and JRE 1.4.2. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.4.46 Cve-2009-1974 - Critical Patch Update Notice (Wls V10.0)

Description: Oracle has released Critical Patch Updates for July 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 10.0. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Server Outage

17.4.47 Cve-2009-2002 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Portal 10.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.4.48 Cve-2009-2625 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle JRockit 1.5.0_19 and 1.6.0_14.Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.4.49 Cve-2009-3396 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.0, 9.1, and 9.2. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Server Outage

17.4.50 Cve-2009-3396 - Critical Patch Update Notice (Wls V10.0)

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 10.0. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Server Outage

17.4.51 Cve-2009-3403 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle JRockit 1.6.0_14, 1.5.0_19 and 1.4.2_21. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.4.52 Cve-2009-3555 - Critical Patch Update Notice (Wls V10.0)

Description: Oracle has released a Critical Patch Update that provides corrective action for a potential security vulnerability for Oracle WebLogic Server 10.0. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Development

17.4.53 Cve-2010-0068 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.4.54 Cve-2010-0068 - Critical Patch Update Notice (Wls V10.0)

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 10.0. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Development

17.4.55 Cve-2010-0069 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.4.56 Cve-2010-0069 - Critical Patch Update Notice (Wls V10.0)

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 10.0. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Development

17.4.57 Cve-2010-0073 - Critical Patch Update Notice (Wls V10.0)

Description: Oracle has released a Critical Patch Update that provides corrective action for a potential security vulnerability for Oracle WebLogic Server 10.0. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Development

17.4.58 Cve-2010-0074 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.4.59 Cve-2010-0074 - Critical Patch Update Notice (Wls V10.0)

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 10.0. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Development

17.4.60 Cve-2010-0078 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.4.61 Cve-2010-0078 - Critical Patch Update Notice (Wls V10.0)

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 10.0. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Development

17.4.62 Cve-2010-0079 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle JRockit 1.6.0_14, 1.5.0_19 and 1.4.2_21. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.4.63 Cve-2010-0849 - Critical Patch Update Notice

Description: Oracle has released a Critical Patch Update that provides corrective action for a potential security vulnerability for Oracle JRockit R27.6.6: JRE/JDK 1.4.2, 5 and 6; R28.0.0, JRE/JDK 5 and 6. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.4.64 Cve-2010-2375 - Critical Patch Update Notice (Wls V10.0)

Description: Oracle has released a Critical Patch Update that provides corrective action for a potential security vulnerability for Oracle WebLogic Server 10.0. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Development

17.4.65 Crashes In Conjunction With A Native Library

Description: If you are using Oracle JRockit in conjunction with a native library that relies on OS signals you may experience crashes due to a signal handling conflict between Oracle JRockit and the native library.Dump stack matches known issue:Thread Stack Trace: at pthread_kill+62()@0xb75c00ee at ptSendSignal +34()@0xb71aedc6 at trapiConvertToDeferredSigsegv+199()@0xb719d207 at trapiSigSegvHandler+40()@0xb719d23c at xehInterpretSavedSigaction +219(amqxerrx.c)@0xb72f276b at xehExceptionHandler+543()@0xb72f2b3f at __libc_sigaction+272()@0xb75c2f80Oracle Engineering found this conflict using IBM's MQSeries native drivers, and it may be present in other libraries that rely on native code.

Severity: Critical

Rationale: Server Outage

17.4.66 Deadlock In Weblogic.Jms.Client.Wlconnectionimpl.Processreconnecttimer

Description: When using Oracle WebLogic Server 10.0 and JMS operations, a deadlock occurs when trying to reconnect with an Oracle WebLogic Server 8.1 SP5 server that has gone down.Found one Java-level deadlock:'weblogic.timers.TimerThread': waiting to lock monitor 0x00000001012cdbe0 (object 0xffffffff23111248, a java.lang.Object), which is held by '[ACTIVE] ExecuteThread: '36' for queue: 'weblogic.kernel.Default (self-tuning)'"[ACTIVE] ExecuteThread: '36' for queue: 'weblogic.kernel.Default (self-tuning)": waiting to lock monitor 0x00000001002d26f8 (object 0xffffffff13ca1368, a weblogic.timers.internal.TimerThread), which is held by 'weblogic.timers.TimerThread'

Severity: Critical

Rationale: Subsystem Outage

17.4.67 Deadlock Occurs In Oracle Weblogic Server (Wls V10.0)

Description: Java level deadlock between weblogic.deployment.jms.JMSSessionPoolTester and

weblogic.deployment.jms.JMSSessionPool reveal in Oracle WebLogic Server Thread dump.

Severity: Critical

Rationale: Server Outage

17.4.68 Http Post Method Can Be Tuned Via Maxpostsize To Harden Security

Description: A denial-of-service attack is a malicious attempt to overload a server by sending more requests than it can handle, preventing access to a service. Attackers may overload the server by sending huge amounts of data in an HTTP POST method. The client can get an HTTP error code 413 (Request Entity Too Large) or the connection may be broken.Prevent this type of attack by setting the MaxPostSize parameter. This limits the number of bytes of data that can be received in a POST from a single request. (By default, the value for MaxPostSize is -1, i.e. unlimited.) If an attacker sends an HTTP POST that exceeds the limit you specify, it triggers a MaxPostSizeExceeded exception and the server logs a "POST size exceeded the parameter MaxPostSize" message.

Severity: Critical

Rationale: Server Outage

17.4.69 Hibernate And Ehcache Cache Locking Problem With Multiple Managed Servers On Same Server

Description: When Hibernate and ehcache are used with Oracle WebLogic Server, the ehcache component writes cached objects to the file system defined by the property java.io.tmpDir. This, in itself, is not an issue. However, when there are two or more managed servers running on each physical server, these managed servers write to the same directory in the file system using the same file names. Consequently, the servers are sharing resources that require explicit locks in order to modify the files, which can result in a deadlock condition.

Severity: Critical

Rationale: Administration

17.4.70 If Weblogic_Patch.Jar Is After Weblogic.Jar The Installed Patches Have No Effect

Description: Some customers write their own startup and environment scripts. Sometimes they invert the CLASSPATH order. When this occurs, patches applied with BSU are not active even if Oracle Enterprise Manager detects them. The weblogic_patch.jar must always come before weblogic_sp.jar and weblogic.jar in the classpath.

Severity: Critical

Rationale: Administration

17.4.71 Jms Server Byteshighcount Is Greater Than 50 Percent Of Jvm Heapsizecurrent

Description: When the JMS Server's BytesHighCount attribute is greater than 50 percent of the JVM's HeapSizeCurrent, and the BytesPagingEnabled and MessagesPagingEnabled attributes are not set, a JMS processing error may have occured or may occur in the future.

Severity: Critical

Rationale: Server Outage

17.4.72 Noncompliant Interface And Implementation Classes Cause Oracle Jrockit To Crash

Description: When an interface is not compliant with the implementation classes, Oracle JRockit may crash or throw a NullPointerException. This occurs because Oracle JRockit does not perform verification of implemented interfaces before a call, unless it is started with the option -Xverify:all.Oracle JRockit R24.5.0 and previous versions crash under these conditions. Oracle JRockit R25.2.1-11 and later throw a NullPointerException where an IncompatibleClassChangeError could be expected.

Severity: Critical

Rationale: Server Outage

17.4.73 Oracle Jrockit 1.4.2_12 Crash At Mmgetobjectsize()

Description: Oracle JRockit 1.4.2_12 crashed on multiple WLS 8 SP4 servers.Oracle JRockit dump shows the following stack trace:Stack 0: start=0xb7a58000, end=0xb7a9c000, guards=0xb7a5d000 (ok),forbidden=0xb7a5b000Thread Stack Trace: at mmGetObjectSize+8()@0xb7e6b3c8 at findNext+166()@0xb7e9a006 at refIterGetNext +44()@0xb7e9a24c at trMarkRootsForThread+325()@0xb7ea83b5 at mmMarkRootsForThread+44()@0xb7e2cc2c at mmParThreadInspection +45()@0xb7e7794d at tsDoGCInspectionForAllThreads+37()@0xb7ed8555 at mmParMark+118()@0xb7e77d16 at mmGCMainLoop+1074()@0xb7d73722 at tsiCallStartFunction+81()@0xb7e1ac81 at tsiThreadStub+126()@0xb7e1bd1e at ptiThreadStub+18()@0xb7e840d2 at start_thread+129()@0x9e6371 at clone +94()@0x88e9be - Java stack -

Severity: Critical

Rationale: Server Outage

17.4.74 Oracle Jrockit R27.3.1 Crashes When Calling Inflate On A Closed Inflator

Description: Sometimes, calling inflate on a closed Inflater results in Oracle JRockit crashing, creating a core file. It can occur with Oracle JRockit R27.3.1.The relevant stack trace will be similar to the following:Thread Stack Trace: at inflate +73()@0x000000001027C409 at RJNI_java_util_zip_Inflater_inflateFast +90()@0x000000001020162A - Java stack - at java/util/zip/ Inflater.inflateFast(JJIJI)I(Native Method) at java/util/zip/ Inflater.inflateBytes(Inflater.java:354) at java/util/zip/Inflater.inflate(Inflater.java:216)

Severity: Critical

Rationale: Administration

17.4.75 Saf Agent Discarding Messages

Description: SAF is discarding messages causing message loss.

Severity: Critical

Rationale: Administration

17.4.76 Ssl Incompatibility When Upgrading To Jdk Version 1.6.0_14 And 1.5.0_19

Description: Upgrading to the versions 1.6.0_14 and 1.5.0_19 of the Sun JDK or Oracle JRockit causes compatibility issues between Sun JDK and Oracle JRockit handling of SSL and Oracle WebLogic Server handling of SSL.

Severity: Critical

Rationale: Non-User Viewable Errors

17.4.77 Ssl Incompatibility When Upgrading To Jdk Version 1.6.0_14 And 1.5.0_19 (Wls V10.0)

Description: Upgrading to the versions 1.6.0_14 and 1.5.0_19 of the Sun JDK or Oracle JRockit causes compatibility issues between Sun JDK and Oracle JRockit handling of SSL and Oracle WebLogic Server handling of SSL.

Severity: Critical

Rationale: Non-User Viewable Errors

17.4.78 Sessions Get Lost After Configuring Saml With Two Domains

Description: Sessions are lost after configuring SAML with two domains (Oracle WebLogic Server 10.0) running on one system.It is a SAML requirement to set all Web application cookie names to the default (JSESSIONID). With this setting, the client browser can differentiate cookies originating from different domains only if the IPAddress or hostname of the SAML source and destination domain are not the same.

Severity: Critical

Rationale: User Viewable Errors

17.4.79 Solaris Os Has Problems With Default Threading Libraries

Description: When starting Oracle WebLogic Server on Solaris 8 or 5.8, the default threading libraries of the operating system may cause various JVM threading issues, which can ultimately result in the server hanging or crashing.

Severity: Critical

Rationale: Server Outage

17.4.80 Using Administration Console To Export/Import Large Jms Message Queue Causes Out Of Memory Error. (Wls V10)

Description: A system OutofMemory error can occur if you use Oracle WebLogic Server Administration Console to export or import a large JMS queue.

Severity: Critical

Rationale: Server Outage

17.4.81 Using The Post-Bind Option With Jrockit On Linux Causes Server Core Dump

Description: Attempting to start a server on a Linux platform when setting the post-bind option in a UNIX machine can cause the server to core dump with a StackOverflow exception.This applies to Oracle JRockit R26.2 and above.

Severity: Critical

Rationale: Administration

17.4.82 Windows 2000 Sp2 And Higher Required For Oracle Jrockit 1.5_02 And 1.5_03

Description: Oracle JRockit 1.5_02 (R25.0.0) and Oracle JRockit 1.5_03 (R25.2.0) running on Windows 2000 requires Service Pack 2 or higher. This signature indicates that you are running no service pack or one less than Service Pack 2. Upgrade to Windows 2000 SP 2 or higher.

Severity: Critical

Rationale: Not Complying with Specifications

17.4.83 Windows 2000 Sp4 And Higher Required For Oracle Jrockit 1.5_04 (R26.0.0) Through 1.5_06

Description: Windows 2000 SP4 and higher required for Oracle JRockit 1.5_04 through Oracle JRockit 1.5_06.

Severity: Critical

Rationale: Not Complying with Specifications

17.4.84 With Oracle Jrockit R27.3.0, Ctrl-C Can Cause Improper Shutdown And Loss Of Data

Description: If you are running on Linux or Solaris and press Ctrl-C to properly shut down your application, it will actually terminate immediately and you risk losing any runtime data that hasn't been saved to disk or a database. This happens because Oracle JRockit fails to register the SIGINT signal handler used for the shut down hooks.This issue does not apply to applications running on Windows.

Severity: Critical

Rationale: Administration

17.5 Rules For Potential WLS V11 Problems Which May Result In System Outages Or Downtime (Deprecated)

The compliance rules for the Rules For Potential Wls V11 Problems Which May Result In System Outages Or Downtime standard follow.

17.5.1 Administration Console Hangs During Restart Of A Remote Managed Server

Description: Cannot display the JNDI tree on the Oracle WebLogic Server console on a managed server. It seems that the problem is caused by an empty <jndi-name> tag, which was accidentally added in the datasource configuration file.<jdbc-data-source-params> <jndi-name>dsGestionRepresentations</jndi-name> <jndi-name></jndi-name><global-transactions-protocol>TwoPhaseCommit</global-transactions-protocol></jdbc-data-source-params>Will see a StackOverflowError in the logs as a symptom of this problem.

Severity: Critical

Rationale: Server Outage

17.5.2 Annotation Does Not Work With Unchecked Exceptions

Description: For Oracle WebLogic Server 10.3 with EJB3.0, an ApplicationException occurs. Annotation does not work with unchecked exceptions.

Severity: Critical

Rationale: Server Outage

17.5.3 Bea07-177.00 - Multiple Security Vulnerabilities In The Java Runtime Environment

Description: Contact Oracle Support or visit support.oracle.com for the following information:- A JavaDoc defect may lead to the generation of HTML documentation pages with potential cross-site scripting (XSS) vulnerability.- A buffer overflow vulnerability in the JRE image parsing code may allow an untrusted applet or application to elevate its privileges.- A vulnerability in the JRE font parsing code may allow an untrusted applet to elevate its privileges.- The Java XML Digital Signature implementation in JDK and JRE 6 does not securely process XSLT stylesheets in XSLT Transforms in XML Signatures.- A JRE Applet Class Loader security vulnerability may allow an untrusted applet that is loaded from a remote system to circumvent network access.

Severity: Critical

Rationale: Administration

17.5.4 Bea07-178.00 - Java Secure Socket Extension Does Not Correctly Process Ssl/Tls Handshake

Description: The Java Secure Socket Extension (JSSE) that is included in various releases of the Java Runtime Environment does not correctly process SSL/TLS handshake requests. This vulnerability may be exploited to create a Denial of Service (DoS) condition to the system as a whole on a server that listens for SSL/TLS connections using JSSE for SSL/TLS support. For more information, please contact Oracle Support or visit support.oracle.com.This advisory corrects this issue by supplying patched versions of JRockit.

Severity: Critical

Rationale: Administration

17.5.5 Bea08-201.00 - Multiple Security Vulnerabilities In The Java Runtime Environment

Description: This is a combined security advisory. These vulnerabilities are fixed in JRockit R27.5.0. Installers, updates, patches and more information are available at support.oracle.com.

Severity: Critical

Rationale: Administration

17.5.6 Cve-2008-1006 - Multiple Security Vulnerabilities In Jrockit

Description: Advisory CVE-2009-1006 refers to all the vulnerability fixes that have been made in JRockit for addressing the applicable issues. The applicable advisories include:CVE 2008-5347CVE 2008-5348CVE 2008-5349CVE 2008-5350CVE

2008-5351CVE 2008-5352CVE 2008-5353CVE 2008-5354CVE 2008-5356CVE 2008-5360xFor more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.5.7 Cve-2008-3103 - Security Vulnerability In Java Management Extensions (Jmx)

Description: A vulnerability in the Java Management Extensions (JMX) management agent included in the Java Runtime Environment (JRE) may allow a JMX client running on a remote host to perform unauthorized operations on a system running JMX with local monitoring enabled.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.5.8 Cve-2008-3104 - Security Vulnerabilities In Java Runtime Environment Allows Same Origin

Description: Security vulnerabilities in the Java Runtime Environment may allow an untrusted applet that is loaded from a remote system to circumvent network access restrictions and establish socket connections to certain services running on machines other than the one that the applet was downloaded from. This may allow the untrusted remote applet the ability to exploit any security vulnerabilities existing in the services it has connected to.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.5.9 Cve-2008-3105 - Security Vulnerability In The Java Runtime Environment Related Xml Data

Description: A vulnerability in the Java Runtime Environment related to the processing of XML data may allow unauthorized access to certain URL resources (such as some files and web pages) or a Denial of Service (DoS) condition to be created on the system running the JRE.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.5.10 Cve-2008-3106 - Security Vulnerability In The Java Runtime Environment Related To Xlm Data

Description: A vulnerability in the Java Runtime Environment with processing XML data may allow an untrusted applet or application that is downloaded from a website unauthorized access to certain URL resources (such as some files and web pages).For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.5.11 Cve-2008-3108 - A Security Vulnerability With The Processing Of Fonts In The Java Runtime

Description: A buffer overflow security vulnerability with the processing of fonts in the Java Runtime Environment (JRE) may allow an untrusted applet or application to elevate its privileges. For example, an untrusted applet may grant itself permissions to read and write local files or execute local applications that are accessible to the user running the untrusted applet.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.5.12 Cve-2008-3109 - Security Vulnerability In The Java Runtime Environment Scripting Language

Description: A vulnerability in the Java Runtime Environment relating to scripting language support may allow an untrusted applet or application to elevate its privileges. For example, an untrusted applet may grant itself permissions to read and write local files or execute local applications that are accessible to the user running the untrusted applet.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.5.13 Cve-2008-3110 - Security Vulnerability In The Java Runtime Environment Scripting Language

Description: A vulnerability in the Java Runtime Environment relating to scripting language support may allow an untrusted applet to access information from another applet.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.5.14 Cve-2008-4008 - Security Vulnerability In Weblogic Plug-In For Apache

Description: This vulnerability may impact the availability, confidentiality, or integrity of WebLogic Server applications which use the Apache web server configured with the WebLogic plug-in for Apache. This vulnerability may be remotely exploitable without authentication, that is, it may be exploited over a network without the need for a username and password.

Severity: Critical

Rationale: Administration

17.5.15 Cve-2008-4010 - Elevation Of Privilege Vulnerability In Some Netui Tags (Wls V10)

Description: This vulnerability in some NetUI tags may allow an attacker to read unauthorized data. This may be exploited over a network.

Severity: Critical

Rationale: Administration

17.5.16 Cve-2008-5457 - Security Vulnerability In Wls Plug-Ins For Apache, Sun, And Iis Web Server (Wls V10)

Description: This vulnerability may impact the availability, confidentiality or integrity of WebLogic Server applications, which use the Apache, Sun, or IIS web server configured with the WebLogic plug-in for Apache, Sun, or IIS, respectively. This vulnerability may be remotely exploitable without authentication, that is, it may be exploited over a network without the need for a username and password.

Severity: Critical

Rationale: Administration

17.5.17 Cve-2008-5459 - Security Policy Not Enforced For Wls Web Services

Description: Under certain circumstances security policies may not be enforced for web services.

Severity: Critical

Rationale: Administration

17.5.18 Cve-2008-5460 - Information Disclosure Vulnerability In Jsp And Servlets (Wls V10)

Description: Certain circumstances may cause some information disclosure in WebLogic Server JSPs and servlets.

Severity: Critical

Rationale: Subsystem Outage

17.5.19 Cve-2008-5461 - Elevation Of Privilege Vulnerability In Oracle Weblogic Console

Description: This vulnerability in Oracle WebLogic Console may allow information disclosure and elevation of privileges. This may be exploited over a network.

Severity: Critical

Rationale: Subsystem Outage

17.5.20 Cve-2008-5462 - Elevation Of Privilege Vulnerability In Weblogic Portal (Wls V10)

Description: This vulnerability in WebLogic Portal may allow elevation of privileges. This may be exploited over a network.

Severity: Critical

Rationale: Administration

17.5.21 Cve-2009-0217 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle JRockit R27.6.3 JRE/JDK 1.6.0_11. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.5.22 Cve-2009-0217 - Critical Patch Update Notice (Wls V10.3)

Description: Oracle has released Critical Patch Updates for July 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 10.3. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Server Outage

17.5.23 Cve-2009-1002 - Elevation Of Privilege Vulnerability In Weblogic Server (Wls V10)

Description: This vulnerability in WebLogic Server may allow elevation of privileges. This may be exploited over a network.

Severity: Critical

Rationale: Administration

17.5.24 Cve-2009-1003 - Source Code Access Vulnerability In Web Pages, Weblogic Server (Wls V10)

Description: This vulnerability in WebLogic Server may allow access to source code of web pages. This may be exploited over a network.

Severity: Critical

Rationale: Administration

17.5.25 Cve-2009-1004 - Strengthened?Weblogic Server Web Services Security

Description: WebLogic Server web services security was strengthened.

Severity: Critical

Rationale: Administration

17.5.26 Cve-2009-1012 - Security Vulnerability In Weblogic Plug-In For Apache Web Server

Description: This vulnerability may impact the availability, confidentiality, or integrity of WebLogic Server applications, which use the Apache, Sun, or IIS web server configured with the WebLogic plug-in for Apache, Sun, or IIS servers, respectively. This vulnerability may be remotely exploitable without authentication. That is. it may be exploited over a network without the need for a username and password.

Severity: Critical

Rationale: Administration

17.5.27 Cve-2009-1016 - Security Vulnerability In Oracle Weblogic Server Plug-Ins For Apache, Sun, And Iis Servers

Description: This vulnerability may impact the availability, confidentiality, or integrity of Oracle WebLogic Server applications, which use the Apache, Sun, or IIS web server configured with the WebLogic Server plug-ins for Apache, Sun, or IIS servers, respectively.

Severity: Critical

Rationale: Administration

17.5.28 Cve-2009-1094 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for July 2009 that provide corrective action for potential security vulnerabilities for Oracle JRockit R27.6.3 and earlier JRE and JDK 6, R27.6.3 and earlier JRE and JDK 5.0, R27.6.3 and earlier SDK and JRE 1.4.2. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.5.29 Cve-2009-1974 - Critical Patch Update Notice (Wls V10.3)

Description: Oracle has released Critical Patch Updates for July 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 10.3. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Server Outage

17.5.30 Cve-2009-1975 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for July 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 10.3. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Server Outage

17.5.31 Cve-2009-2002 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Portal 10.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.5.32 Cve-2009-2625 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle JRockit 1.5.0_19 and 1.6.0_14.Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.5.33 Cve-2009-3396 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.0, 9.1, and 9.2. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Server Outage

17.5.34 Cve-2009-3396 - Critical Patch Update Notice (Wls V10.3)

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 10.3. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Server Outage

17.5.35 Cve-2009-3403 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle JRockit 1.6.0_14, 1.5.0_19 and 1.4.2_21. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.5.36 Cve-2009-3555 - Critical Patch Update Notice (Wls V10.3)

Description: Oracle has released a Critical Patch Update that provides corrective action for a potential security vulnerability for Oracle WebLogic Server 10.3. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Development

17.5.37 Cve-2010-0068 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.5.38 Cve-2010-0069 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.5.39 Cve-2010-0069 - Critical Patch Update Notice (Wls V10.3)

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 10.3. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Development

17.5.40 Cve-2010-0073 - Critical Patch Update Notice (Wls V10.3)

Description: Oracle has released a Critical Patch Update that provides corrective action for a potential security vulnerability for Oracle WebLogic Server 10.3. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Development

17.5.41 Cve-2010-0074 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.5.42 Cve-2010-0074 - Critical Patch Update Notice (Wls V10.3)

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 10.3. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Development

17.5.43 Cve-2010-0078 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.5.44 Cve-2010-0078 - Critical Patch Update Notice (Wls V10.3)

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 10.3. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Development

17.5.45 Cve-2010-0079 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle JRockit 1.6.0_14, 1.5.0_19 and 1.4.2_21. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.5.46 Cve-2010-0849 - Critical Patch Update Notice

Description: Oracle has released a Critical Patch Update that provides corrective action for a potential security vulnerability for Oracle JRockit R27.6.6: JRE/JDK 1.4.2, 5 and 6; R28.0.0, JRE/JDK 5 and 6. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.5.47 Cve-2010-2375 - Critical Patch Update Notice (Wls V10.3)

Description: Oracle has released a Critical Patch Update that provides corrective action for a potential security vulnerability for Oracle WebLogic Server 10.3. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Development

17.5.48 Crashes In Conjunction With A Native Library

Description: If you are using Oracle JRockit in conjunction with a native library that relies on OS signals you may experience crashes due to a signal handling conflict between Oracle JRockit and the native library.Dump stack matches known issue:Thread Stack Trace: at pthread_kill+62()@0xb75c00ee at ptSendSignal +34()@0xb71aedc6 at trapiConvertToDeferredSigsegv+199()@0xb719d207 at trapiSigSegvHandler+40()@0xb719d23c at xehInterpretSavedSigaction +219(amqxerrx.c)@0xb72f276b at xehExceptionHandler+543()@0xb72f2b3f at __libc_sigaction+272()@0xb75c2f80Oracle Engineering found this conflict using IBM's MQSeries native drivers, and it may be present in other libraries that rely on native code.

Severity: Critical

Rationale: Server Outage

17.5.49 Deadlock Occurs In Oracle Weblogic Server (Wls V10.3)

Description: Java level deadlock between weblogic.deployment.jms.JMSSessionPoolTester and weblogic.deployment.jms.JMSSessionPool reveal in Oracle WebLogic Server Thread dump.

Severity: Critical

Rationale: Server Outage

17.5.50 Document Style Operation Must Not Have A Non-Header Inout Or Out Parameter

Description: When generating a webservice using JAX-RPC 1.1 with document style from a Web Service Definition Language (WSDL) file, the customer is getting the following error: [jwsc] [ERROR] - A document style operation must not have a non header INOUT or OUT Parameter.

Severity: Critical

Rationale: Development

17.5.51 Http Post Method Can Be Tuned Via Maxpostsize To Harden Security

Description: A denial-of-service attack is a malicious attempt to overload a server by sending more requests than it can handle, preventing access to a service. Attackers may overload the server by sending huge amounts of data in an HTTP POST method. The client can get an HTTP error code 413 (Request Entity Too Large) or the connection may be broken.Prevent this type of attack by setting the MaxPostSize parameter. This limits the number of bytes of data that can be received in a POST from a single request. (By default, the value for MaxPostSize is -1, i.e. unlimited.) If an attacker sends an HTTP POST that exceeds the limit you specify, it triggers a MaxPostSizeExceeded exception and the server logs a "POST size exceeded the parameter MaxPostSize" message.

Severity: Critical

Rationale: Server Outage

17.5.52 Hibernate And Ehcache Cache Locking Problem With Multiple Managed Servers On Same Server

Description: When Hibernate and ehcache are used with Oracle WebLogic Server, the ehcache component writes cached objects to the file system defined by the property java.io.tmpDir. This, in itself, is not an issue. However, when there are two or more managed servers running on each physical server, these managed servers write to the same directory in the file system using the same file names. Consequently, the servers are sharing resources that require explicit locks in order to modify the files, which can result in a deadlock condition.

Severity: Critical

Rationale: Administration

17.5.53 If Weblogic_Patch.Jar Is After Weblogic.Jar The Installed Patches Have No Effect

Description: Some customers write their own startup and environment scripts. Sometimes they invert the CLASSPATH order. When this occurs, patches applied with BSU are not active even if Oracle Enterprise Manager detects them. The weblogic_patch.jar must always come before weblogic_sp.jar and weblogic.jar in the classpath.

Severity: Critical

Rationale: Administration

17.5.54 Inner Classes Are Public Local Variable, Resulting In Wrong Types Definition In Wsdl

Description: When a Web Service uses inner classes as data types to a web method the resulting types are incorrect in the Web Service Definition Language (WSDL) produced by JWSC.

Severity: Critical

Rationale: Server Outage

17.5.55 Jms Server Byteshighcount Is Greater Than 50 Percent Of Jvm Heapsizecurrent

Description: When the JMS Server's BytesHighCount attribute is greater than 50 percent of the JVM's HeapSizeCurrent, and the BytesPagingEnabled and MessagesPagingEnabled attributes are not set, a JMS processing error may have occured or may occur in the future.

Severity: Critical

Rationale: Server Outage

17.5.56 Noncompliant Interface And Implementation Classes Cause Oracle Jrockit To Crash

Description: When an interface is not compliant with the implementation classes, Oracle JRockit may crash or throw a NullPointerException. This occurs because Oracle JRockit does not perform verification of implemented interfaces before a call, unless it is started with the option -Xverify:all.Oracle JRockit R24.5.0 and previous versions crash under these conditions. Oracle JRockit R25.2.1-11 and later throw a NullPointerException where an IncompatibleClassChangeError could be expected.

Severity: Critical

Rationale: Server Outage

17.5.57 Oracle Jrockit 1.4.2_12 Crash At Mmgetobjectsize()

Description: Oracle JRockit 1.4.2_12 crashed on multiple WLS 8 SP4 servers.Oracle JRockit dump shows the following stack trace:Stack 0: start=0xb7a58000, end=0xb7a9c000, guards=0xb7a5d000 (ok),forbidden=0xb7a5b000Thread Stack Trace: at mmGetObjectSize+8()@0xb7e6b3c8 at findNext+166()@0xb7e9a006 at refIterGetNext +44()@0xb7e9a24c at trMarkRootsForThread+325()@0xb7ea83b5 at mmMarkRootsForThread+44()@0xb7e2cc2c at mmParThreadInspection +45()@0xb7e7794d at tsDoGCInspectionForAllThreads+37()@0xb7ed8555 at mmParMark+118()@0xb7e77d16 at mmGCMainLoop+1074()@0xb7d73722 at tsiCallStartFunction+81()@0xb7e1ac81 at tsiThreadStub+126()@0xb7e1bd1e at ptiThreadStub+18()@0xb7e840d2 at start_thread+129()@0x9e6371 at clone +94()@0x88e9be - Java stack -

Severity: Critical

Rationale: Server Outage

17.5.58 Oracle Jrockit R27.3.1 Crashes When Calling Inflate On A Closed Inflator

Description: Sometimes, calling inflate on a closed Inflater results in Oracle JRockit crashing, creating a core file. It can occur with Oracle JRockit R27.3.1.The relevant

stack trace will be similar to the following:Thread Stack Trace: at inflate +73()@0x000000001027C409 at RJNI_java_util_zip_Inflater_inflateFast +90()@0x000000001020162A - Java stack - at java/util/zip/Inflater.inflateFast(JJIJI)I(Native Method) at java/util/zip/Inflater.inflateBytes(Inflater.java:354) at java/util/zip/Inflater.inflate(Inflater.java:216)

Severity: Critical

Rationale: Administration

17.5.59 Parseexception Occurs While Deploying Ear

Description: The application fails when being accessed at first. Once Oracle WebLogic Server is rebooted, the server can be accessed successfully. ParseException occurs while deploying an EAR that has a Kodo connector.

Severity: Critical

Rationale: Server Outage

17.5.60 Saf Agent Discarding Messages

Description: SAF is discarding messages causing message loss.

Severity: Critical

Rationale: Administration

17.5.61 Ssl Incompatibility When Upgrading To Jdk Version 1.6.0_14 And 1.5.0_19

Description: Upgrading to the versions 1.6.0_14 and 1.5.0_19 of the Sun JDK or Oracle JRockit causes compatibility issues between Sun JDK and Oracle JRockit handling of SSL and Oracle WebLogic Server handling of SSL.

Severity: Critical

Rationale: Non-User Viewable Errors

17.5.62 Ssl Incompatibility When Upgrading To Jdk Version 1.6.0_14 And 1.5.0_19 (Wls V10.3)

Description: Upgrading to the versions 1.6.0_14 and 1.5.0_19 of the Sun JDK or Oracle JRockit causes compatibility issues between Sun JDK and Oracle JRockit handling of SSL and Oracle WebLogic Server handling of SSL.

Severity: Critical

Rationale: Non-User Viewable Errors

17.5.63 Solaris Os Has Problems With Default Threading Libraries

Description: When starting Oracle WebLogic Server on Solaris 8 or 5.8, the default threading libraries of the operating system may cause various JVM threading issues, which can ultimately result in the server hanging or crashing.

Severity: Critical

Rationale: Server Outage

17.5.64 Using The Post-Bind Option With Jrockit On Linux Causes Server Core Dump

Description: Attempting to start a server on a Linux platform when setting the post-bind option in a UNIX machine can cause the server to core dump with a StackOverflow exception.This applies to Oracle JRockit R26.2 and above.

Severity: Critical

Rationale: Administration

17.5.65 Windows 2000 Sp2 And Higher Required For Oracle Jrockit 1.5_02 And 1.5_03

Description: Oracle JRockit 1.5_02 (R25.0.0) and Oracle JRockit 1.5_03 (R25.2.0) running on Windows 2000 requires Service Pack 2 or higher. This signature indicates that you are running no service pack or one less than Service Pack 2. Upgrade to Windows 2000 SP 2 or higher.

Severity: Critical

Rationale: Not Complying with Specifications

17.5.66 Windows 2000 Sp4 And Higher Required For Oracle Jrockit 1.5_04 (R26.0.0) Through 1.5_06

Description: Windows 2000 SP4 and higher required for Oracle JRockit 1.5_04 through Oracle JRockit 1.5_06.

Severity: Critical

Rationale: Not Complying with Specifications

17.5.67 With Oracle Jrockit R27.3.0, Ctrl-C Can Cause Improper Shutdown And Loss Of Data

Description: If you are running on Linux or Solaris and press Ctrl-C to properly shut down your application, it will actually terminate immediately and you risk losing any runtime data that hasn't been saved to disk or a database. This happens because Oracle JRockit fails to register the SIGINT signal handler used for the shut down hooks.This issue does not apply to applications running on Windows.

Severity: Critical

Rationale: Administration

17.5.68 Workmanager Requires Authentication During Sever Startup (Wls V10)

Description: If you are using ALBPM 6.0.4 on Oracle WebLogic Server 10.3, and if you have ALBPM processes that contain Global Automatic Activities, then these Global Automatic Activities listen to JMS queues for messages.In ALBPM 6.x implementation, the engine implements this type of Global Automatic Activity by scheduling a work item with the WorkManager (default or custom). The WorkManager runs the work item in one of its threads. The work item, when executed, dynamically creates a JMS queue consumer that represents a Global Automatic Activity.The issue is that you may not notice any consumers on some queues after server start up.

Severity: Critical

Rationale: Server Outage

17.6 Rules For Potential WLS V9 Problems Which May Result In System Outages Or Downtime (Deprecated)

The compliance rules for the Rules For Potential Wls V9 Problems Which May Result In System Outages Or Downtime standard follow.

17.6.1 Administration Console Hangs During Restart Of A Remote Managed Server

Description: Cannot display the JNDI tree on the Oracle WebLogic Server console on a managed server. It seems that the problem is caused by an empty <jndi-name> tag, which was accidentally added in the datasource configuration file.<jdbc-data-source-params> <jndi-name>dsGestionRepresentations</jndi-name> <jndi-name></jndi-name><global-transactions-protocol>TwoPhaseCommit</global-transactions-protocol></jdbc-data-source-params>When reading the tree a java.lang.StackOverflowError appears in the logs.

Severity: Critical

Rationale: Server Outage

17.6.2 An Org.Hibernate.Lazyinitializationexception Occurs For Calls Over Iiop. (Wls V9.2)

Description: When using the -Dweblogic.iiop.useJavaSerialization flag in a call over IIOP, an org.hibernate.LazyInitializationException occurs.

Severity: Critical

Rationale: Server Outage

17.6.3 Assertionerror With Ejbs When Multiple Ejbtimerruntimembeans Created With The Same Name

Description: Oracle WebLogic Server was creating multiple EJBTimerRuntimeMBeans with the same name. As a result of the duplicate names, subsequent EJBTimerRuntimeMBeans with the same name failed to register or unregister. The following AssertionError appears in the server logs with message BEA-080004:An error was thrown by the RMI server:weblogic.management.remote.iiop.IIOPServerImpl.newClient(Ljava.lang.Object;) java.lang.AssertionError: Registered more than one instance with the same objectName :com.bea:ServerRuntime=myserver,Name=MedRecSessionBean,ApplicationRuntime=medrecapp, Type=EJBTimerRuntime, EJBComponentRuntime=MedRecSessionBeanWorkaround or Solution:Oracle WebLogic Server now uses unique names for the EJBTimerRuntimeMBean.

Severity: Critical

Rationale: Administration

17.6.4 Bea06-114.00 - Application Code Installed On A Server May Be Able To Decrypt Passwords

Description: Any site that is running untrusted application code is susceptible to this vulnerability.Application code (for example, EJBs or servlets) can be coded in such a way so as to allow it to decrypt encrypted passwords on the server.This patch resolves the issue by protecting the code to disallow application access. Even after installing

this patch, to optimize security Oracle recommends that application code should be inspected for suspicious code before being installed on the server.

Severity: Critical

Rationale: Administration

17.6.5 Bea06-116.00 - Non-Active Security Provider Appears Active

Description: Newly configured security providers appear to be active despite the fact that the server will not use them until after a server restart. After configuring a new security provider, it may appear that the provider is active before a server restart, as no indication is given that the server is still using the security providers from the last restart. This may lead an administrator to delete or add users, and delete or add security policies to the new provider. The patch for Security Advisory BEA06-116.00 ensures that the WebLogic Administration Console and WebLogic Scripting Tool properly display a warning that the server must be rebooted before a new security provider becomes active. WebLogic Scripting Tool will now display the correct providers in the runtime tree.

Severity: Critical

Rationale: Administration

17.6.6 Bea06-117.00 - Connectionfilters May Leave Server Vulnerable To A Denial-Of-Service Attack

Description: Under certain conditions, connection filters may cause server slowdown, which could make the server vulnerable to a denial-of-service attack.

Severity: Critical

Rationale: Performance

17.6.7 Bea06-119.00 - Vulnerability Of User-Specified Jndi Resources

Description: When using the WebLogic Server Console to set security policies on JNDI resources, the security policies do not properly protect the JNDI resources.

Severity: Critical

Rationale: Server Outage

17.6.8 Bea06-124.00 - Applications Installed On Weblogic Server Can Obtain Private Keys

Description: All sites that allow untrusted applications to be hosted in the server are vulnerable to this issue.An application hosted in the server can obtain the private keys.This patch resolves the issue by restricting access to the private keys.

Severity: Critical

Rationale: Server Outage

17.6.9 Bea06-124.00 - Applications Installed On Weblogic Server Can Obtain Private Keys

Description: All sites that allow untrusted applications to be hosted in the server are vulnerable to this issue.An application hosted in the server can obtain the private keys.This patch resolves the issue by restricting access to the private keys.

Severity: Critical

Rationale: Server Outage

17.6.10 Bea06-126.00 - Console Incorrectly Set Jdbc Policies

Description: All sites where administrators have used the WebLogic Server Administration Console to set custom JDBC security policies are vulnerable to this issue. Sites where the console has not been used to set JDBC security policies are not affected.When setting JDBC security policies, the console was not setting them correctly. This could result in those JDBC resources not being properly secured.This patch resolves the issue by correcting how the console sets JDBC security policies.After the patch is applied, all JDBC policies will need to be reviewed to ensure correctness.

Severity: Critical

Rationale: Administration

17.6.11 Bea06-127.00 - Weblogic Server Http Handlers Log Username And Password On Failure

Description: All sites that that use WebLogic Server HTTP handlers and that host protected Java Web Service (JWS) or web apps are affected by this issue.If access to a protected JWS or web app fails, the username and password used in the access attempt may be logged to the server log. This can result in the password (either valid or invalid) being visible in clear text in the WebLogic Server log.This patch resolves the issue by ensuring that the username and password are removed from the failure message written to the log.

Severity: Critical

Rationale: Server Outage

17.6.12 Bea06-81.02 - Remote Anonymous Binds Are Possible To The Embedded Ldap Server

Description: All sites are vulnerable to this attack.It is possible for a remote user to bind anonymously to the embedded LDAP server and 1) look at user entries (but not attributes) if the schema can be guessed, or 2) launch a denial-of-service attack against the embedded LDAP server by creating many connections to the LDAP server.The patch for Security Advisory BEA06-81.02 resolves the issue by adding an attribute to restrict anonymous bind. After applying this patch and rebooting, anonymous bind will be restricted by default.

Severity: Critical

Rationale: Administration

17.6.13 Bea07-136.00 - Jdbcdatasourcefactory Mbean Password Field Is Not Encrypted

Description: All sites with JDBCDataSourceFactory MBeans that use the Properties attribute to store a password are vulnerable to this issue.A password entered in the JDBCDataSourceFactory MBean Properties was not being removed and encrypted in the Password attribute. This behavior allowed an administrator to view the password in clear text.This patch resolves the issue by ensuring that a password entered in the JDBCDataSourceFactory MBean Properties attribute is properly protected.

Severity: Critical

Rationale: Administration

17.6.14 Bea07-138.00 - Problem With Certificate Validation On Weblogic Server Web Service Clients

Description: This vulnerability can occur in WebLogic clients using Web Services Security (WSSE). In special circumstances an attacker may be able to mount a man-in-the-middle attack.This patch corrects validation to prevent this attack.

Severity: Critical

Rationale: Non-User Viewable Errors

17.6.15 Bea07-143.00 - Ws-Security Runtime Fails To Enforce Decryption Certificate

Description: The Web Services Security (WSSE) runtime may fail to enforce the use of a credential configured for decrypting messages sent by a client. In specific circumstances a malicious remote client may be able to exploit this vulnerability and bypass the application configured security. Patches are available to enforce proper validation by the WSSE runtime.

Severity: Critical

Rationale: Non-User Viewable Errors

17.6.16 Bea07-144.00 - Ejb Calls Can Be Unintentionally Executed With Administrative Privileges

Description: This vulnerability may occur in a transactional Message Driven Bean (MDB) using EJB container persistence. Some of the persistence operations can be called with an administrative identity. This issue only occurs when using the WebLogic Server 6.1 compatibility realm.This advisory resolves the issue by enforcing the execution of these operations with the proper identity.

Severity: Critical

Rationale: Administration

17.6.17 Bea07-145.00 - Permissions On Ejb Methods With Array Parameters May Not Be Enforced

Description: A vulnerability has been found in WebLogic Server in which a security policy created via the console on an EJB method with array parameters may not be enforced. An attacker could exploit this vulnerability to gain unauthorized access to these particularly defined EJB methods.This advisory resolves the issue by properly enforcing EJB security restrictions.

Severity: Critical

Rationale: Administration

17.6.18 Bea07-146.00 - Denial-Of-Service Vulnerability In The Proxy Plug-In For Apache Web Server

Description: Under certain circumstances, the WebLogic Server proxy plug-in for Apache web server may not properly handle a protocol error. As a result, the proxy plug-in could cause the Apache server to fail or to mark back-end WebLogic servers as unavailable. Open sessions may fail and applications hosted by back-end WebLogic

servers may be unreachable. All applications using the WebLogic Server proxy plug-in on an Apache web server are vulnerable to this.

Severity: Critical

Rationale: User Viewable Errors

17.6.19 Bea07-147.00 - Malformed Http Requests May Reveal Data From Previous Requests

Description: An error has been found in the handling of malformed HTTP requests in WebLogic Server. An attacker could exploit this condition to find data involved in previous requests on the server, potentially from other users.This advisory resolves the problem by enforcing proper handling for this type of request.

Severity: Critical

Rationale: Administration

17.6.20 Bea07-149.00 - Security Policy Changes May Not Be Seen By Managed Server

Description: All sites that use admin servers to set security policy for managed servers are vulnerable.In very specific circumstances a policy change made on an admin server for a currently unavailable managed server will never reach the managed server. This is caused by a problem in the handling of the admin server's change log.This would lead to an administrator thinking that the managed server was running with the latest security policies when in fact the managed server might be running with an older set of security policies.This patch resolves the issue by ensuring that security policies will be correctly sent to the managed server.

Severity: Critical

Rationale: Administration

17.6.21 Bea07-150.00 - A Denial Of Service Attack Is Possible On Wls Running On Solaris 9

Description: A client can mount a denial of service attack by manipulating socket connections to a WebLogic Server running on Solaris 9. As a result of this attack, the server may not be able to process other valid requests. This advisory resolves the issue by closing the bad socket connections.

Severity: Critical

Rationale: Administration

17.6.22 Bea07-151.00 - Inadvertent Removal Of Access Restrictions

Description: Any sites that use roles and entitlements to manage WebLogic Portal resources are susceptible to this vulnerability. If an administrative user deletes entitlements for a given role other roles entitlements are inadvertently affected.This patch resolves the issue by enforcing proper access restrictions.

Severity: Critical

Rationale: Administration

17.6.23 Bea07-156.00 - Inadvertent Corruption Of Weblogic Portal Entitlement Policies

Description: Sites that operate in an Oracle WebLogic Server clustered environment and use WebLogic Portal entitlements to manage WebLogic Portal resources are susceptible to this vulnerability. If an administrative user changes a WebLogic Portal entitlement policy on a managed server while the Administrative Server is down, the policy change may not be successfully propagated to the other managed servers in the cluster.This patch resolves the issue by preventing entitlement policy changes when the Administration server is down.

Severity: Critical

Rationale: Administration

17.6.24 Bea07-161.00 - Weblogic Server Embedded Ldap May Be Susceptible To A Brute Force Attack

Description: On specific configurations, the Oracle WebLogic Server embedded LDAP does not limit or audit failed login attempts, and an attacker, inside the firewall, could mount a trial and error attempt to guess the administrator's password. The attacker can also produce a denial of service condition on the LDAP port with the repeated attempts to logon.This advisory resolves this condition by allowing the definition of quotas limiting the usage of the WebLogic Server embedded LDAP. The quotas limit the maximum number of connections, the maximum number of operations per connection, the maximum number of connections per subject, and the maximum number of connections per IP address. In addition, login attempts and information about exceeded quotas are logged.

Severity: Critical

Rationale: Administration

17.6.25 Bea07-162.00 - Admin Console May Display Sensitive Web Service Attributes In Clear Text

Description: The Administration Console supports the configuration of Web Service security to secure particular web services. Administrators can specify security properties required for a particular web service, including passwords used by credential providers and token handlers. During the creation of the configuration, the console may display these sensitive attributes in clear text. However, these sensitive attributes are correctly encrypted when the configuration is written to disk.A patch is available to correct this issue by updating the Administration Console pages so that Web Service Security credential provider and token handler sensitive properties are not displayed in clear text.

Severity: Critical

Rationale: Administration

17.6.26 Bea07-163.00 - Wlst Script Generated By Configtoscript May Not Encrypt Attributes

Description: The WebLogic configToScript command converts an existing server configuration to an executable WebLogic Scripting Tool script and the resulting script can be used to create a new WebLogic domain. However, the generated script may not encrypt sensitive attributes (in particular, the node manager password) when a new

domain is created with the script.A patch is available to allow proper encryption of these sensitive attributes.

Severity: Critical

Rationale: Server Outage

17.6.27 Bea07-164.01 - Security Policy May Not Be Applied To Weblogic Administration Deployers

Description: Security advisory BEA07-164.01 contains the corrected remedy for this vulnerability on Oracle WebLogic Server and WebLogic Express 9.1 and 9.0. This advisory supersedes security advisory BEA07-164.00.

Severity: Critical

Rationale: Server Outage

17.6.28 Bea07-166.00 - Cross-Site Scripting Attacks In The Weblogic Portal Groupspace Application

Description: Rich text content in the WebLogic GroupSpace application is susceptible to cross-site scripting (XSS) attacks. Because rich text content in GroupSpace is actually HTML, it is possible for an authenticated user to add malicious JavaScript code that will execute in another users' environment (e.g., browser) when the HTML is rendered.This patch gives administrators a way to prevent this vulnerability by providing a configurable option to turn off the rich text editor and use a plain text editor instead.

Severity: Critical

Rationale: Administration

17.6.29 Bea07-167.00 - Inadvertent Corruption Of Entitlements Could Result In Unauthorized Access

Description: An authenticated WebLogic Portal administrator or Delegated administrator may cause an inadvertent corruption of a visitor entitlements role when editing the role description if more than 255 characters are entered. This will cause any resources that were protected to no longer be protected. This vulnerability can occur by either editing a role description via the WebLogic Portal Administration Console or through a portal application using the WebLogic Portal APIs.A fix has been provided which prevents the entry of more than 255 characters.

Severity: Critical

Rationale: Administration

17.6.30 Bea07-169.00 - Ssl May Verify Rsa Signatures Incorrectly If The Rsa Key Exponent Is 3

Description: WebLogic SSL may verify incorrectly RSA signatures if the RSA public key exponent is 3. An attacker can create certificates with a forged signature that makes the SSL certificate chain to be improperly verified as valid.This advisory corrects this problem by rejecting RSA certificates with a public key exponent of 3.For additional details about this vulnerability, see the link to Mitre in the For More Information section.

Severity: Critical

Rationale: Administration

17.6.31 Bea07-170.00 - Exposure Of Filenames In Development Mode

Description: The WebLogic Workshop Test View may reveal parent directory information to the WebLogic Workshop Directory (wlwdir) when the application is deployed in an exploded format in a development environment. The WebLogic Workshop Test View console should always be disabled in a production environment.WebLogic Integration 9.2 is only susceptible if the application is deployed explicitly in an exploded form. By default, WebLogic Integration 9.2 does not use the exploded deployment model.This patch resolves this problem by preventing users from navigating beyond the corresponding web application directory.

Severity: Critical

Rationale: Administration

17.6.32 Bea07-171.00 - Non-Trusted Applets May Be Able To Elevate Privileges

Description: The Sun Java Runtime Environment (JRE) contains vulnerabilities that can allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable system.There were two vulnerabilities related to serialization in the Java Runtime Environment. These vulnerabilities would allow a malicious applet or application to elevate its privileges. Earlier BEA JRockit releases supporting applets may be affected by this issue. The latest version of Oracle JRockit JVM cannot be used to run applets, so it is not affected by this issue.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.6.33 Bea07-172.00 - Buffer Overflow In Processing Gif Images

Description: A buffer overflow while processing GIF images in the Java Runtime Environment may allow a malicious applet to elevate its privileges. For example, an applet may grant itself permissions to read and write local files or execute local applications with the privileges of the user running the applet. Earlier versions of BEA JRockit supporting applets may be affected by this issue. Newer versions of BEA JRockit cannot be used to run applets.Under special circumstances, a server running BEA JRockit may also be affected if it can receive (through a web upload) a maliciously crafted image and this image is decoded in the server.

Severity: Critical

Rationale: Administration

17.6.34 Bea07-173.00 - Application Started Through Web Start May Be Able To Elevate Privileges

Description: Java Web Start enables standalone Java applications to be launched from a browser. A vulnerability was reported in Java Web Start that allows a non-trusted application to elevate its privileges. For example, the non-trusted application could read and write local files accessible to the user running the Java Web Start Application. For more information, please contact Oracle Support or visit support.oracle.com.Early releases of BEA JRockit (prior to R26.0) may be affected by this vulnerability and

patches are available to correct this problem. The latest releases of BEA JRockit do not ship with Java Web Start and are not affected by this vulnerability.

Severity: Critical

Rationale: Administration

17.6.35 Bea07-174.00 - Non-Trusted Applets May Be Able To Elevate Privileges

Description: The Sun Java Runtime Environment contains vulnerabilities that can allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable system.Two buffer overflow conditions have been identified that may allow non-trusted applets to elevate their privileges. For example, an applet might be able to grant itself permission to read and write local files, or execute local applications that are accessible to the user running the non-trusted applet. Earlier versions of BEA JRockit supporting applets may be affected by these issues.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.6.36 Bea07-175.00 - Ssl Clients May Miss Possible Cipher Suites Resulting In Use Of Null Cipher (Wls V9)

Description: In some circumstances, SSL clients that run outside the server environment may not find all possible ciphers with which to construct the list of potential SSL cipher suites resulting in use of the default null cipher (no encryption).This advisory corrects this issue by supplying jars and instructions to ensure all cipher suites are found.

Severity: Critical

Rationale: Server Outage

17.6.37 Bea07-176.00 - Server May Select Null Cipher Suite For Ssl Communication With Ssl Clients. (Wls V9)

Description: An attacker could obtain and exploit information that is not encrypted when a null cipher suite is in use. Under certain circumstances, when a client does not offer support for any of the cipher suites available in the server, then the server may select a cipher suite that uses a null cipher; this may result in SSL communication that is not encrypted.This advisory corrects this issue by logging a message when null cipher is in use and also provides administrators the ability to disable the use of null ciphers during SSL communications with SSL clients.

Severity: Critical

Rationale: Server Outage

17.6.38 Bea07-177.00 - Multiple Security Vulnerabilities In The Java Runtime Environment

Description: Contact Oracle Support or visit support.oracle.com for the following information:- A JavaDoc defect may lead to the generation of HTML documentation pages with potential cross-site scripting (XSS) vulnerability.- A buffer overflow vulnerability in the JRE image parsing code may allow an untrusted applet or application to elevate its privileges.- A vulnerability in the JRE font parsing code may

allow an untrusted applet to elevate its privileges.- The Java XML Digital Signature implementation in JDK and JRE 6 does not securely process XSLT stylesheets in XSLT Transforms in XML Signatures.- A JRE Applet Class Loader security vulnerability may allow an untrusted applet that is loaded from a remote system to circumvent network access.

Severity: Critical

Rationale: Administration

17.6.39 Bea07-178.00 - Java Secure Socket Extension Does Not Correctly Process Ssl/Tls Handshake

Description: The Java Secure Socket Extension (JSSE) that is included in various releases of the Java Runtime Environment does not correctly process SSL/TLS handshake requests. This vulnerability may be exploited to create a Denial of Service (DoS) condition to the system as a whole on a server that listens for SSL/TLS connections using JSSE for SSL/TLS support. For more information, please contact Oracle Support or visit support.oracle.com.This advisory corrects this issue by supplying patched versions of JRockit.

Severity: Critical

Rationale: Administration

17.6.40 Bea08-159.01 - Requests Served Through Weblogic Proxy Servlets May Acquire More Privileges

Description: WebLogic HttpClusterServlet or HttpProxyServlet, configured with the "SecureProxy" parameter, may serve external requests to back-end WebLogic servers on behalf of a system identity instead of the proxy's own identity. These external requests may be wrongly granted access to certain administrative resources that are only accessible to an administrator.This advisory resolves the problem by enforcing the use of the proxy identity. The configuration of a proxy has also been enhanced to permit connections using two-way SSL.

Severity: Critical

Rationale: Administration

17.6.41 Bea08-191.00 - Tampering Html Request Headers Could Lead To An Elevation Of Privileges (Wls V9)

Description: An attacker can spoof certain information in a request header, which can potentially allow access to application servlets that rely on this information for authentication.This advisory corrects this issue by ensuring that the header information is properly handled before passing it to the servlet.

Severity: Critical

Rationale: Administration

17.6.42 Bea08-193.00 - Non-Authorized User May Be Able To Receive Messages From A Secured Jms (Wls V9)

Description: WebLogic security policies can be configured to restrict the access to a JMS destination. If an application user does not have the "receive" permission to a JMS destination (queue/topic), an attempt of receiving messages from that destination by

the application should fail with security errors. By exploiting this vulnerability an unauthorized user may be able to receive messages from a standalone (physical) JMS Topic destination or a member of a secured Distributed Topic member destination.This advisory resolves this issue by checking permissions before allowing a subscriber to use a durable subscription.

Severity: Critical

Rationale: Administration

17.6.43 Bea08-194.00 - A Non-Authorized User May Be Able To Send Messages To A Protected Queue. (Wls V9)

Description: The distributed queue feature in WebLogic JMS provides higher availability in a clustered environment. If a JMS client sends a message to a distributed queue and encounters a problem with one member of that distributed queue (the member is down, the member exceeds its quota, access denied, etc), internally the JMS subsystem will retry another member of the same distributed destination. In certain configurations, an unauthorized user is able to send messages to a secure distributed queue.This advisory corrects the problem and ensures that the correct user identity is maintained.

Severity: Critical

Rationale: Administration

17.6.44 Bea08-195.00 - Cross-Site Scripting Vulnerability In The Oracle Weblogic Server Administration Console Unexpected Exception Page. (Wls V9)

Description: The WebLogic Server Administration Console uses fields contained in a URL to identify which information should be included when displaying information to a user.An attacker may be able to inject JavaScript into the console output.This advisory corrects the cross site scripting issue by sanitizing the output.

Severity: Critical

Rationale: Administration

17.6.45 Bea08-196.00 - A Session Fixation Exploit Could Result In Elevated Privileges. (Wls V9.2)

Description: In order to exploit this vulnerability, an attacker must have access to the server's console login page and have a non-administrator user account on that server. A session fixation vulnerability exists which can result in elevation of the attacker's privileges. For more information about Session Fixation attacks, see:http://en.wikipedia.org/wiki/Session_fixationThis advisory corrects this issue by always regenerating an auth cookie on login.

Severity: Critical

Rationale: Administration

17.6.46 Bea08-197.00 - Account Lockout Can Be Bypassed, Allowing A Brute-Force Password Attack

Description: In order to avoid brute-force credential attacks, Oracle WebLogic Server has a mechanism that locks the corresponding user account after a certain number of invalid login attempts. By default, the account is locked after 5 invalid login attempts

and remains locked for 30 minutes.Even after a user has been locked out, logon requests to certain carefully constructed URLs can still give hints as to whether the password is correct or not. This allows a sophisticated attacker to successfully run a brute-force password attack, a dictionary attack, or other similar attacks. All sites that use servlets are vulnerable to this problem.The patch associated with this advisory corrects the problem.

Severity: Critical

Rationale: Administration

17.6.47 Bea08-199.00 - A Carefully Constructed Url May Cause Sun, Iis, Or Apache Web Servers To Crash. (Wls V9)

Description: An attacker can use a carefully constructed URL to cause BEA's proxy plugin to crash the Sun, IIS, or Apache web server process. On re-start, this may cause in-flight requests to be lost. This can cause a temporary denial of service. This attack can be exploited remotely, and the attacker does not require authentication.This advisory resolves the issue in the plugin by correctly handling URLs.

Severity: Critical

Rationale: Administration

17.6.48 Bea08-201.00 - Multiple Security Vulnerabilities In The Java Runtime Environment

Description: This is a combined security advisory. These vulnerabilities are fixed in JRockit R27.5.0. Installers, updates, patches and more information are available at support.oracle.com.

Severity: Critical

Rationale: Administration

17.6.49 Bea08-80.04 - Patches Available To Prevent Multiple Cross-Site Scripting Vulnerabilities (Wls V9)

Description: Cross-Site Scripting (XSS) vulnerabilityFor more information, see:http://download.oracle.com/docs/cd/E13222_01/wls/docs81/servlet/progtasks.html#160803Caution About Existing Samples:Our samples are intended to provide a simple tutorial regarding a few specific features. They are not comprehensive guides to best practices. Many of them omit the use of the Utils.encodeXSS() method or other XSS preventative techniques in needed places and are hence vulnerable to XSS attacks.

Severity: Critical

Rationale: Administration

17.6.50 Cve-2008-1006 - Multiple Security Vulnerabilities In Jrockit

Description: Advisory CVE-2009-1006 refers to all the vulnerability fixes that have been made in JRockit for addressing the applicable issues. The applicable advisories include:CVE 2008-5347CVE 2008-5348CVE 2008-5349CVE 2008-5350CVE 2008-5351CVE 2008-5352CVE 2008-5353CVE 2008-5354CVE 2008-5356CVE 2008-5360xFor more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.6.51 Cve-2008-2576 - Information Disclosure Vulnerability In The Foreignjms Component

Description: Information Disclosure vulnerability in the ForeignJMS component.

Severity: Critical

Rationale: Administration

17.6.52 Cve-2008-2577 - Elevation Of Privilege Vulnerability In The Console/Wlst

Description: Elevation of privilege vulnerability in the Console/WLST.

Severity: Critical

Rationale: Administration

17.6.53 Cve-2008-2578 - Information Disclosure Vulnerability In The Weblogic Console Or Server Log

Description: Information Disclosure vulnerability in the WebLogic console or server log.

Severity: Critical

Rationale: Administration

17.6.54 Cve-2008-2579 - Information Disclosure Vulnerability In Weblogic Plug-Ins For Web Servers (Wls V9)

Description: Information disclosure vulnerability in WebLogic Server plug-ins for Apache, Sun, and IIS Web servers.

Severity: Critical

Rationale: Administration

17.6.55 Cve-2008-2580 - Information Disclosure In Jsp Pages (Wls V9)

Description: Information disclosure in JSP pages.

Severity: Critical

Rationale: Administration

17.6.56 Cve-2008-2581 - Elevation Of Privilege Vulnerabilities In The Uddi Explorer. (Wls V9)

Description: Elevation of privilege vulnerabilities in the UDDI Explorer.

Severity: Critical

Rationale: Administration

17.6.57 Cve-2008-2582 - Denial-Of-Service Vulnerability In Weblogic Server (Oracle Weblogic Server 9.X)

Description: Denial-of-Service vulnerability in WebLogic Server (Oracle WebLogic Server 9.x)

Severity: Critical

Rationale: Server Outage

17.6.58 Cve-2008-3103 - Security Vulnerability In Java Management Extensions (Jmx)

Description: A vulnerability in the Java Management Extensions (JMX) management agent included in the Java Runtime Environment (JRE) may allow a JMX client running on a remote host to perform unauthorized operations on a system running JMX with local monitoring enabled.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.6.59 Cve-2008-3104 - Security Vulnerabilities In Java Runtime Environment Allows Same Origin

Description: Security vulnerabilities in the Java Runtime Environment may allow an untrusted applet that is loaded from a remote system to circumvent network access restrictions and establish socket connections to certain services running on machines other than the one that the applet was downloaded from. This may allow the untrusted remote applet the ability to exploit any security vulnerabilities existing in the services it has connected to.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.6.60 Cve-2008-3105 - Security Vulnerability In The Java Runtime Environment Related Xml Data

Description: A vulnerability in the Java Runtime Environment related to the processing of XML data may allow unauthorized access to certain URL resources (such as some files and web pages) or a Denial of Service (DoS) condition to be created on the system running the JRE.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.6.61 Cve-2008-3106 - Security Vulnerability In The Java Runtime Environment Related To Xlm Data

Description: A vulnerability in the Java Runtime Environment with processing XML data may allow an untrusted applet or application that is downloaded from a website unauthorized access to certain URL resources (such as some files and web pages).For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.6.62 Cve-2008-3108 - A Security Vulnerability With The Processing Of Fonts In The Java Runtime

Description: A buffer overflow security vulnerability with the processing of fonts in the Java Runtime Environment (JRE) may allow an untrusted applet or application to elevate its privileges. For example, an untrusted applet may grant itself permissions to read and write local files or execute local applications that are accessible to the user running the untrusted applet.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.6.63 Cve-2008-3109 - Security Vulnerability In The Java Runtime Environment Scripting Language

Description: A vulnerability in the Java Runtime Environment relating to scripting language support may allow an untrusted applet or application to elevate its privileges. For example, an untrusted applet may grant itself permissions to read and write local files or execute local applications that are accessible to the user running the untrusted applet.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.6.64 Cve-2008-3110 - Security Vulnerability In The Java Runtime Environment Scripting Language

Description: A vulnerability in the Java Runtime Environment relating to scripting language support may allow an untrusted applet to access information from another applet.For more information, please contact Oracle Support or visit support.oracle.com.

Severity: Critical

Rationale: Administration

17.6.65 Cve-2008-3257 - Security Vulnerability In Oracle Weblogic Server Plug-In For Apache (Wls V9)

Description: Recently an exploit has been made public which may impact the availability, confidentiality or integrity of WebLogic Server applications which use the Apache web server configured with the WebLogic plug-in for Apache. This vulnerability may be remotely exploitable without authentication (that is, it may be exploited over a network without the need for a username and password).

Severity: Critical

Rationale: Server Outage

17.6.66 Cve-2008-4008 - Security Vulnerability In Weblogic Plug-In For Apache

Description: This vulnerability may impact the availability, confidentiality, or integrity of WebLogic Server applications which use the Apache web server configured with the WebLogic plug-in for Apache. This vulnerability may be remotely exploitable without authentication, that is, it may be exploited over a network without the need for a username and password.

Severity: Critical

Rationale: Administration

17.6.67 Cve-2008-4009 - Elevation Of Privilege Vulnerability If More Than One Authorizer Is Used

Description: If you configure more than one authorizer (e.g. an XACMLAuthorizer and a DefaultAuthorizer), certain elevation of privileges may occur for some resources.

Severity: Critical

Rationale: Administration

17.6.68 Cve-2008-4010 - Elevation Of Privilege Vulnerability In Some Netui Tags (Wls V9)

Description: This vulnerability in some NetUI tags may allow an attacker to read unauthorized data.

Severity: Critical

Rationale: Administration

17.6.69 Cve-2008-4011 - Elevation Of Privileges For Some Applications (Wls V9.0)

Description: Under certain conditions, some applications in admin state may be made available to non admin users.

Severity: Critical

Rationale: Administration

17.6.70 Cve-2008-4011 - Elevation Of Privileges For Some Applications (Wls V9.1)

Description: Under certain conditions, some applications in admin state may be made available to non admin users.

Severity: Critical

Rationale: Administration

17.6.71 Cve-2008-4011 - Elevation Of Privileges For Some Applications (Wls V9.2)

Description: Under certain conditions, some applications in admin state may be made available to non admin users.

Severity: Critical

Rationale: Administration

17.6.72 Cve-2008-4013 - Protected Web Applications May Be Displayed Under Certain Conditions. (Wls V9.0)

Description: If you upgrade from Oracle WebLogic Server 8.1 Maintenance Pack 3 to a higher version and use auth-method as CLIENT-CERT, some web apps which were protected in Oracle WebLogic Server 8.1 Maintenance Pack 3 may be made available to an invalid user.

Severity: Critical

Rationale: Administration

17.6.73 Cve-2008-4013 - Protected Web Apps May Be Displayed Under Certain Conditions (Wls V9.1)

Description: If you upgrade from Oracle WebLogic Server 8.1 Maintenance Pack 3 to a higher version and use auth-method as CLIENT-CERT, some Web applications which were protected in Oracle WebLogic Server 8.1 Maintenance Pack 3 may be made available to an invalid user.

Severity: Critical

Rationale: Administration

17.6.74 Cve-2008-4013 - Protected Web Apps May Be Displayed Under Certain Conditions. (Wls V9.2)

Description: If you upgrade from Oracle WebLogic Server 8.1SP3 to a higher version and use auth-method as CLIENT-CERT, some web apps which were protected in Oracle WebLogic Server 8.1SP3 may be made available to an invalid user.

Severity: Critical

Rationale: Administration

17.6.75 Cve-2008-5457 - Security Vulnerability In Oracle Weblogic Server Plug-Ins For Apache, Sun, And Iis Web Servers. (Wls V9)

Description: This vulnerability may impact the availability, confidentiality, or integrity of WebLogic Server applications, which use the Apache, Sun, or IIS Web server configured with the WebLogic plug-in for Apache, Sun, or IIS servers, respectively. This vulnerability may be remotely exploitable without authentication; that is, it may be exploited over a network without the need for a username and password.

Severity: Critical

Rationale: Administration

17.6.76 Cve-2008-5460 - Information Disclosure Vulnerability In Jsp And Servlets (Wls V9)

Description: Certain circumstances may cause some information disclosure in WebLogic Server JSPs and servlets.

Severity: Critical

Rationale: Subsystem Outage

17.6.77 Cve-2008-5461 - Elevation Of Privilege Vulnerability In Weblogic Console

Description: This vulnerability in WebLogic Console may allow information disclosure and elevation of privileges. This may be exploited over a network.

Severity: Critical

Rationale: Administration

17.6.78 Cve-2008-5462 - Elevation Of Privilege Vulnerability In Weblogic Portal (Wls V9.2)

Description: This vulnerability in WebLogic Portal may allow elevation of privileges. This may be exploited over a network.

Severity: Critical

Rationale: Administration

17.6.79 Cve-2009-0217 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle JRockit R27.6.3 JRE/JDK 1.6.0_11. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.6.80 Cve-2009-0217 - Critical Patch Update Notice (Wls V9)

Description: Oracle has released Critical Patch Updates for July 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic 9.0, 9.1 and 9.2. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Server Outage

17.6.81 Cve-2009-1002 - Elevation Of Privilege Vulnerability In Weblogic Server (Wls V9)

Description: This vulnerability in WebLogic Server may allow elevation of privileges. This may be exploited over a network.

Severity: Critical

Rationale: Administration

17.6.82 Cve-2009-1003 - Source Code Access Vulnerability In Web Pages, Weblogic Server (Wls V9)

Description: This vulnerability in Oracle WebLogic Server may allow access to source code of Web pages. This may be exploited over a network.

Severity: Critical

Rationale: Administration

17.6.83 Cve-2009-1012 - Security Vulnerability In Weblogic Plug-In For Apache Web Server

Description: This vulnerability may impact the availability, confidentiality, or integrity of WebLogic Server applications, which use the Apache, Sun, or IIS web server configured with the WebLogic plug-in for Apache, Sun, or IIS servers, respectively. This vulnerability may be remotely exploitable without authentication. That is. it may be exploited over a network without the need for a username and password.

Severity: Critical

Rationale: Administration

17.6.84 Cve-2009-1016 - Security Vulnerability In Oracle Weblogic Server Plug-Ins For Apache, Sun, And Iis Servers

Description: This vulnerability may impact the availability, confidentiality, or integrity of Oracle WebLogic Server applications, which use the Apache, Sun, or IIS web server configured with the WebLogic Server plug-ins for Apache, Sun, or IIS servers, respectively.

Severity: Critical

Rationale: Administration

17.6.85 Cve-2009-1094 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for July 2009 that provide corrective action for potential security vulnerabilities for Oracle JRockit R27.6.3 and earlier JRE and JDK 6, R27.6.3 and earlier JRE and JDK 5.0, R27.6.3 and earlier SDK and JRE 1.4.2. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.6.86 Cve-2009-1974 - Critical Patch Update Notice (Wls V9)

Description: Oracle has released Critical Patch Updates for July 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.0, 9.1, and 9.2.

Severity: Critical

Rationale: Server Outage

17.6.87 Cve-2009-2002 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Portal 10.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.6.88 Cve-2009-2002 - Critical Patch Update Notice (Wls V9.2)

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Portal 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.6.89 Cve-2009-2625 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle JRockit 1.5.0_19 and 1.6.0_14.Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.6.90 Cve-2009-3396 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.0, 9.1, and 9.2. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Server Outage

17.6.91 Cve-2009-3403 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for October 2009 that provide corrective action for potential security vulnerabilities for Oracle JRockit 1.6.0_14, 1.5.0_19 and 1.4.2_21. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.6.92 Cve-2009-3555 - Critical Patch Update Notice (Wls V9)

Description: Oracle has released a Critical Patch Update that provides corrective action for a potential security vulnerability for Oracle WebLogic Server 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.6.93 Cve-2010-0068 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.6.94 Cve-2010-0069 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.6.95 Cve-2010-0073 - Critical Patch Update Notice (Wls V9)

Description: Oracle has released a Critical Patch Update that provides corrective action for a potential security vulnerability for Oracle WebLogic Server 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.6.96 Cve-2010-0074 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.6.97 Cve-2010-0078 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle WebLogic Server 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.6.98 Cve-2010-0079 - Critical Patch Update Notice

Description: Oracle has released Critical Patch Updates for January 2010 that provide corrective action for potential security vulnerabilities for Oracle JRockit 1.6.0_14, 1.5.0_19 and 1.4.2_21. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.6.99 Cve-2010-0849 - Critical Patch Update Notice

Description: Oracle has released a Critical Patch Update that provides corrective action for a potential security vulnerability for Oracle JRockit R27.6.6: JRE/JDK 1.4.2, 5 and 6; R28.0.0, JRE/JDK 5 and 6. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Administration

17.6.100 Cve-2010-2375 - Critical Patch Update Notice (Wls V9)

Description: Oracle has released a Critical Patch Update that provides corrective action for a potential security vulnerability for Oracle WebLogic Server 9.x. Please refer to the Remedy and For More Information sections.

Severity: Critical

Rationale: Non-User Viewable Errors

17.6.101 Cluster Hangs In Muxer Threads Under Load

Description: During high load tests, Muxer threads can become stuck in both managed servers. Thread dumps report stack similar to the following:'ExecuteThread: '2' for queue: 'weblogic.socket.Muxer'' daemon prio=10 tid=00a1eb68 nid=26 lwp_id=332127 in Object.wait() [4fae8000..4fae76f8] at java.lang.Object.wait(Native Method) - waiting on <6df388f8> (a java.lang.Object) at java.lang.Object.wait(Object.java:474) at weblogic.rjvm.RJVMImpl.ensureConnectionEstablished(RJVMImpl.java:317) - locked <6df388f8> (a java.lang.Object) at weblogic.rjvm.RJVMImpl.getOutputStream(RJVMImpl.java:340) ...This issue occurs due to an issue in the servlet code.

Severity: Critical

Rationale: Administration

17.6.102 Crashes In Conjunction With A Native Library

Description: If you are using Oracle JRockit in conjunction with a native library that relies on OS signals you may experience crashes due to a signal handling conflict between Oracle JRockit and the native library.Dump stack matches known issue:Thread Stack Trace: at pthread_kill+62()@0xb75c00ee at ptSendSignal +34()@0xb71aedc6 at trapiConvertToDeferredSigsegv+199()@0xb719d207 at trapiSigSegvHandler+40()@0xb719d23c at xehInterpretSavedSigaction +219(amqxerrx.c)@0xb72f276b at xehExceptionHandler+543()@0xb72f2b3f at __libc_sigaction+272()@0xb75c2f80Oracle Engineering found this conflict using IBM's MQSeries native drivers, and it may be present in other libraries that rely on native code.

Severity: Critical

Rationale: Server Outage

17.6.103 Deadlock Occurs In Oracle Weblogic Server (Wls V9.2)

Description: Java level deadlock between weblogic.deployment.jms.JMSSessionPoolTester and weblogic.deployment.jms.JMSSessionPool reveal in Oracle WebLogic Server Thread dump.

Severity: Critical

Rationale: Server Outage

17.6.104 Deleting Channel Used By Rdbms Event Generator Can Cause Deadlock In Server

Description: Deleting a channel used by an RDBMS Event Generator can cause a deadlock in the server.

Severity: Critical

Rationale: Administration

17.6.105 Ejb Client Stuck Rmi Call Over T3

Description: In Oracle WebLogic Server 9.2, a stuck situation can occur between a client and an EJB session. The problem happens if the client application and the EJB are deployed on different JVMs. For a standalone Java the issue can be resolved by using the wlclient.jar on the first order in the Application Classpath. However, for a client application that is running on a different JVM, the Stuck behavior still persists.You could see the following exception:java.rmi.UnmarshalException: Method not found: 'newMethod(Ljava.lang.String;)' at @ weblogic.rmi.internal.MethodDescriptor.getCanonical(MethodDescriptor.....

Severity: Critical

Rationale: Server Outage

17.6.106 Ejb-Based Web Service Leaks Ejb Beans When Message Handler Throws An Exception

Description: EJB-based Web Service leaks EJB beans when the message handler throws an exception. If the SOAP message handler encounters any exception, it fails to release the associated service bean from the cache, which will lead to the leak.

Severity: Critical

Rationale: Subsystem Outage

17.6.107 Entitlements Not Working For Visitor Tools Search Tab

Description: When using the portal visitor tools, portlets residing in entitled portlet categories are still visible to non-entitled users when initially viewing and arranging the portlets. This occurs prior to selecting the "add content" button within the visitor tools.

Severity: Critical

Rationale: Administration

17.6.108 Errors Occur When Using Jax-Rpc Type Classes Generated By Oracle Workshop For Weblogic

Description: Schema enumeration types are not handled properly in the XBeans used by Oracle WebLogic Integration when generating JAX-RPC style objects from a Web Service Definition Language (WSDL) file. Per the JAX-RPC specifications, the generated JAVA types should not have a default constructor that is public. Since XBeans validate that Java Type objects have a default public constructor before binding them with the XML Schema objects, these special type JAX-RPC Java Objects fail to validate, causing the build error in Oracle WebLogic Integration.Example of a build error:'Type

com.frk.middleware.xmlschemas.contactmodifyprofile.v100.ActionType has no default constructor and cannot be unmarshalled from XML.'

Severity: Critical

Rationale: Not Complying with Specifications

17.6.109 Eventgeneratorutils Should Not Use Localhost

Description: If you specify the listen address explicitly, creating or viewing the Event Generator tab in the Oracle WebLogic Integration Console causes a ManagementException and a ConnectException to be thrown. This occurs because the server listens only at the specified address, while the console uses "localhost" to access the server.

Severity: Critical

Rationale: Development

17.6.110 Failed Deployment: Workshop Fails To Publish

Description: During deployment using DynamicUpdateOperation, Application MBeans are nulled out.Replication Steps:1. After four or five partial builds, Workshop fails to publish. Usually, but not always, the error is related to the fact that the root web application could not be deployed.2. While building the publishing fails.3. Then, as an attempted workaround, the following steps were taken: a. Shutdown server. b. Close Workshop. c. Delete the domain "tmp" folder on the admin server. d. Delete both the apt_src and build folder for the projects. e. Restart Workshop. f. Perform a complete clean up. g. Perform a complete build. h. Restart the server.However, this procedure works sometimes. When it fails, you must repeat steps 3.f and 3.g multiple times.

Severity: Critical

Rationale: Development

17.6.111 Http Post Method Can Be Tuned Via Maxpostsize To Harden Security

Description: A denial-of-service attack is a malicious attempt to overload a server by sending more requests than it can handle, preventing access to a service. Attackers may overload the server by sending huge amounts of data in an HTTP POST method. The client can get an HTTP error code 413 (Request Entity Too Large) or the connection may be broken.Prevent this type of attack by setting the MaxPostSize parameter. This limits the number of bytes of data that can be received in a POST from a single request. (By default, the value for MaxPostSize is -1, i.e. unlimited.) If an attacker sends an HTTP POST that exceeds the limit you specify, it triggers a MaxPostSizeExceeded exception and the server logs a "POST size exceeded the parameter MaxPostSize" message.

Severity: Critical

Rationale: Server Outage

17.6.112 Hibernate And Ehcache Cache Locking Problem With Multiple Managed Servers On Same Server

Description: When Hibernate and ehcache are used with Oracle WebLogic Server, the ehcache component writes cached objects to the file system defined by the property java.io.tmpDir. This, in itself, is not an issue. However, when there are two or more

managed servers running on each physical server, these managed servers write to the same directory in the file system using the same file names. Consequently, the servers are sharing resources that require explicit locks in order to modify the files, which can result in a deadlock condition.

Severity: Critical

Rationale: Administration

17.6.113 If Weblogic_Patch.Jar Is After Weblogic.Jar The Installed Patches Have No Effect

Description: Some customers write their own startup and environment scripts. Sometimes they invert the CLASSPATH order. When this occurs, patches applied with BSU are not active even if Oracle Enterprise Manager detects them. The weblogic_patch.jar must always come before weblogic_sp.jar and weblogic.jar in the classpath.

Severity: Critical

Rationale: Administration

17.6.114 Intermittent False Ldap Createexception Causes Oracle Weblogic Portal Synch Issues

Description: In some cases, Oracle WebLogic Server 9.2 may raise the following exceptions in the Oracle WebLogic Portal running on a managed server:weblogic.management.utils.CreateExceptionnetscape.ldap.LDAPException: error result (68)This is due to a timing issue that can occur between the administration server and the managed server when a security policy is changed - in this case, attempting to create a new role when the role already exists. Oracle WebLogic Server fails to detect the existing role, causing the managed server to attempt to create the duplicate role in the Oracle WebLogic Server embedded LDAP.

Severity: Critical

Rationale: Subsystem Outage

17.6.115 Jms Distributed Topic Does Not Resume Communication Between Nodes After A Network Failure

Description: When a Distributed Topic is configured, if a network failure occurs and the Oracle WebLogic Servers lose contact with one another, then the members of the Distributed Destination will not be able to send JMS messages between nodes, even when the network connection has been re-established.

Severity: Critical

Rationale: Subsystem Outage

17.6.116 Jms Jdbc Store Does Not Recover After Database Failure And Reconnection

Description: JMS JDBC store does not recover after database failure and reconnection. It results in the following exception for the affected JMS JDBC Store (Oracle DB):[Store: 280065]failed to connect to database (server="XXXXXXXX" store="XXXXXXX" table="Store1WLStore"):(LinkedCause, "weblogic.jdbc.extensions.ConnectionDeadSQLException: weblogic.common.resourcepool.ResourceDeadException: Could not create pool

connection. The DBMS driver exception was: Io exception: The Network Adapter could not establish the connection")

Severity: Critical

Rationale: Subsystem Outage

17.6.117 Jms Server Byteshighcount Is Greater Than 50 Percent Of Jvm Heapsizecurrent

Description: When the JMS Server's BytesHighCount attribute is greater than 50 percent of the JVM's HeapSizeCurrent, and the BytesPagingEnabled and MessagesPagingEnabled attributes are not set, a JMS processing error may have occured or may occur in the future.

Severity: Critical

Rationale: Server Outage

17.6.118 Jms Subsystem Consumes Too Much Memory

Description: When sending a large number of messages to a JMS queue without any clients to de-queue, Oracle WebLogic Server 9.1 server runs out of memory very quickly.

Severity: Critical

Rationale: Server Outage

17.6.119 Jmsxdeliverycount Property In Messages Sent Through Messaging Bridge

Description: When Oracle WebLogic Server Messaging Bridge attempts to send messages from Oracle WebLogic Server to SonicMQ, the send operation fails with the following exception:<Jan 18, 2007 12:36:02 PM CET> <Debug> <MessagingBridgeRuntimeVerbose> <blade179> <online1> <[ACTIVE] ExecuteThread: '3'for queue: 'weblogic.kernel.Default (self-tuning)'> <<anonymous>> <Oracle1-0135C6595CEBDA119AFB> <> <1169120162762> <000000> <Exception:javax.jms.JMSException: Message Property cannot be set by a JMS client at progress.message.jimpl.JMSExceptionUtil.createJMSException

Severity: Critical

Rationale: Subsystem Outage

17.6.120 Jsps That Include Another Jsp May Result In Infinite Loop On Japanese Environment

Description: If a JSP is included from another JSP, and it is responding to Japanese characters from a client, an infinite loop results that causes high CPU consumption and a stuck thread. The stack trace of the stuck thread is as follows:"[STUCK] ExecuteThread: '0' for queue: 'weblogic.kernel.Default(self-tuning)'" daemon prio=2 tid=0x2b95b530 nid=0xbec runnable [0x2b2df000..0x2b2dfd18] at sun.nio.cs.ext.DoubleByteDecoder.decodeArrayLoop(DoubleByteDecoder.java:94) at sun.nio.cs.ext.DoubleByteDecoder.decodeLoop(DoubleByteDecoder.java:144) at sun.nio.cs.ext.MS932$Decoder.decodeLoop(MS932.java:62) at java.nio.charset.CharsetDecoder.decode(CharsetDecoder.java:544) at weblogic.servlet.internal.CharChunkOutput.write(CharChunkOutput.java:107)

Severity: Critical

Rationale: Server Outage

17.6.121 Mdb Hangs At Weblogic.Messaging.Util.Deliverylist.Waituntilidle

Description: Message Driven Bean (MDB) thread hangs at weblogic.messaging.util.DeliveryList.waitUntilIdle() when using Oracle WebLogic Server 8.1 Threading Model -Dweblogic.Use81StyleExecuteQueues=true.

Severity: Critical

Rationale: Subsystem Outage

17.6.122 Managed Server May Become Defunct If It Is Shut Down Abruptly Via The Node Manager

Description: On Linux OS i686, when a Managed Server is shut down abruptly by means of the Node Manager, the Managed Server may become defunct. This occurs because the Node Manager ignores the SIGCHLD signal, which is not POSIX-compliant.

Severity: Critical

Rationale: Server Outage

17.6.123 Managed Server Starts In Msi If Networkchannel Used To Contact The Admin Disallows Http

Description: If the Administration Server port has not been enabled for either HTTP or HTTP tunneling, when you start a Managed Server through Node Manager, the server will incorrectly boot in Managed Server Independence mode because it cannot find the Administration Server.

Severity: Critical

Rationale: Server Outage

17.6.124 Memory Leak In Jms Thin Client When Running Load Test

Description: Memory leak occurs in JMS thin client when running load tests; objects are not being released properly. This causes OutOfMemory errors on both the client and server side.

Severity: Critical

Rationale: Administration

17.6.125 Memory Leak In Localcallstatemanager For A Provisional Response 100 Trying

Description: Instances of com.bea.wcp.sip.engine.server.LocalCallStateManager $CallState are not cleaned up when a UA sends a BYE before responding to a re-INVITE.This may occur if a UA hangs up (sends a BYE) before it has sent an OK response to a re-INVITE. Oracle WebLogic SIP Server may erroneously wait forever for the OK. - > INVITE< - 100 Trying< - 180 Ringing< - 200 OK - > ACK< - INVITE - > 100 Trying - > BYE (For ACK)< - 200 OK (For BYE)If the UA sends a BYE before responding to the re-INVITE, these call state instances are never destroyed. Over time, this may causes a memory leak of tens of megabytes.If the 100 Trying is not sent, then the re-INVITE times out with a 408 response; thus, dropping the sessions and not creating a memory leak.

Severity: Critical

Rationale: Server Outage

17.6.126 Memory Leak Issue On Devpollsocketmuxer When Running Hp-Ux Dev/Poll

Description: On an HP-UX platform, when an I/O operation on a File Descriptor is canceled, the socket is not being properly cleaned. This causes a File Descriptor leak, which will eventually result in an OutOfMemoryError.

Severity: Critical

Rationale: Server Outage

17.6.127 Messages Left In A Pending State In A Jms Queue

Description: Under high load, messages may become stuck in JMS queues. The JMS messages remain in a state of "receive," and the messages are still not delivered to the Error Dest, even after some hours. Upon a server restart, the messages are redelivered successfully.MessagingKernel debug analysis reveals that the messages stuck in the JMS Queue(s) failed to be unacknowledged by Oracle WebLogic Server, with the following error:Debug> <MessagingKernel> <000000> <Error rolling back received message: weblogic.messaging.kernel.KernelException: Message has already been acknowledgedweblogic.messaging.kernel.KernelException: Message has already been acknowledged at weblogic.messaging.kernel.internal.QueueImpl.negativeAcknowledgeInternal(QueueImpl.java:1314)...

Severity: Critical

Rationale: Subsystem Outage

17.6.128 Multiple Issues When Pathservice Is Not Available

Description: The weblogic.jms.extensions.WLMessageProducer.send(jmsMessage) causes the client application to hang when the following circumstances occur at the same time:* WLMessageProducer.setUnitOfOrder("example1") was set before the application called wlMessageProducer.send(message)* The distributed destination for the message contained DistributedDestinationBean.setUnitOfOrderRouting("PathService") instead of the default "Hash"* An exception occurred when using the path service. This could be attributed to a network problem or the server not being rebooted.

Severity: Critical

Rationale: Subsystem Outage

17.6.129 Nodemanager Fails To Start If Path To The Node Manager Libraries Is Not Set Correctly

Description: The following fatal error occurs if the path to the NodeManager libraries is not set prior to starting the NodeManager: <SEVERE> <Fatal error in node manager server> weblogic.nodemanager.common.ConfigException: Native version is enabled but node manager native library could not be loaded at weblogic.nodemanager.server.NMServerConfig.initProcessControl(NMServerConfig.java:212) at weblogic.nodemanager.server.NMServerConfig.<init>(NMServerConfig.java:172)...

Severity: Critical

Rationale: Server Outage

17.6.130 Noncompliant Interface And Implementation Classes Cause Oracle Jrockit To Crash

Description: When an interface is not compliant with the implementation classes, Oracle JRockit may crash or throw a NullPointerException. This occurs because Oracle JRockit does not perform verification of implemented interfaces before a call, unless it is started with the option -Xverify:all.Oracle JRockit R24.5.0 and previous versions crash under these conditions. Oracle JRockit R25.2.1-11 and later throw a NullPointerException where an IncompatibleClassChangeError could be expected.

Severity: Critical

Rationale: Server Outage

17.6.131 Null Pointer Exception In Weblogic.Wsee.Bind.Internal.Formqualifiedhelper.Getpropertyforelement()

Description: In Oracle WebLogic Server 9.2, a Web Services client runtime NullPointerException may occur inweblogic.wsee.bind.internal.FormQualifiedHelper.getPropertyForElement(). This can occur if the source Web Service Definition Language (WSDL) contains an anonymous type as a referenced fault element. This same source WSDL works without runtime issues in Oracle WebLogic Server 8.1, Websphere 6.0.2, Websphere 6.1, Artix 4.2, and JBoss 4.0.3.

Severity: Critical

Rationale: Not Complying with Specifications

17.6.132 Oracle Jrockit 1.4.2_12 Crash At Mmgetobjectsize()

Description: Oracle JRockit 1.4.2_12 crashed on multiple WLS 8 SP4 servers.Oracle JRockit dump shows the following stack trace:Stack 0: start=0xb7a58000, end=0xb7a9c000, guards=0xb7a5d000 (ok),forbidden=0xb7a5b000Thread Stack Trace: at mmGetObjectSize+8()@0xb7e6b3c8 at findNext+166()@0xb7e9a006 at refIterGetNext +44()@0xb7e9a24c at trMarkRootsForThread+325()@0xb7ea83b5 at mmMarkRootsForThread+44()@0xb7e2cc2c at mmParThreadInspection +45()@0xb7e7794d at tsDoGCInspectionForAllThreads+37()@0xb7ed8555 at mmParMark+118()@0xb7e77d16 at mmGCMainLoop+1074()@0xb7d73722 at tsiCallStartFunction+81()@0xb7e1ac81 at tsiThreadStub+126()@0xb7e1bd1e at ptiThreadStub+18()@0xb7e840d2 at start_thread+129()@0x9e6371 at clone +94()@0x88e9be - Java stack -

Severity: Critical

Rationale: Server Outage

17.6.133 Oracle Jrockit 1.5.0-04 Causes Server To Hang During Startup

Description: When using Oracle JRockit 1.5.0_04 in a Oracle WebLogic Server domain with RFID Enterprise 2.0, the server may hang during startup. This problem with slow startup occurs only if the default Java heap settings have been modified (for example, when specifying a setting such as -Xmx1024mb). If the heap settings have been modified, up to 99 percent of the CPU memory may be utilized during startup.This problem does not happen with Oracle JRockit 1.5.0_06.

Severity: Critical

Rationale: Server Outage

17.6.134 Oracle Jrockit R27.3.1 Crashes When Calling Inflate On A Closed Inflator

Description: Sometimes, calling inflate on a closed Inflater results in Oracle JRockit crashing, creating a core file. It can occur with Oracle JRockit R27.3.1.The relevant stack trace will be similar to the following:Thread Stack Trace: at inflate +73()@0x000000001027C409 at RJNI_java_util_zip_Inflater_inflateFast +90()@0x000000001020162A - Java stack - at java/util/zip/ Inflater.inflateFast(JJIJI)I(Native Method) at java/util/zip/ Inflater.inflateBytes(Inflater.java:354) at java/util/zip/Inflater.inflate(Inflater.java:216)

Severity: Critical

Rationale: Administration

17.6.135 Oracle Service Bus - Stuck Threads In Xquery Cachingfactory.Createengine Hashmap.Getentry

Description: In Oracle Service Bus, stuck threads can occur when processing xQueries, when CachingFactory.createEnginge() performs a HashMap.getEntry().

Severity: Critical

Rationale: Server Outage

17.6.136 Oracle Weblogic Integration Runs Out Of Java Heap Memory

Description: Oracle WebLogic Integration 9.2 runs out of Java heap memory, which results in an Out of Memory error in the Oracle WebLogic Server Administration Console.The following error message is displayed:"java.lang.OutOfMemoryError: Java heap space"

Severity: Critical

Rationale: Server Outage

17.6.137 Oracle Weblogic Server Does Not Abort Transaction When Returning From Service Method

Description: In Oracle WebLogic Server 9.2, when there is an active transaction on a thread that has not been committed or rolled back, the web container does not abort the transaction when the servlet execution is complete.

Severity: Critical

Rationale: Not Complying with Specifications

17.6.138 Out Of Memory Exception Occurs When Editing Oracle Service Bus Stage Node

Description: If a schema used in Oracle Service Bus has recursive nodes, upon stage and edit, a node eventually causes the following OutOfMemoryError:<Apr 19, 2007 7:48:17 AM MDT> <Error> <netuix> <BEA-423147> <Exception [com.bea.portlet.adapter.scopedcontent.ActionLookupFailedException:java.lang.OutOfMemory Error: Java heap space] thrown while trying to do task [handlePostbackData] in class

[com.bea.netuix.servlets.controls.content.StrutsContent].com.bea.portlet.adapter.scopedcontent.ActionLookupFailedException: java.lang.OutOfMemoryError: Java heap space...java.lang.OutOfMemoryError: Java heap space>

Severity: Critical

Rationale: Administration

17.6.139 Production Mode Error - Using Demo Keystores Leaves Ssl Vulnerable To Attack

Description: When running Oracle WebLogic Server in a production environment, the Demo Identity Keystore and DemoTrust Keystore should not be enabled. All of the digital certificates and trusted CA certificates in the Demo Identity Keystore and DemoTrust Keystore are signed by an Oracle WebLogic Server demonstration certificate authority. As a result, all of the Oracle WebLogic Server installations trust each other. This leaves the SSL connections vulnerable to many types of security attacks.

Severity: Critical

Rationale: Server Outage

17.6.140 Rjvm Exception: Closing T3Msgabbrevjvmconnection

Description: Router information in the client's RJVM is getting corrupted. Therefore, the managed server is unable to establish connection after restarting. The Java client fails with an exception similar to the following:Closing: weblogic.rjvm.t3.MuxableSocketT3$T3MsgAbbrevJVMConnection@175e058 because of Server expected to route a message received over an uninitialized connection: 'JVMMessage from ...

Severity: Critical

Rationale: Server Outage

17.6.141 Ssl Incompatibility When Upgrading To Jdk Version 1.6.0_14 And 1.5.0_19

Description: Upgrading to the versions 1.6.0_14 and 1.5.0_19 of the Sun JDK or Oracle JRockit causes compatibility issues between Sun JDK and Oracle JRockit handling of SSL and Oracle WebLogic Server handling of SSL.

Severity: Critical

Rationale: Non-User Viewable Errors

17.6.142 Server May Run Out Of Threads If Number Of Log Files Is Not Limited

Description: In Oracle WebLogic Server, when Log File Rotation is enabled, and the Max Number of Log Files value (NumberOfFilesLimited) is not set to true, then Server will not limit the number of backup log files.In this case, a situation may arise where there are too many log files to be rotated and Oracle WebLogic Server threads get struck while trying to roll the log files. This will lead to server outage.To prevent this situation, do either of the following:a) Periodically backup the log files to a different location (Manual Process).b) Set the NumberOfFileLimited=true for the Log MBean.

Severity: Critical

Rationale: Server Outage

17.6.143 Sessions Are Lost After Configuring Saml With Two Domains On The Same Computer

Description: Sessions are lost after configuring SAML with two domains (Oracle WebLogic Server 9.x or Oracle WebLogic Server 10.x) running on one system.It is a SAML requirement to set all webapp cookie names to the default (JSESSIONID). With this setting, the client browser can differentiate cookies originating from different domains only if the IPAddress or hostname of the SAML source and destination domain are not the same.

Severity: Critical

Rationale: User Viewable Errors

17.6.144 Soap Messages With Attachments Are Not Handled Properly

Description: MimeMessage is reset to null after writing the data to stream. This causes thegetContentType call to fail, and so eventually SOAP attachments are not handledcorrectly.

Severity: Critical

Rationale: Subsystem Outage

17.6.145 Solaris Os Has Problems With Default Threading Libraries

Description: When starting Oracle WebLogic Server on Solaris 8 or 5.8, the default threading libraries of the operating system may cause various JVM threading issues, which can ultimately result in the server hanging or crashing.

Severity: Critical

Rationale: Server Outage

17.6.146 Stackoverflowerror Is Reported When Viewing Jndi Tree From Console

Description: If one data source with an empty JNDI name is deployed to a server, a StackOverflowError will be reported when viewing JNDI tree of the server.

Severity: Critical

Rationale: Administration

17.6.147 Stuck Threads And High Cpu Usage Caused By Failing Synchronization On Java.Util.Hashmap

Description: Unsynchronized HashMap leads to stuck threads and high CPU usage.The relevant stack trace is as follows:Thread-333 "[STUCK] ExecuteThread: '10' for queue: 'weblogic.kernel.Default(self-tuning)'" <alive, suspended, priority=1, DAEMON> { java.util.HashMap.put(HashMap.java:416) weblogic.descriptor.internal.DuplicateChecker.register(DuplicateChecker.java:52) weblogic.descriptor.internal.DuplicateChecker.registerIfNoDuplicate(DuplicateChecker.java:18) weblogic.descriptor.internal.ReferenceManager.registerBean(ReferenceManager.java:205) ....

Severity: Critical

Rationale: Subsystem Outage

17.6.148 The Customer Has Applied A Patch From Oracle Bug 8087768 But Still Getting Ora-00001 On Load

Description: The customer has applied a patch from Oracle Bug 8087768 (8068770 + 8085020); however, ORA-00001 still occurs under the load.

Severity: Critical

Rationale: Performance

17.6.149 Transaction Fails To Commit With Xaer_Proto Exception When Writing To Message Queue

Description: When Oracle WebLogic Server writes a message to the Message Queue via JMS wrappers, the transaction fails during commit, and an MQXAR is registered. When the registration is removed, the transaction works properly. If you use the JMS wrappers to write the message to Oracle WebLogic Server JMS, it also works correctly.

Severity: Critical

Rationale: Administration

17.6.150 Users Can Reconnect To Node Manager Without The Correct Username And Password

Description: During a WLST session, after disconnecting from the Node Manager, users are able to reconnect to the Node Manager without passing the correct username and password to the nmConnect() method.

Severity: Critical

Rationale: Administration

17.6.151 Using Admin Console To Export/Import Large Jms Message Queue Causes Out Of Memory Error

Description: When there is a large JMS Queue (large number of messages/large messages), using the Oracle WebLogic Server Administration Console to export the queue causes an Out of Memory error.

Severity: Critical

Rationale: Server Outage

17.6.152 Using Oracle Weblogic Server Jsp To Recompile Jsp File'S Antidependent Files Causes Infinite Compile Loop

Description: For Oracle WebLogic Server 9.1, using the Oracle WebLogic Server JSP compiler may result in an infinite loop where the compilation never completes.

Severity: Critical

Rationale: Subsystem Outage

17.6.153 Using Xquery File That Uses Xsds With Recursive Nodes Results In Out Of Memory Exceptions

Description: Using large schema (XQuery file using XSDs with circular imports) in the Eclipse XQuery Mapper is resulting in Out Of Memory Exceptions (OOMEs).Patch Oracle Bug 8111384 enables the XQuery Mapper to load large schema.

Severity: Critical

Rationale: Server Outage

17.6.154 Using The Post-Bind Option With Jrockit On Linux Causes Server Core Dump

Description: Attempting to start a server on a Linux platform when setting the post-bind option in a UNIX machine can cause the server to core dump with a StackOverflow exception.This applies to Oracle JRockit R26.2 and above.

Severity: Critical

Rationale: Administration

17.6.155 Wldf Is Causing High Cpu Usage, Even After Wldf Is Turned Off

Description: Oracle WebLogic Server Diagnostic Framework indexes log files in the background to facilitate accessor queries. With heavy logging activity, this can burden the CPU (up to 100%) even when no accessor queries are performed.

Severity: Critical

Rationale: Performance

17.6.156 Wldf With Jdbc Archive Selects Contents Of Table On Server Startup

Description: The Archive component of the Oracle WebLogic Diagnostic Framework (WLDF) captures and persists data events, log records, and metrics. WLDF can be configured to archive diagnostic data to a file store or a Java Database Connectivity (JDBC) data source. When using a JDBC archive for WLDF, Oracle WebLogic Server issues a full table select against each of the archive tables when starting the server. In a large database, issuing full selects when the server starts can delay the startup time and add large memory overhead to the server at runtime. You may use a file-based archive as a workaround. Oracle Bug 8143627 changes the behavior of Oracle WebLogic Server to verify that the table and columns exist, but not return any results.

Severity: Critical

Rationale: Administration

17.6.157 Weblogic.Net.Http.Httpurlconnection May Cause Failures When Keepalive Is Used

Description: WebLogic.net.http.HttpURLConnection may cause failures when KeepAlive is used. This can occur in the following scenario: A Web service is deployed on Oracle WebLogic Server 9.2, and the Service is called every 10 seconds from a JAX-WS client deployed on another Oracle WebLogic Server 9.2 server. Both servers are separated by an Apache 2.2.3 forward and reverse proxy, as follows: The JAX-WS client uses weblogic.net.http.HttpURLConnection to call the Web service. The response from the Oracle WebLogic Server 9.2 Web service arrives with chunked encoding; but, at the receiving end, the Oracle WebLogic Server HttpURLConnection

fails to strip the chunk internal information and sends a corrupted InputStream to JAX-WS, causing a parsing failure.

Severity: Critical

Rationale: Not Complying with Specifications

17.6.158 Windows 2000 Sp2 And Higher Required For Oracle Jrockit 1.5_02 And 1.5_03

Description: Oracle JRockit 1.5_02 (R25.0.0) and Oracle JRockit 1.5_03 (R25.2.0) running on Windows 2000 requires Service Pack 2 or higher. This signature indicates that you are running no service pack or one less than Service Pack 2. Upgrade to Windows 2000 SP 2 or higher.

Severity: Critical

Rationale: Not Complying with Specifications

17.6.159 Windows 2000 Sp4 And Higher Required For Oracle Jrockit 1.5_04 (R26.0.0) Through 1.5_06

Description: Windows 2000 SP4 and higher required for Oracle JRockit 1.5_04 through Oracle JRockit 1.5_06.

Severity: Critical

Rationale: Not Complying with Specifications

17.6.160 With Oracle Jrockit R27.3.0, Ctrl-C Can Cause Improper Shutdown And Loss Of Data

Description: If you are running on Linux or Solaris and press Ctrl-C to properly shut down your application, it will actually terminate immediately and you risk losing any runtime data that hasn't been saved to disk or a database. This happens because Oracle JRockit fails to register the SIGINT signal handler used for the shut down hooks.This issue does not apply to applications running on Windows.

Severity: Critical

Rationale: Administration

17.6.161 Workmanager Requires Authentication During Sever Startup (Wls V9)

Description: If you are using ALBPM 6.0.4 on Oracle WebLogic Server 9.2.x, and if you have ALBPM processes that contain Global Automatic Activities, then these Global Automatic Activities listen to JMS queues for messages. In ALBPM 6.x implementation, the engine implements this type of Global Automatic Activity by scheduling a work item with the WorkManager (default or custom). The WorkManager runs the work item in one of its threads. The work item, when executed, dynamically creates a JMS queue consumer that represents a Global Automatic Activity. The issue is that you may not notice any consumers on some queues after server start up.

Severity: Critical

Rationale: Server Outage

17.6.162 Xml To Java Transformation Fails

Description: XQuery transformations (Java to XML and vice-versa) may throw a com.bea.transform.TransformException. This can occur if an array field of "custom type" is present, or if the element "paging" is not recognized by the mapping.

Severity: Critical

Rationale: Subsystem Outage

17.7 WebLogic Domain Configuration Compliance

The compliance rules for the Weblogic Domain Configuration Compliance standard follow.

17.7.1 Administration Port Enabled

Description: The compliance standard rule verifies whether BEA WebLogic Domain Administration Port is enabled or not. An Administration Port limits all administration traffic between server instances in a WebLogic Domain to a single port.

Severity: Critical

Rationale: Administration Port Enabled rule enables you to separate administration traffic from application traffic in your domain. The administration port accepts only secure, SSL traffic, and all connections via the port require authentication by a server administrator.

17.7.2 Exalogic Optimizations Enabled

Description: The compliance standard rule verifies whether ExalogicOptimizationsEnabled flag of the domain is enabled or not.

Severity: Critical

Rationale: ExalogicOptimizationsEnabled attribute improves thread management and request processing, and reduced lock contention. This attribute should be enabled only when configuring a WebLogic domain for Oracle Exalogic.

17.7.3 Production Mode Enabled

Description: The compliance standard rule verifies whether all the BEA WebLogic Managed Servers of the Domain target are running in production mode or not.

Severity: Critical

Rationale: All the WebLogic Servers of a Domain use different default values for various services depending on the type of environment you specify. You can indicate whether the Domain is to be used in a development environment or a production environment.

18

Oracle WebLogic Server Compliance Standards

These are the compliance rules for the Oracle WebLogic Server compliance standards

18.1 Weblogic Server Configuration Compliance

The compliance rules for the Weblogic Server Configuration Compliance standard follow.

18.1.1 Enable Java Net Fast Path Check

Description: The compliance standard rule verifies whether Java Net FastPath attribute is enabled or not. This attribute enables the Oracle JDBC driver to reduce data copies and fragmentation.

Severity: Critical

Rationale: Enabling this attribute, enables Fast Application Notification (FAN) event awareness of WebLogic Server.

18.1.2 Gathered Writes Enabled

Description: The compliance standard rule verifies whether gathered writes over NIO socket channels enabled or not.

Severity: Critical

Rationale: Enabling GatheredWritesEnabled attribute increases efficiency during I/O in environments with high network throughput.

18.1.3 Jdbc Datasource Protocol Check

Description: The rule verifies whether JDBCDatasourceProtocol attribute is SDP protocol or not. WebLogic Server data sources using a JDBC connection string with the protocol portion being set to SDP (PROTOCOL=SDP) are restricted to Exalogic Elastic Cloud Software.

Severity: Critical

Rationale: JDBC Datasource Protocol Check

18.1.4 Jms File Store Configured To Zfs Storage Check

Description: The compliance standard rule verifies whether JMS persistent file store is configured to ZFS storage.

Severity: Critical

Rationale: By configuring the file store to ZFS store, it will be automatically migrated from an unhealthy server instance to a healthy server instance.

18.1.5 Jms Server Maximum Message Count Check

Description: The compliance standard rule verifies whether maximum message count quota for JMS server to be configured for a reasonable value.

Severity: Critical

Rationale: Tuning maximum message count for JMS Server, may improve performance dramatically, such as when the JMS application defers acknowledges or commits

18.1.6 Jsse Enabled

Description: The compliance standard rule verifies whether JSSE as SSL is enabled or not for Weblogic Server target.

Severity: Critical

Rationale: JSSE is the Java standard framework for SSL and TLS and includes both blocking-IO and non-blocking-IO APIs. When WebLogic Server with JSSE SSL is used as either an SSL client or as the SSL server, it can communicate via SSL with instances of WebLogic Server (version 8.1 and later) that use the Certicom SSL implementation.

18.1.7 Oracle Optimize Utf8 Conversion Check

Description: The compliance standard rule verifies whether the Oracle JDBC optimize UTF-8 conversion option is enabled or not.

Severity: Critical

Rationale: Enabling this attribute, enforces UTF-8 encoding for all files and directories in the file system. When 'Reject non UTF-8' option set, any attempts to create a file or directory with an invalid UTF-8 encoding will fail.

18.1.8 Outbound Enable Check For Sdp Channel

Description: The compliance standard rule verifies whether outbound attribute is enabled for the custom replication channel that uses SDP.

Severity: Critical

Rationale: Enabling this attribute, allows all outbound traffic to use this channel. SDP is an Infiniband feature that can be used as an alternative to TCP/IP that reduces network latency and CPU utilization.

18.1.9 Performance Pack Enabled

Description: The compliance standard rule verifies whether BEA WebLogic Server Performance Pack is enabled or not

Severity: Critical

Rationale: Benchmarks show major performance improvements in WebLogic Server when you use the performance pack for your platform. Performance packs use a platform-optimized (native) socket multiplexor to improve server performance.

18.1.10 Scattered Reads Enabled

Description: The compliance standard rule verifies whether scattered reads over NIO socket channels are enabled or not.

Severity: Critical

Rationale: Enabling ScatteredReadsEnabled attribute increases efficiency during I/O in environments with high network throughput.

18.1.11 Synchronous Write Policy Check For Jms File Stores

Description: The compliance standard rule verifies whether synchronous-write-policy is configured to direct-write for JMS file stores.

Severity: Critical

Rationale: Configuring synchronous write policy to direct-write will improve reliability.

19

Pluggable Database Compliance Standards

These are the compliance rules for the Pluggable Database compliance standards

19.1 Basic Security Configuration For Oracle Pluggable Database

The compliance rules for the Basic Security Configuration For Oracle Pluggable Database standard follow.

19.1.1 Access To Dba_Roles View

Description: Ensures restricted access to DBA_ROLES view

Severity: Minor Warning

Rationale: DBA_ROLES view contains details of all roles in the database. Knowledge of the structure of roles in the database can be taken advantage of by a malicious user.

19.1.2 Access To Dba_Role_Privs View

Description: Ensures restricted access to DBA_ROLE_PRIVS view

Severity: Minor Warning

Rationale: The DBA_ROLE_PRIVS view lists the roles granted to users and other roles. Knowledge of the structure of roles in the database can be taken advantage of by a malicious user.

19.1.3 Access To Dba_Sys_Privs View

Description: Ensures restricted access to DBA_SYS_PRIVS view

Severity: Minor Warning

Rationale: DBA_SYS_PRIVS view can be queried to find system privileges granted to roles and users. Knowledge of the structure of roles in the database can be taken advantage of bya malicious user.

19.1.4 Access To Dba_Tab_Privs View

Description: Ensures restricted access to DBA_TAB_PRIVS view

Severity: Minor Warning

Rationale: Lists privileges granted to users or roles on objects in the database. Knowledge of the structure of roles in the database can be taken advantage of by a malicious user.

19.1.5 Access To Dba_Users View

Description: Ensures restricted access to DBA_USERS view

Severity: Minor Warning

Rationale: Contains user password hashes and other account information. Access to this information can be used to mount brute-force attacks.

19.1.6 Access To Stats$Sqltext Table

Description: Ensures restricted access to STATS$SQLTEXT table

Severity: Minor Warning

Rationale: This table provides full text of the recently-executed SQL statements. The SQL statements can reveal sensitive information.

19.1.7 Access To Stats$Sql_Summary Table

Description: Ensures restricted access to STATS$SQL_SUMMARY table

Severity: Minor Warning

Rationale: Contains first few lines of SQL text of the most resource intensive commands given to the server. Sql statements executed without bind variables can show up here exposing privileged information.

19.1.8 Access To Sys.Aud$ Table

Description: Ensures restricted access to SYS.AUD$ table

Severity: Minor Warning

Rationale: A knowlegeable and malicious user can gain access to sensitive audit information.

19.1.9 Access To Sys.Source$ Table

Description: Ensures restricted access to SYS.SOURCE$ table

Severity: Minor Warning

Rationale: Contains source of all stored packages units in the database.

19.1.10 Access To Sys.User$ Table

Description: Ensures restricted access to SYS.USER$ table

Severity: Minor Warning

Rationale: Username and password hash may be read from the SYS.USER$ table, enabling a hacker to launch a brute-force attack.

19.1.11 Access To Sys.User_History$ Table

Description: Ensures restricted access to SYS.USER_HISTORY$ table

Severity: Minor Warning

Rationale: Username and password hash may be read from the SYS.USER_HISTORY$ table, enabling a hacker to launch a brute-force attack.

19.1.12 Default Passwords

Description: Ensure there are no default passwords for known accounts

Severity: Warning

Rationale: A malicious user can gain access to the database using default passwords.

19.1.13 Execute Privileges On Dbms_Job To Public

Description: Ensures PUBLIC is not granted EXECUTE privileges on DBMS_JOB package

Severity: Critical

Rationale: Granting EXECUTE privilege to PUBLIC on DBMS_JOB package allows users to schedule jobs on the database.

19.1.14 Execute Privileges On Dbms_Sys_Sql To Public

Description: Ensures PUBLIC is not granted EXECUTE privileges on DBMS_SYS_SQL package

Severity: Critical

Rationale: The DBMS_SYS_SQL package can be used to run PL/SQL and SQL as the owner of the procedure rather than the caller.

19.1.15 Password Complexity Verification Function Usage

Description: Ensures PASSWORD_VERIFY_FUNCTION resource for the profile is set

Severity: Critical

Rationale: Having passwords that do not meet minimum complexity requirements offer substantially less protection than complex passwords.

19.1.16 Password Grace Time

Description: Ensures that all profiles have PASSWORD_GRACE_TIME set to a reasonable number of days

Severity: Critical

Rationale: A high value for the PASSWORD_GRACE_TIME parameter may cause serious database security issues by allowing the user to keep the same password for a long time.

19.1.17 Password Lifetime

Description: Ensures that all profiles have PASSWORD_LIFE_TIME set to a reasonable number of days

Severity: Warning

Rationale: A long password life time gives hackers a long time to try and cook the password. May cause serious database security issues.

19.1.18 Password Locking Time

Description: Ensures PASSWORD_LOCK_TIME is set to a reasonable number of days for all profiles

Severity: Warning

Rationale: Having a low value increases the likelihood of Denial of Service attacks.

19.1.19 Restricted Privilege To Execute Utl_Http

Description: Ensure PUBLIC does not have execute privileges on the UTL_HTTP package

Severity: Critical

Rationale: Privileges granted to the PUBLIC role automatically apply to all users. A malicious user can gain access to email, network and http modules using the EXECUTE privilege.

19.1.20 Restricted Privilege To Execute Utl_Smtp

Description: Ensure PUBLIC does not have execute privileges on the UTL_SMTP package

Severity: Critical

Rationale: Privileges granted to the PUBLIC role automatically apply to all users. A malicious user can gain access to email, network and http modules using the EXECUTE privilege.

19.1.21 Restricted Privilege To Execute Utl_Tcp

Description: Ensure PUBLIC does not have execute privileges on the UTL_TCP package

Severity: Critical

Rationale: Privileges granted to the PUBLIC role automatically apply to all users. A malicious user can gain access to email, network and http modules using the EXECUTE privilege.

19.1.22 Well Known Accounts

Description: Checks for accessibility of well-known accounts

Severity: Warning

Rationale: A knowledgeable malicious user can gain access to the database using a well-known account.

19.2 Configuration Best Practices For Oracle Database

The compliance rules for the Configuration Best Practices For Oracle Database standard follow.

19.2.1 Disabled Automatic Statistics Collection

Description: Checks if the STATISTICS_LEVEL initialization parameter is set to BASIC

Severity: Critical

Rationale: Automatic statistics collection allows the optimizer to generate accurate execution plans and is essential for identifying and correcting performance problems. By default, STATISTICS_LEVEL is set to TYPICAL. If the STATISTICS_LEVEL initialization parameter is set to BASIC the collection of many important statistics, required by Oracle database features and functionality, are disabled.

19.2.2 Not Using Automatic Pga Management

Description: Checks if the PGA_AGGREGATE_TARGET initialization parameter has a value of 0 or if WORKAREA_SIZE_POLICY has value of MANUAL.

Severity: Warning

Rationale: Automatic PGA memory management simplifies and improves the way PGA memory is allocated. When enabled, Oracle can dynamically adjust the portion of the PGA memory dedicated to work areas while honoring the PGA_AGGREGATE_TARGET limit set by the DBA.'

19.2.3 Statistics_Level Parameter Set To All

Description: Checks if the STATISTICS_LEVEL initialization parameter is set to ALL

Severity: Minor Warning

Rationale: Automatic statistics collection allows the optimizer to generate accurate execution plans and is essential for identifying and correcting performance problems. The STATISTICS_LEVEL initialization parameter is currently set to ALL, meaning additional timed OS and plan execution statistics are being collected. These statistics are not necessary and create additional overhead on the system.

19.2.4 Timed_Statistics Set To False

Description: Checks if the TIMED_STATISTICS initialization parameter is set to FALSE.

Severity: Critical

Rationale: Setting TIMED_STATISTICS to FALSE prevents time related statistics, e.g. execution time for various internal operations, from being collected. These statistics are useful for diagnosing and performance tuning. Setting TIMED_STATISTICS to TRUE will allow time related statistics to be collected, and will also provide more value to the trace file and generates more accurate statistics for long-running operations.

19.2.5 Use Of Non-Standard Initialization Parameters

Description: Checks for use of non-standard initialization parameters

Severity: Minor Warning

Rationale: Non-standard initialization parameters are being used. These may have been implemented based on poor advice or incorrect assumptions. In particular, parameters associated with SPIN_COUNT on latches and undocumented optimizer features can cause a great deal of problems that can require considerable investigation.

19.3 High Security Configuration For Oracle Pluggable Database

The compliance rules for the High Security Configuration For Oracle Pluggable Database standard follow.

19.3.1 Access To *_Catalog_* Roles

Description: Ensure grant of %_CATALOG_% is restricted

Severity: Critical

Rationale: %_CATALOG_% Roles have critical access to database objects, that can lead to exposure of vital information in database system.

19.3.2 Access To All_Source View

Description: Ensures restricted access to ALL_SOURCE view

Severity: Minor Warning

Rationale: ALL_SOURCE view contains source of all stored packages in the database.

19.3.3 Access To Dba_* Views

Description: Ensures SELECT privilege is never granted to any DBA_ view

Severity: Warning

Rationale: The DBA_* views provide access to privileges and policy settings of the database. Some of these views also allow viewing of sensitive PL/SQL code that can be used to understand the security policies.

19.3.4 Access To Role_Role_Privs View

Description: Ensures restricted access to ROLE_ROLE_PRIVS view

Severity: Minor Warning

Rationale: Lists roles granted to other roles. Knowledge of the structure of roles in the database can be taken advantage of by a malicious user.

19.3.5 Access To Sys.Link$ Table

Description: Ensures restricted access to LINK$ table

Severity: Minor Warning

Rationale: A knowlegeable and malicious user can gain access to user passwords from the SYS.LINK$ table.

19.3.6 Access To User_Role_Privs View

Description: Ensures restricted access to USER_ROLE_PRIVS view

Severity: Minor Warning

Rationale: Lists the roles granted to the current user. Knowledge of the structure of roles in the database can be taken advantage of by a malicious user.

19.3.7 Access To User_Tab_Privs View

Description: Ensures restricted access to USER_TAB_PRIVS view

Severity: Minor Warning

Rationale: Lists the grants on objects for which the user is the owner, grantor or grantee. Knowledge of the grants in the database can be taken advantage of by a malicious user.

19.3.8 Access To V$ Views

Description: Ensures SELECT privilege is not granted to any V$ Views

Severity: Critical

Rationale: V$ tables contain sensitive information about Oracle database and should only be accessible by system administrators. Check for any user that has access and revoke where possible

19.3.9 Access To X_$ Views

Description: Ensure access on X$ views is restricted

Severity: Critical

Rationale: This can lead to revealing of internal database structure information.

19.3.10 Audit Alter Any Table Privilege

Description: Ensures ALTER ANY TABLE Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing ALTER ANY TABLE will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

19.3.11 Audit Alter User Privilege

Description: Ensures ALTER USER Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing ALTER USER will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

19.3.12 Audit Create Any Library Privilege

Description: Ensures CREATE ANY LIBRARY is being audited by access for all users

Severity: Critical

Rationale: Auditing CREATE ANY LIBRARY will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

19.3.13 Audit Create Library Privilege

Description: Ensures CREATE LIBRARY Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing CREATE LIBRARY will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

19.3.14 Audit Create Role Privilege

Description: Ensures CREATE ROLE Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing the creation of roles will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

19.3.15 Audit Create Session Privilege

Description: Ensures CREATE SESSION Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing CREATE SESSION will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

19.3.16 Audit Create User Privilege

Description: Ensures CREATE USER Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing CREATE USER will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

19.3.17 Audit Drop Any Procedure Privilege

Description: Ensures DROP ANY PROCEDURE Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing DROP ANY PROCEDURE will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

19.3.18 Audit Drop Any Role Privilege

Description: Ensures DROP ANY ROLE Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing the creation of roles will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

19.3.19 Audit Drop Any Table Privilege

Description: Ensures DROP ANY TABLE Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing DROP ANY TABLE will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

19.3.20 Audit Execute Any Procedure Privilege

Description: Ensures EXECUTE ANY PROCEDURE Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing the creation of roles will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

19.3.21 Audit Grant Any Object Privilege

Description: Ensures SELECT ANY DICTIONARY Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing SELECT ANY DICTIONARY will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

19.3.22 Audit Grant Any Privilege

Description: Ensures GRANT ANY PRIVILEGE is being audited by access for all users

Severity: Critical

Rationale: Auditing GRANT ANY PRIVILEGE will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

19.3.23 Audit Insert Failure

Description: Ensures that insert failures are audited for critical data objects

Severity: Warning

Rationale: Not auditing insert failures for critical data objects may allow a malicious user to infiltrate system security..

19.3.24 Audit Select Any Dictionary Privilege

Description: Ensures SELECT ANY DICTIONARY Privilege is being audited by access for all users

Severity: Critical

Rationale: Auditing SELECT ANY DICTIONARY will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events

19.3.25 Connect Time

Description: Ensure that users profile settings CONNECT_TIME have appropriate value set for the particular database and application

Severity: Critical

Rationale: Sessions held open for excessive periods of time can consume system resources and cause a denial of service for other users of the Oracle database. The CONNECT_TIME parameter limits the upper bound on how long a session can be held open. This parameter is specified in minutes. Sessions that have exceeded their connect time are aborted and rolled back

19.3.26 Cpu Per Session

Description: Ensures that all profiles have CPU_PER_SESSION set to a reasonable number of CPU cycles

Severity: Critical

Rationale: Allowing a single application or user to consume excessive CPU resources will result in a denial of service to the Oracle database

19.3.27 Execute Privileges On Dbms_Lob To Public

Description: Ensures PUBLIC group is not granted EXECUTE privileges to the DBMS_LOB package

Severity: Critical

Rationale: The DBMS_LOB package can be used to access any file on the system as the owner of the Oracle software installation.

19.3.28 Execute Privileges On Utl_File To Public

Description: Ensure PUBLIC does not have EXECUTE privilege on the UTL_FILE package

Severity: Critical

Rationale: Privileges granted to the PUBLIC role automatically apply to all users. A malicious user can read and write arbitrary files in the system when granted the UTL_FILE privilege.

19.3.29 Execute Privilege On Sys.Dbms_Export_Extension To Public

Description: Ensure PUBLIC does not have execute privileges on the SYS.DBMS_EXPORT_EXTENSION package

Severity: Critical

Rationale: Privileges granted to the PUBLIC role automatically apply to all users. DBMS_EXPORT_EXTENSION can allow sql injection. Thus a malicious will be able to take advantage.

19.3.30 Execute Privilege On Sys.Dbms_Random Public

Description: Ensure PUBLIC does not have execute privileges on the SYS.DBMS_RANDOM package

Severity: Critical

Rationale: Privileges granted to the PUBLIC role automatically apply to all users. DBMS_RANDOM can allow sql injection. Thus a malicious will be able to take advantage.

19.3.31 Granting Select Any Table Privilege

Description: Ensures SELECT ANY PRIVILEGE is never granted to any user or role

Severity: Warning

Rationale: The SELECT ANY TABLE privilege can be used to grant users or roles with the ability to view data in tables that are not owned by them. A malicious user with access to any user account that has this privilege can use this to gain access to sensitive data.

19.3.32 Logical Reads Per Session

Description: Ensure that users profile settings LOGICAL_READS_ PER_SESSION have appropriate value set for the particular database and application

Severity: Critical

Rationale: Allowing a single application or user to perform excessive amounts of reads to disk will result in a denial of service to the Oracle database

19.3.33 Limit Os Authentication

Description: Ensures database accounts does not rely on OS authentication

Severity: Critical

Rationale: If the host operating system has a required userid for database account for which password is set EXTERNAL, then Oracle does not check its credentials anymore. It simplyassumes the host must have done its authentication and lets the user into the database without any further checking.

19.3.34 Private Sga

Description: Ensure that users PRIVATE_SGA profile settings have appropriate values set for the particular database and application

Severity: Critical

Rationale: Allowing a single application or user to consume the excessive amounts of the System Global Area will result in a denial of service to the Oracle database

19.3.35 Password Reuse Max

Description: Ensures that all profiles have PASSWORD_REUSE_MAX set to a reasonable number of times

Severity: Warning

Rationale: Old passwords are usually the best guesses for the current password. A low value for the PASSWORD_REUSE_MAX parameter may cause serious database security issues by allowing users to reuse their old passwords more often.

19.3.36 Password Reuse Time

Description: Ensures that all profiles have PASSWORD_REUSE_TIME set to a reasonable number of days

Severity: Critical

Rationale: A low value for the PASSWORD_REUSE_TIME parameter may cause serious database security issues by allowing users to reuse their old passwords more often.

19.3.37 Proxy Account

Description: Ensures that the proxy accounts have limited privileges

Severity: Warning

Rationale: The proxy user only needs to connect to the database. Once connected it will use the privileges of the user it is connecting on behalf of. Granting any other privilege than the CREATE SESSION privilege to the proxy user is unnecessary and open to misuse.

19.3.38 Sessions_Per_User

Description: Ensures that all profiles have SESSIONS_PER_USER set to a reasonable number

Severity: Critical

Rationale: Allowing an unlimited amount of sessions per user can consume Oracle resources and cause a denial of service. Limit the number of session for each individual user

19.3.39 System Privileges To Public

Description: Ensure system privileges are not granted to PUBLIC

Severity: Critical

Rationale: Privileges granted to the public role automatically apply to all users. There are security risks granting SYSTEM privileges to all users.

19.3.40 Unlimited Tablespace Quota

Description: Ensures database users are allocated a limited tablespace quota

Severity: Warning

Rationale: Granting unlimited tablespace quotas can cause the filling up of the allocated disk space. This can lead to an unresponsive database.

19.4 Storage Best Practices For Oracle Database

The compliance rules for the Storage Best Practices For Oracle Database standard follow.

19.4.1 Dictionary Managed Tablespaces

Description: Checks for dictionary managed tablespaces

Severity: Minor Warning

Rationale: These tablespaces are dictionary managed. Oracle recommends using locally managed tablespaces, with AUTO segment-space management, to enhance performance and ease of space management.

19.4.2 Non-System Data Segments In System Tablespaces

Description: Checks for data segments owned by non-system users located in tablespaces SYSTEM, SYSAUX and SYSEXT.

Severity: Minor Warning

Rationale: These segments belonging to non-system users are stored in system tablespaces SYSTEM or SYSAUX or SYSEXT. This violation makes it more difficult to manage these data segments and may result in performance degradation in the system tablespace. This is also a security issue. If non-system users are storing data in a system tablespace it is possible that all available space in the system tablespace may be consumed, thus causing the database to stop working.

19.4.3 Non-System Users With System Tablespace As Default Tablespace

Description: Checks for non-system users using SYSTEM or SYSAUX as the default tablespace

Severity: Minor Warning

Rationale: These non-system users use a system tablespace as the default tablespace. This violation will result in non-system data segments being added to the system tablespace, making it more difficult to manage these data segments and possibly resulting in performance degradation in the system tablespace. This is also a security issue. All Available space in the system tablespace may beconsumed, thus causing the database to stop working.

19.4.4 Non-Uniform Default Extent Size For Tablespaces

Description: Checks for dictionary managed or migrated locally managed tablespaces with non-uniform default extent size

Severity: Minor Warning

Rationale: Dictionary managed or migrated locally managed tablespaces using non-uniform default extent sizes have been found. This means that the extents in a single tablespace will vary insize leading to fragmentation, inefficient space usage and performance degradation.

19.4.5 Tablespace Not Using Automatic Segment-Space Management

Description: Checks for locally managed tablespaces that are using MANUAL segment space management

Severity: Minor Warning

Rationale: Automatic segment-space management is a simpler and more efficient way of managing space within a segment. It completely eliminates any need to specify and tune the PCTUSED, FREELISTS and FREELIST GROUPS storage parameters for schema objects created in the tablespace. In a RAC environment there is the additional benefit of avoiding the hard partitioning of space inherent with using free list groups.

19.4.6 Users With Permanent Tablespace As Temporary Tablespace

Description: Checks for users using a permanent tablespace as the temporary tablespace

Severity: Minor Warning

Rationale: These users use a permanent tablespace as the temporary tablespace. Using temporary tablespaces allows space management for sort operations to be more efficient. Using a permanent tablespace for these operations may result in performance degradation, especially for Real Application Clusters. There is an additional security concern. This makes it possible for users to use all available space in the system tablespace, causing the database to stop working.

20

Siebel Enterprise Compliance Standards

These are the compliance rules for the Siebel Enterprise compliance standards

20.1 Target Sync Info For Siebel

The compliance rules for the Target Sync Info For Siebel standard follow.

20.1.1 Siebel Target Properties Out Of Sync

Description: Ensure that the siebel target properties are same in EM and actual siebel setup.

Severity: Warning

Rationale: Some of the target properties present on the siebel setup may be different in EM.

20.1.2 Siebel Targets Out Of Sync

Description: Ensure that the siebel target info is same in EM and actual siebel topology reported by the gateway server.

Severity: Warning

Rationale: Some of the targets present on the siebel topology may not be monitored in EM.

21

Systems Infrastructure Switch Compliance Standards

These are the compliance rules for the Systems Infrastructure Switch compliance standards

21.1 Orachk Systems Infrastructure Switch Best Practices For Oracle Exadata Database Machine

The compliance rules for the Orachk Systems Infrastructure Switch Best Practices For Oracle Exadata Database Machine standard follow.

21.1.1 Exadata Critical Issue Ib1-Ib3

Description: Exadata Critical Issue IB1-IB3

Severity: Critical

Rationale:

21.1.2 Exadata Software Version Compatibility With Infiniband Software Version

Description: Exadata software version compatibility with infiniband software version

Severity: Critical

Rationale:

21.1.3 Exadata Software Version Compatibility With Infiniband Software Version

Description: Exadata software version compatibility with infiniband software version

Severity: Critical

Rationale:

21.1.4 Hostname In /Etc/Hosts

Description: The Impact of verifying that the InfiniBand switch name is properly configured in the /etc/host file is minimal. To correct a mis-configuration requires editing the /etc/hosts file and rebooting the InfiniBand switch.

Severity: Warning

Rationale: If the InfiniBand Switch name is not properly configured in the /etc/hosts file, certain switch connection methods may fail.

21.1.5 Infiniband Switch Ntp Configuration

Description: Synchronized timestamps are important to switch operation and message logging, both within an InfiniBand switch between the InfiniBand switches. There is little impact to correctly configure the switches.

Severity: Warning

Rationale: If the InfiniBand switches are not correctly configured, there is a risk of improper operation and disjoint message timestamping.

21.1.6 Infiniband Subnet Manager Status

Description: Enable SM on a limited number of switches as follows:-1 rack to 4 racks - SM enabled on all (service opensmd status should show it as running)4 racks and above - SM enabled only on the spine switches (On other switches,run disablesm to disable the SM and service opensmd status should show it is not running)

Severity: Warning

Rationale:

21.1.7 Infiniband Subnet Manager Status For Spine

Description: Enable SM on a limited number of switches as follows:-1 rack to 4 racks - SM enabled on all (service opensmd status should show it as running)4 racks and above - SM enabled only on the spine switches (On other switches,run disablesm to disable the SM and service opensmd status should show it is not running)

Severity: Warning

Rationale:

21.1.8 Infiniband Subnet Manager Status On Leaf

Description: Enable SM on a limited number of switches as follows:-1 rack to 4 racks - SM enabled on all (service opensmd status should show it as running)4 racks and above - SM enabled only on the spine switches (On other switches,run disablesm to disable the SM and service opensmd status should show it is not running)

Severity: Warning

Rationale:

21.1.9 Infiniband Switch Hostname Configuration

Description: Infiniband switch HOSTNAME configuration

Severity: Warning

Rationale:

21.1.10 Infiniband Switch Controlled_Handover Configuration

Description: The Impact of verifying key parameters in the InfiniBand switch /etc/opensm/opensm.conf file is minimal. To correct a mis-configuration requires editing the /etc/opensm/opensm.conf file and rebooting the InfiniBand switch.

Severity: Warning

Rationale: If key parameters in the InfiniBand switch /etc/opensm/opensm.conf file are not correct, the InfiniBand switch may be unstable or performance may be sub-optimal.

21.1.11 Infiniband Switch Log_Flags Configuration

Description: The Impact of verifying key parameters in the InfiniBand switch /etc/opensm/opensm.conf file is minimal. To correct a mis-configuration requires editing the /etc/opensm/opensm.conf file and rebooting the InfiniBand switch.

Severity: Warning

Rationale: If key parameters in the InfiniBand switch /etc/opensm/opensm.conf file are not correct, the InfiniBand switch may be unstable or performance may be sub-optimal.

21.1.12 Infiniband Switch Polling_Retry_Number Configuration

Description: The Impact of verifying key parameters in the InfiniBand switch /etc/opensm/opensm.conf file is minimal. To correct a mis-configuration requires editing the /etc/opensm/opensm.conf file and rebooting the InfiniBand switch.

Severity: Warning

Rationale: If key parameters in the InfiniBand switch /etc/opensm/opensm.conf file are not correct, the InfiniBand switch may be unstable or performance may be sub-optimal.

21.1.13 Infiniband Switch Polling_Retry_Number Configuration

Description: The Impact of verifying key parameters in the InfiniBand switch /etc/opensm/opensm.conf file is minimal. To correct a mis-configuration requires editing the /etc/opensm/opensm.conf file and rebooting the InfiniBand switch.

Severity: Warning

Rationale: If key parameters in the InfiniBand switch /etc/opensm/opensm.conf file are not correct, the InfiniBand switch may be unstable or performance may be sub-optimal.

21.1.14 Infiniband Switch Routing_Engine Configuration

Description: The Impact of verifying key parameters in the InfiniBand switch /etc/opensm/opensm.conf file is minimal. To correct a mis-configuration requires editing the /etc/opensm/opensm.conf file and rebooting the InfiniBand switch.

Severity: Warning

Rationale: If key parameters in the InfiniBand switch /etc/opensm/opensm.conf file are not correct, the InfiniBand switch may be unstable or performance may be sub-optimal.

21.1.15 Infiniband Switch Sminfo_Polling_Timeout Configuration

Description: The Impact of verifying key parameters in the InfiniBand switch /etc/opensm/opensm.conf file is minimal. To correct a mis-configuration requires editing the /etc/opensm/opensm.conf file and rebooting the InfiniBand switch.

Severity: Warning

Rationale: If key parameters in the InfiniBand switch /etc/opensm/opensm.conf file are not correct, the InfiniBand switch may be unstable or performance may be sub-optimal.

21.1.16 Infiniband Switch Sminfo_Polling_Timeout Configuration

Description: The Impact of verifying key parameters in the InfiniBand switch /etc/opensm/opensm.conf file is minimal. To correct a mis-configuration requires editing the /etc/opensm/opensm.conf file and rebooting the InfiniBand switch.

Severity: Warning

Rationale: If key parameters in the InfiniBand switch /etc/opensm/opensm.conf file are not correct, the InfiniBand switch may be unstable or performance may be sub-optimal.

21.1.17 Is Orachk Configured

Description: Verify whether ORAchk is configured for this target.

Severity: Warning

Rationale: ORAchk must be configured before associating compliance content. Else, ORAchk results will not be available for compliance evaluation.

21.1.18 Switch Firmware Version

Description: The Impact of verifying that the InfiniBand switch software is at version 1.3.3-2 or higher is minimal. The impact of upgrading the InfiniBand switch(s) to 1.3.3-2 varies depending upon the upgrade method chosen and your current InfiniBand switch software level.

Severity: Critical

Rationale: InfiniBand switch software version 1.3.3-2 fixes several potential InfiniBand fabric stability issues. Remaining on an InfiniBand switch software version below 1.3.3-2 raises the risk of experiencing a potential outage.

21.1.19 Verify Average Ping Times To Dns Nameserver [Ib Switch]

Description: Secure Shell (SSH) remote login procedures require communication between the remote target device and the DNS nameserver. Minimal average ping times to the DNS nameserver improve SSH login times and help to avoid problems such as timeouts or failed connection attempts.The impact of verifying average ping times to the DNS nameserver is minimal. The impact required to minimize average ping times to the DNS nameserver varies by configuration and cannot be estimated here.

Severity: Warning

Rationale: Long ping times between remote SSH targets and the active DNS server may cause remote login failures, performance issues, or dropped application connections.

21.1.20 Verify No Ib Switch Ports Disabled Due To Excessive Symbol Errors

Description: Notification of a disabled port enables quick repair and redundancy restoration.

Severity: Critical

Rationale: Quick repair from a disabled port ensures the node will not be inaccessible if a secondary IB failure occurs (ie remaining ports fails or down due to switch reboot).

21.1.21 Verify Switch Localtime Configuration Across Switches

Description: Verify switch localtime configuration across switches

Severity: Critical

Rationale:

21.1.22 Verify Switch Version Consistency Across Switches

Description: Verify switch version consistency across switches

Severity: Critical

Rationale:

21.1.23 Sm_Priority Configuration On Infiniband Switch

Description: Configure SM failover timeout at 5 seconds, controlled_handover to TRUE, sm_priority to 5(8 for spine switch) and log_max_size to 8 which is the correct opensm configuration for the Infiniband Switch

Severity: Warning

Rationale: These are recommended values for the Infiniband Switch for best practices for sm_priority

21.2 Orachk Systems Infrastructure Switch Best Practices For Recovery Appliance

The compliance rules for the Orachk Systems Infrastructure Switch Best Practices For Recovery Appliance standard follow.

21.2.1 Exadata Software Version Compatibility With Infiniband Software Version

Description: Exadata software version compatibility with infiniband software version

Severity: Critical

Rationale:

21.2.2 Exadata Software Version Compatibility With Infiniband Software Version

Description: Exadata software version compatibility with infiniband software version

Severity: Critical

Rationale:

21.2.3 Infiniband Switch Ntp Configuration

Description: Synchronized timestamps are important to switch operation and message logging, both within an InfiniBand switch between the InfiniBand switches. There is little impact to correctly configure the switches.

Severity: Warning

Rationale: If the InfiniBand switches are not correctly configured, there is a risk of improper operation and disjoint message timestamping.

21.2.4 Infiniband Subnet Manager Status

Description: Enable SM on a limited number of switches as follows:-1 rack to 4 racks - SM enabled on all (service opensmd status should show it as running)4 racks and above - SM enabled only on the spine switches (On other switches,run disablesm to disable the SM and service opensmd status should show it is not running)

Severity: Warning

Rationale:

21.2.5 Infiniband Subnet Manager Status For Spine

Description: Enable SM on a limited number of switches as follows:-1 rack to 4 racks - SM enabled on all (service opensmd status should show it as running)4 racks and above - SM enabled only on the spine switches (On other switches,run disablesm to disable the SM and service opensmd status should show it is not running)

Severity: Warning

Rationale:

21.2.6 Infiniband Subnet Manager Status On Leaf

Description: Enable SM on a limited number of switches as follows:-1 rack to 4 racks - SM enabled on all (service opensmd status should show it as running)4 racks and above - SM enabled only on the spine switches (On other switches,run disablesm to disable the SM and service opensmd status should show it is not running)

Severity: Warning

Rationale:

21.2.7 Infiniband Switch Hostname Configuration

Description: Infiniband switch HOSTNAME configuration

Severity: Warning

Rationale:

21.2.8 Infiniband Switch Controlled_Handover Configuration

Description: The Impact of verifying key parameters in the InfiniBand switch /etc/opensm/opensm.conf file is minimal. To correct a mis-configuration requires editing the /etc/opensm/opensm.conf file and rebooting the InfiniBand switch.

Severity: Warning

Rationale: If key parameters in the InfiniBand switch /etc/opensm/opensm.conf file are not correct, the InfiniBand switch may be unstable or performance may be sub-optimal.

21.2.9 Infiniband Switch Log_Flags Configuration

Description: The Impact of verifying key parameters in the InfiniBand switch /etc/opensm/opensm.conf file is minimal. To correct a mis-configuration requires editing the /etc/opensm/opensm.conf file and rebooting the InfiniBand switch.

Severity: Warning

Rationale: If key parameters in the InfiniBand switch /etc/opensm/opensm.conf file are not correct, the InfiniBand switch may be unstable or performance may be sub-optimal.

21.2.10 Infiniband Switch Polling_Retry_Number Configuration

Description: The Impact of verifying key parameters in the InfiniBand switch /etc/opensm/opensm.conf file is minimal. To correct a mis-configuration requires editing the /etc/opensm/opensm.conf file and rebooting the InfiniBand switch.

Severity: Warning

Rationale: If key parameters in the InfiniBand switch /etc/opensm/opensm.conf file are not correct, the InfiniBand switch may be unstable or performance may be sub-optimal.

21.2.11 Infiniband Switch Polling_Retry_Number Configuration

Description: The Impact of verifying key parameters in the InfiniBand switch /etc/opensm/opensm.conf file is minimal. To correct a mis-configuration requires editing the /etc/opensm/opensm.conf file and rebooting the InfiniBand switch.

Severity: Warning

Rationale: If key parameters in the InfiniBand switch /etc/opensm/opensm.conf file are not correct, the InfiniBand switch may be unstable or performance may be sub-optimal.

21.2.12 Infiniband Switch Routing_Engine Configuration

Description: The Impact of verifying key parameters in the InfiniBand switch /etc/opensm/opensm.conf file is minimal. To correct a mis-configuration requires editing the /etc/opensm/opensm.conf file and rebooting the InfiniBand switch.

Severity: Warning

Rationale: If key parameters in the InfiniBand switch /etc/opensm/opensm.conf file are not correct, the InfiniBand switch may be unstable or performance may be sub-optimal.

21.2.13 Infiniband Switch Sminfo_Polling_Timeout Configuration

Description: The Impact of verifying key parameters in the InfiniBand switch /etc/opensm/opensm.conf file is minimal. To correct a mis-configuration requires editing the /etc/opensm/opensm.conf file and rebooting the InfiniBand switch.

Severity: Warning

Rationale: If key parameters in the InfiniBand switch /etc/opensm/opensm.conf file are not correct, the InfiniBand switch may be unstable or performance may be sub-optimal.

21.2.14 Infiniband Switch Sminfo_Polling_Timeout Configuration

Description: The Impact of verifying key parameters in the InfiniBand switch /etc/opensm/opensm.conf file is minimal. To correct a mis-configuration requires editing the /etc/opensm/opensm.conf file and rebooting the InfiniBand switch.

Severity: Warning

Rationale: If key parameters in the InfiniBand switch /etc/opensm/opensm.conf file are not correct, the InfiniBand switch may be unstable or performance may be sub-optimal.

21.2.15 Is Orachk Configured

Description: Verify whether ORAchk is configured for this target.

Severity: Warning

Rationale: ORAchk must be configured before associating compliance content. Else, ORAchk results will not be available for compliance evaluation.

21.2.16 Switch Firmware Version

Description: The Impact of verifying that the InfiniBand switch software is at version 1.3.3-2 or higher is minimal. The impact of upgrading the InfiniBand switch(s) to 1.3.3-2 varies depending upon the upgrade method chosen and your current InfiniBand switch software level.

Severity: Critical

Rationale: InfiniBand switch software version 1.3.3-2 fixes several potential InfiniBand fabric stability issues. Remaining on an InfiniBand switch software version below 1.3.3-2 raises the risk of experiencing a potential outage.

21.2.17 Verify Average Ping Times To Dns Nameserver [Ib Switch]

Description: Secure Shell (SSH) remote login procedures require communication between the remote target device and the DNS nameserver. Minimal average ping times to the DNS nameserver improve SSH login times and help to avoid problems such as timeouts or failed connection attempts.The impact of verifying average ping times to the DNS nameserver is minimal. The impact required to minimize average ping times to the DNS nameserver varies by configuration and cannot be estimated here.

Severity: Warning

Rationale: Long ping times between remote SSH targets and the active DNS server may cause remote login failures, performance issues, or dropped application connections.

21.2.18 Verify No Ib Switch Ports Disabled Due To Excessive Symbol Errors

Description: Notification of a disabled port enables quick repair and redundancy restoration.

Severity: Critical

Rationale: Quick repair from a disabled port ensures the node will not be inaccessible if a secondary IB failure occurs (ie remaining ports fails or down due to switch reboot).

21.2.19 Verify Switch Localtime Configuration Across Switches

Description: Verify switch localtime configuration across switches

Severity: Critical

Rationale:

21.2.20 Verify Switch Version Consistency Across Switches

Description: Verify switch version consistency across switches

Severity: Critical

Rationale:

21.2.21 Sm_Priority Configuration On Infiniband Switch

Description: Configure SM failover timeout at 5 seconds, controlled_handover to TRUE, sm_priority to 5(8 for spine switch) and log_max_size to 8 which is the correct opensm configuration for the Infiniband Switch

Severity: Warning

Rationale: These are recommended values for the Infiniband Switch for best practices for sm_priority

22

Security Technical Implementation Guides

This section explains how to use the Security Technical Implementation Guides (STIG) based compliance standards, as well as how to customize them to meet environmental-specific requirements.

22.1 About Security Technical Implementation Guides

In keeping with Oracle's commitment to provide a secure environment, Enterprise Manager supports an implementation in the form of compliance standards of several Security Technical Implementation Guides (STIG). A STIG is a set of rules, checklists, and other best practices created by the Defense Information Systems Agency (DISA) to ensure compliance with Department of Defense (DOD)-mandated security requirements.

The currently available STIG based compliance standards are:

- Security Technical Implementation Guide (STIG Version 1.8) for Oracle Database [Release 1.8]
- Security Technical Implementation Guide (STIG Version 1.8) for Oracle Cluster Database [Release 1.8]
- Security Technical Implementation Guide (STIG Version 8 Release 1.11) for Oracle Database
- Security Technical Implementation Guide (STIG Version 8 Release 1.11) for Oracle Cluster Database
- Oracle 12*c* Database STIG - Version 1, Release 3 for Oracle Database
- Oracle 12*c* Database STIG - Version 1, Release 3 for Oracle Cluster Database
- Oracle 11.2*g* Database STIG - Version 1, Release 6 for Oracle Database
- Oracle 11.2*g* Database STIG - Version 1, Release 6 for Oracle Cluster Database
- Security Technical Implementation Guide (STIG Version 1.1) for Oracle WebLogic Server 12c
- Security Technical Implementation Guide (STIG Version 1.2) for Oracle WebLogic Server 12c
- Security Technical Implementation Guide (STIG Version 1) for Oracle HTTP Server 12.1.3

For detailed information on STIGs, visit the Information Assurance Support Environment website: `http://iase.disa.mil/stigs/Pages/index.aspx`.

22.2 Associating STIG Compliance Standards Targets

To determine whether a database, WebLogic Domain satisfies STIG Compliance Standards, or other supported target type, you have to associate the database or WebLogic Domain target with the standards.

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Select the **Compliance Standards** tab and search for the STIG standard.
3. Select the appropriate standard and click **Associate Targets**. There are four target types, Oracle Database, Oracle Cluster Database, Oracle WebLogic Domain, and Oracle HTTP Server. For an Oracle HTTP Server (OHS) target type, both managed OHS and standalone OHS are supported. You can associate the OHS STIG standard to managed OHS targets as well as standalone OHS targets. Also, the OHS STIG standard is applicable to OHS release 12.1.3 target.
4. Click **Add** and select the database or WebLogic Domain targets you want to monitor. The targets appear in the table after you close the selector dialog.

   Note: The WebLogic Server STIG is applicable to WebLogic 12.1.3 domains that are JRF enabled.
5. Click **OK** then confirm that you want to save the association. The association internally deploys the configuration extension "STIG Configuration" to the appropriate Management Agents.
6. After deployment and subsequent configuration collection occurs, you can view the results. From the **Enterprise** menu, select **Compliance**, then select either **Dashboard** or **Results**.

22.3 Handling STIG Compliance Standards Violations

Relationship between monitoring templates, configuration collections and compliance:

Compliance standard rules in the STIG for WLS and Oracle HTTP Server compliance standard are of the type "Repository Rule". For those rules that are automated, this means that Enterprise Manager compares each rule against configuration items collected and stored in the management repository.

By default, WLS configuration items required for measuring compliance to this STIG for WLS compliance standard are enabled out of the box. However, administrators can choose to disable WLS configuration collection via the target's Metric and Collection Settings page or via Monitoring Templates. Disabling such collections could negatively impact Enterprise Manager's ability to measure compliance with the STIG for WLS 12c.

There are four options for handling STIG Compliance Standards:

- Fixing the Violation per the STIG Check Recommendation
- Clearing Manual Rule Violations
- Suppressing the Violation
- Customizing the Compliance Standard and Configuration Extension

22.3.1 Fixing the Violation per the STIG Check Recommendation

Address the violation by fixing the security configuration on the supported target types according to the STIG check recommendation.

1. From the **Enterprise** menu, select **Compliance**, then select **Results**.
2. Select the STIG Compliance Standards row and click **Manage Violations**.
3. Locate the rule violation row in the table and note the recommended fix in the far right column.

After making the change per the recommendation, refresh the database or WebLogic Domain configuration in Enterprise Manager. For example, for the database target:

1. Go to the database target home page.
2. From the database menu, select **Configuration**, then select **Last Collected**.
3. From the **Actions** menu on the right, select **Refresh**.
4. From the **Enterprise** menu, select **Compliance**, then select **Results**. Verify that the violation no longer appears for the database target.

22.3.2 Clearing Manual Rule Violations

Checks that cannot be automated are implemented as Manual Rules. These checks must be performed by the administrator following the procedure described in the rule description or in the STIG guide itself.

When compliance standards containing manual rules are first associated to a target, each manual rule will generate one violation. Administrators can then *clear* the violation after successfully completing the check. The user performing the operation, as well as a description of the operation, are recorded during the process. Users can also set an expiration date at which time the violation will be re-generated. This provides for periodic reassessment of compliance.

1. From the **Enterprise** menu, select **Compliance**, then select **Results**.
2. Select the STIG compliance Standard row, and click **Manage Violations**.
3. Select the **Manual Rule Violations** tab.
4. Select one or more rules and click **Clear Violations**.
5. Enter a reason and optionally an expiration date and click **OK**.

22.3.3 Suppressing the Violation

Suppressing a violation removes it from the compliance score calculation, as well as the results. Although suppressed, you can still create reports using the management views showing the suppressed violations.

Violations can be permanently or temporarily suppressed allowing for permanent exceptions or grace periods. If you choose to enter a date, the violation will re-appear on that date unless it has been cleared as a result of the underlying condition being corrected.

1. From the **Enterprise** menu, select **Compliance**, then select **Results**.
2. Select the STIG Compliance Standards row and click **Manage Violations**.
3. Select **Unsuppressed Violations**.
4. Select the rows listing the violations you want to suppress and click the **Suppress Violations** button.
5. In the dialog that opens, select Indefinite or select an expiration date. Optionally provide a reason for the suppression. Click **OK**.

22.3.4 Customizing the Compliance Standard and Configuration Extension

In some cases, the rule detecting the violation, while desirable in its intent, needs some fine-tuning to work in your environment. The STIG Compliance Standard allows you to view and customize the query that evaluates the compliance standard violation. The process involves the following tasks:

- Customizing the Configuration Extension
- Customizing the Compliance Standard Rule
- Creating a Compliance Standard to Include the Customized Rule

To illustrate the process, assume a scenario where you want to update the query for the database rule `DG0116 DBMS privileged role assignments`.

22.3.4.1 Customizing the Configuration Extension

To customize the STIG Configuration extension:

1. From the **Enterprise** menu, select **Configuration**, then select **Configuration Extensions**.
2. Select the appropriate STIG Configuration table row (database instance or cluster database) and click the **Create Like** button.
3. Provide a new name for the extension; for example, Custom STIG Configuration.
4. On the **Files & Commands** tab, select all the command rows and click **Delete**.
5. On the **SQL** tab, locate the rule alias DG0116 DBMS privileged role assignments. Delete all other rows above and below it.
6. Modify the query for DG0116 and rename the alias; for example, Custom DG0116 DBMS privileged role assignments.
7. Preview the results: select the sample target and click **Preview**.
8. If the violation no longer appears, save the Custom STIG Configuration Extension.

22.3.4.2 Customizing the Compliance Standard Rule

To customize the Compliance Standard rule:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Select the **Compliance Standard Rules** tab and search for rule `DG0116 DBMS privileged role assignments` with agent-side rule type.

3. Select the rule and click the **Create Like** button.
4. Change the name; for example, Custom DG0116 DBMS privileged role assignments. Click **Continue**.
5. On the Check Definition page, click the magnifying glass icon to select a new STIG Configuration Extension (Custom STIG Configuration Extension) and alias (Custom DG0116 DBMS privileged role assignments).
6. Select the custom configuration extension and alias and click **OK**, then click **Next** to go the Test page.
7. Select a target and test the compliance rule.
8. Click **Next**, then click **Finish** to create the new compliance rule.

22.3.4.3 Creating a Compliance Standard to Include the Customized Rule

To create a Compliance Standard with a new rule:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Select the **Compliance Standards** tab and search for STIG for database instance with agent-side rule type.
3. Select the compliance standard and click the **Create Like** button.
4. Change the name; for example, Custom Security Technical Implementation Guide. Click **Continue**.
5. Open the Oracle Database Check Procedures folder in the left pane and scroll down to DG0116 DBMS privileged role assignments.
6. Right-click the rule and select **Remove Rule Reference** from the pop-up menu. Click **OK** to confirm removal.
7. Right-click the Oracle Database Check Procedures folder and select **Add Rules** from the pop-up menu.
8. Locate the Custom DG0116 DBMS privileged role assignments row in the table and click **OK**.
9. On the Compliance Standard Create Like page, click the **Save** button to create the new compliance standard.

You can now associate the custom compliance standard with target databases as described in Associating STIG Compliance Standards Targets.

22.4 STIG Compliance Standard Rules Exceptions

The Enterprise Manager implementation of Security Technical Implementation Guide has some exceptions. The following sections list these exceptions:

- Windows Databases
- Oracle WebLogic Domains
- Oracle HTTP Server

22.4.1 Windows Databases

The Enterprise Manager implementation of Security Technical Implementation Guide for Oracle Database does not fully support Windows databases. The following rules do not report violations on Windows databases:

DG0009 DBMS software library permissions
DG0019 DBMS software ownership
DG0012 DBMS software storage location
DG0102 DBMS services dedicated custom account
DO0120 Oracle process account host system privileges
DO0145 Oracle SYSDBA OS group membership
DG0152 DBMS network port, protocol and services (PPS) use
DG0179 DBMS warning banner
DO0286 Oracle connection timeout parameter
DO0287 Oracle SQLNET.EXPIRE_TIME parameter
DO6740 Oracle listener ADMIN_RESTRICTIONS parameter
DO6746 Oracle Listener host references
DO6751 SQLNET.ALLOWED_LOGON_VERSION

22.4.2 Oracle WebLogic Domains

The Enterprise Manager implementation of Security Technical Implementation Guide (STIG Version 1.1) and Security Technical Implementation Guide (STIG Version 1.2) for Oracle WebLogic Server 12*c* is not fully automated.

The following rules will always report violations and need to be verified manually:

WBLC-01-000013 WebLogic audit security-relevant information
WBLC-01-000014 WebLogic disable network protocols
WBLC-01-000018 WebLogic audit account creation
WBLC-01-000019 WebLogic audit account modification
WBLC-01-000030 WebLogic log privileged activity
WBLC-01-000032 WebLogic invalid consecutive access attempts
WBLC-01-000033 WebLogic user invalid access attempts
WBLC-01-000034 WebLogic lock user account
WBLC-02-000069 WebLogic log DoD-selected audit records
WBLC-02-000073 WebLogic log HTTPD event
WBLC-02-000074 WebLogic log JVM event
WBLC-02-000075 WebLogic log severity level
WBLC-02-000083 WebLogic alert audit failure events
WBLC-02-000084 WebLogic alert audit processing failure
WBLC-02-000086 WebLogic notify audit processing failure
WBLC-02-000093 WebLogic use system clock for audit records
WBLC-02-000094 WebLogic synchronize system clocks
WBLC-02-000095 WebLogic protect unauthorized audit information read access
WBLC-02-000098 WebLogic protect unauthorized audit tools access
WBLC-02-000099 WebLogic protect unauthorized audit tools modification
WBLC-02-000100 WebLogic protect unauthorized audit tools deletion
WBLC-03-000125 WebLogic limit privileges to software libraries
WBLC-03-000127 WebLogic enable essential capabilities

WBLC-03-000128 WebLogic restrict use of unauthorized items
WBLC-05-000150 WebLogic identify and authenticate users
WBLC-05-000153 WebLogic authenticate users individually
WBLC-05-000168 WebLogic encrypt password for authentication
WBLC-05-000169 WebLogic LDAP encryption for authentication
WBLC-05-000174 WebLogic PKI-based authentication for user accounts
WBLC-05-000176 WebLogic FIPS-compliant encryption for configuration
WBLC-05-000177 WebLogic FIPS-compliant encryption for users and processes
WBLC-08-000214 WebLogic NSA-approved cryptography classified compartmentalized
WBLC-08-000218 WebLogic public information protection
WBLC-08-000222 WebLogic hosted application separation
WBLC-08-000236 WebLogic Denial of Service
WBLC-08-000237 WebLogic prioritize resources
WBLC-08-000238 WebLogic secure failure
WBLC-09-000252 WebLogic security-relevant error
WBLC-09-000253 WebLogic log messages corrective action
WBLC-09-000254 WebLogic log messages limited access
WBLC-09-000257 WebLogic notifications to response personnel
WBLC-10-000270 WebLogic audit subsystem failure notification
WBLC-10-000271 WebLogic centralized enterprise tool
WBLC-10-000272 WebLogic multi-factor user authentication

22.4.3 Oracle HTTP Server

The Enterprise Manager implementation of the Security Technical Implementation Guide (STIG Version 1) for Oracle HTTP Server 12.1.3 is not fully automated.

The following rules will always report violations and need to be verified manually:

OH12-1X-000225 Symbolic links not used in web content directory tree
OH12-1X-000226 OHS secure administration
OH12-1X-000266 OHS Accounts Verification

Enterprise Manager's compliance standard for STIG Version 1 for OHS 12.1.3 includes CAT I level rules from the DISA published STIG Version 1 for OHS 12.1.3. CAT II and CAT III rules are not included in the compliance standard and must consequently be tracked outside of Enterprise Manager Cloud Control. For a complete list of all rules in the DISA published STIG Version 1 for OHS 12.1.3, refer to http://iase.disa.mil/stigs/app-security/web-servers/Pages/index.aspx.

22.5 Oracle Database STIG Compliance Standard Modifications from Guide

The Enterprise Manager implementations of the Oracle Database 11g STIGs and 12c STIGs deviate slightly from the checklist. These modifications include error corrections, enhancements to the check (i.e. additional default users) or automated scripts where manual checks may have been specified. It is important that you review and understand the modifications to ensure they are acceptable in your environment. If not, follow the previously discussed customization procedures in order to match your requirements. For detailed information on these changes, see Security Technical Implementation Guidelines (STIG) Rules Enhanced by Oracle .

Note:

There are no modifications or deviations for the Security Technical Implementation Guide (STIG Version 1.1) for Oracle WebLogic Server 12*c*, Security Technical Implementation Guide (STIG Version 1.2) for Oracle WebLogic Server 12c, and Security Technical Implementation Guide (STIG Version 1) for Oracle HTTP Server 12.1.3 compliance standard.

Table 22-1 Deviations from Oracle Database 12c, Version 1, Release 3 STIGS

STIG ID	Oracle Modification
SV-75899r1_rule	Combined the rule queries to check if audit is enabled by means of either Traditional or Unified system. Need to manually check if audit data is retained for at least one year.
SV-75903r1_rule	Provided an even more specific query to check if instance name contains version number.
SV-75905r1_rule	Combined the rule queries to return db_link as violations only if dba_repcatalog has records.
SV-75907r1_rule	Need to manually check if each file is located on a separate RAID device.
SV-75909r1_rule	Used the more stricter query to get the violation. Need to manually check if a RAID device is used.
SV-75923r1_rule	Added default users/roles to the query - 'APEX_030200', 'APEX_040200', 'DVSYS', 'SYSKM', and 'DV_ACCTMGR'.
SV-75927r1_rule	Added default users/roles to the query: 'DBA', 'DV_ACCTMGR', 'DV_OWNER', 'RECOVERY_CATALOG_OWNER', 'SPATIAL_CSW_ADMIN_USR', and 'SPATIAL_WFS_ADMIN_USR'.
SV-75931r2_rule	Script provided by Oracle.
SV-75937r2_rule	Script provided by Oracle.
SV-75945r1_rule	Added a query to check whether privilege analysis policy is defined/run to analyze non-required application user privilege assignment.
SV-75947r1_rule	Combined the rule queries to check if audit is enabled by means of either Traditional or Unified system.
SV-75951r1_rule	Changed the query to include demo accounts - 'HR', 'OE', 'PM', 'IX', 'SH', and 'SCOTT'.
SV-75953r1_rule	Script provided by Oracle.
SV-75957r1_rule	Changed the query to include more default users/roles which are not in the list.
SV-76001r1_rule	Script provided by Oracle.
SV-76017r1_rule	Combined rule queries.

Table 22-1 (Cont.) Deviations from Oracle Database 12c, Version 1, Release 3 STIGS

STIG ID	Oracle Modification
SV-76021r2_rule	Script provided by Oracle.
SV-76023r1_rule	Script provided by Oracle.
SV-76025r1_rule	Script provided by Oracle.
SV-76035r1_rule	Script provided by Oracle.
SV-76037r1_rule	Script provided by Oracle.
SV-76039r1_rule	Script provided by Oracle.
SV-76041r1_rule	Script provided by Oracle.
SV-76043r1_rule	Combined rule queries to check if audit is enabled by means of either Traditional or Unified system. Need to manually check if remote sessions that are accessing security information are being audited.
SV-76045r1_rule	Script provided by Oracle.
SV-76051r1_rule	A query added by Oracle.
SV-76053r1_rule	A query added by Oracle.
SV-76055r1_rule	Combined rule queries to check if audit is enabled by means of either Traditional or Unified system and to check if account creation is being audited.
SV-76059r1_rule	Combined rule queries to check if audit is enabled by means of either Traditional or Unified system and to check if account modification is being audited.
SV-76061r1_rule	Combined rule queries to check if audit is enabled by means of either Traditional or Unified system. Need to manually check if account disabling is being audited.
SV-76063r1_rule	Combined rule queries to check if audit is enabled by means of either Traditional or Unified system and to check if account termination is being audited.
SV-76081r1_rule	A query added by Oracle.
SV-76085r1_rule	Combined rule queries to check if audit is enabled by means of either Traditional or Unified system. Need to manually check if all use of privileged accounts are audited.
SV-76093r1_rule	A query added by Oracle.
SV-76095r1_rule	A query added by Oracle.
SV-76097r1_rule	A query added by Oracle.
SV-76099r1_rule	Script provided by Oracle.
SV-76101r1_rule	Script provided by Oracle.

Table 22-1 (Cont.) Deviations from Oracle Database 12c, Version 1, Release 3 STIGS

STIG ID	Oracle Modification
SV-76103r1_rule	A query added by Oracle.
SV-76105r1_rule	A query added by Oracle.
SV-76111r1_rule	Combined rule queries to check if audit is enabled by means of either Traditional or Unified system.
SV-76115r1_rule	Combined rule queries to check if audit is enabled by means of either Traditional or Unified system.
SV-76117r1_rule	Combined rule queries to check if audit is enabled by means of either Traditional or Unified system.
SV-76121r1_rule	Combined rule queries to check if audit is enabled by means of either Traditional or Unified system.
SV-76123r1_rule	Combined rule queries to check if audit is enabled by means of either Traditional or Unified system.
SV-76125r1_rule	Combined rule queries to check if audit is enabled by means of either Traditional or Unified system.
SV-76127r1_rule	Combined rule queries to check if audit is enabled by means of either Traditional or Unified system.
SV-76129r1_rule	Combined rule queries to check if audit is enabled by means of either Traditional or Unified system.
SV-76131r1_rule	Combined rule queries to check if audit is enabled by means of either Traditional or Unified system.
SV-76143r2_rule	A query added by Oracle.
SV-76145r1_rule	A query added by Oracle.
SV-76147r1_rule	A query added by Oracle.
SV-76157r1_rule	A query added by Oracle.
SV-76159r1_rule	Combined rule queries to check if audit records are being protected.
SV-76161r1_rule	Script provided by Oracle.
SV-76163r1_rule	A query added by Oracle.
SV-76167r1_rule	A query added by Oracle.
SV-76173r1_rule	Made to be operated manually as query cannot be executed successfully because of special characters being added.
SV-76175r1_rule	Script provided by Oracle.
SV-76181r1_rule	A query added by Oracle.
SV-76193r1_rule	Script provided by Oracle.

Table 22-1 (Cont.) Deviations from Oracle Database 12c, Version 1, Release 3 STIGS

STIG ID	Oracle Modification
SV-76195r1_rule	Script provided by Oracle.
SV-76197r1_rule	Script provided by Oracle.
SV-76199r1_rule	Script provided by Oracle.
SV-76203r1_rule	Script provided by Oracle.
SV-76205r1_rule	Script provided by Oracle.
SV-76207r1_rule	A query added by Oracle.
SV-76209r1_rule	A query added by Oracle.
SV-76211r2_rule	A query added by Oracle.
SV-76213r1_rule	A query added by Oracle.
SV-76215r1_rule	A query added by Oracle.
SV-76217r1_rule	A query added by Oracle.
SV-76219r1_rule	A query added by Oracle.
SV-76221r1_rule	A query added by Oracle.
SV-76229r1_rule	A query added by Oracle.
SV-76237r1_rule	Script provided by Oracle.
SV-76245r1_rule	A query added by Oracle.
SV-76247r2_rule	A query added by Oracle.
SV-76249r1_rule	Script provided by Oracle.
SV-76251r1_rule	A query added by Oracle.
SV-76253r1_rule	A query added by Oracle.
SV-76255r1_rule	A query added by Oracle.
SV-76257r1_rule	A query added by Oracle.
SV-76261r1_rule	Modified the query to exclude -'SYSTEM', 'SYSAUX', 'UD1', 'TEMP', 'SYSEXT', and 'UNDOTBS'.
SV-76263r1_rule	Modified the query to exclude -'SYSTEM', 'SYSAUX', 'UD1', 'TEMP', 'SYSEXT', and 'UNDOTBS'.
SV-76275r1_rule	A query added by Oracle.
SV-76287r2_rule	Combined to check if audit is enabled by means of either Traditional or Unified system and to check if account creation is being audited. Need to manually check if they are being notified.

Table 22-1 (Cont.) Deviations from Oracle Database 12c, Version 1, Release 3 STIGS

STIG ID	Oracle Modification
SV-76289r2_rule	Combined to check if audit is enabled by means of either Traditional or Unified system and to check if account modification is being audited. Need to manually check if it is notified.
SV-76291r2_rule	Combined to check if audit is enabled by means of either Traditional or Unified system and to check if account disabling is being audited. Need to manually check if it is notified.
SV-76293r2_rule	Combined to check if audit is enabled by means of either Traditional or Unified system and to check if account termination is being audited. Need to manually check if it is notified.
SV-76299r1_rule	Changed query to exclude oracle default users/roles.
SV-76301r1_rule	Script provided by Oracle.
SV-76307r1_rule	A query added by Oracle.
SV-76309r1_rule	A query added by Oracle.
SV-76339r1_rule	A query added by Oracle.
SV-76365r1_rule	Script provided by Oracle.
SV-76377r1_rule	A query added by Oracle.
SV-76455r1_rule	Script provided by Oracle.
SV-76457r1_rule	A query added by Oracle.

Table 22-2 Deviations from Oracle Database 11g, V8, R8, and R11 STIGS

STIG ID	Oracle Modification
DG0008	Added Default Users/Roles
DG0009	Script provided by Oracle
DG0012	Script provided by Oracle
DG0019	Script provided by Oracle
DG0077	Added Default Users/Roles
DG0079	Incorrect query. Replaced NULL with string 'NULL'.
DG0091	Added Default Users
DG0102	Script provided by Oracle
DG0116	Added Default Users

Table 22-2 (Cont.) Deviations from Oracle Database 11g, V8, R8, and R11 STIGS

STIG ID	Oracle Modification
DG0117	Added Default Users
DG0119	Added Default Users
DG0121	Added Default Users
DG0123	Added Default Users
DG0152	Script Provided by Oracle
DG0179	Script Provided by Oracle
DO0120	Script Provided by Oracle
DO0145	Script Provided by Oracle
DO0155	Added Default Users
DO0221	Used default instance name as orcl.
DO0231	Added Default Users
DO0250	Combined the rule queries to return db_link as violations only if dba_repcatalog has records
DO0270	Used stricter query to get the violations
DO0286	Script Provided by Oracle
DO0287	Script Provided by Oracle
DO0340	Added Default Users
DO0350	Added Default Users/Roles
DO3536	Combined the queries. De-referenced the DEFAULT value for the limit.
DO3609	Added Default Users/Roles
DO3689	Added Default Users/Roles
DO6740	Script Provided by Oracle
DO6746	Script Provided by Oracle

Table 22-3 Deviations from Oracle Database 11gR2, V1, Release 2 STIG

STIG ID	Oracle Modification
SV-66381r1_rule	Query implemented by Oracle. Discounted default users.
SV-66395r1_rule	Added 'SYSTEM' and 'DELETE_CATALOG_ROLE' as filters.
SV-66401r1_rule	Fixed table name in query. Added privilege to be checked. Discounted Default Users.

Table 22-3 (Cont.) Deviations from Oracle Database 11gR2, V1, Release 2 STIG

STIG ID	Oracle Modification
SV-66405r1_rule	Fixed table name in query. Added privilege to be checked. Discounted Default Users.
SV-66419r1_rule	STIG document has incorrect query. Prepared a new query for the rule. Discounted default users.
SV-66427r1_rule	Combined the 3 conditions into 1. The query raises a violation if: **1.** audit_trail parameter is set to none. **2.** audit_trail is not set to none and table_space is not encrypted.
SV-66439r1_rule	Discounted default users.
SV-66441r1_rule	Dereferenced default profile.
SV-66459r1_rule	Rule checks the database archive log mode from repository table instead of using the "archive log list" command.
SV-66485r1_rule	Query provided by Oracle. Used limit=35 from the Fix Text.
SV-66489r1_rule	Query provided by Oracle. Used limit=6 from the Fix Text.
SV-66507r1_rule	Dereferenced default profile.
SV-66553r1_rule	Query provided by Oracle.
SV-66571r1_rule	Query provided by Oracle. Used limit=35 from the Fix Text.
SV-66599r1_rule	Query provided by Oracle. Discounted default users.
SV-66623r1_rule	Query provided by Oracle. Discounted default users.
SV-66627r1_rule	Discounted default users.
SV-66647r1_rule	Joined queries from document. Discounted default users.
SV-66651r1_rule	Joined queries from document. Discounted default users.
SV-66657r1_rule	Script provided by Oracle
SV-66663r1_rule	Added check for SYSTEM tablespace.
SV-66665r1_rule	Added check for SYSTEM tablespace.
SV-66669r1_rule	This rule always passes for Oracle.
SV-66673r1_rule	This rule always passes for Oracle.
SV-68205r1_rule	User should manually discount db_links used for replication.
SV-68229r1_rule	Added default users.
SV-68233r1_rule	Additional column selected in query for better violation context.

Table 22-3 (Cont.) Deviations from Oracle Database 11gR2, V1, Release 2 STIG

STIG ID	Oracle Modification
SV-68235r1_rule	Added default users.
SV-68241r1_rule	Additional column selected in query for better violation context.
SV-68249r1_rule	Added default users.
SV-68257r1_rule	Added default users.
SV-68283r1_rule	Script provided by Oracle.
SV-66431r1_rule	Use v$parameter in query instead of sys.v$parameter.

22.6 Oracle WebLogic STIG Compliance Standard

The Enterprise Manager implementation of the Security Technical Implementation Guide (STIG Version 1.1) for Oracle WebLogic Server 12c and Security Technical Implementation Guide (STIG Version 1.2) for Oracle WebLogic Server 12c contains automated rules. These rules check for WebLogic configuration settings and generate violations. It is important that you review and understand implemented rules to ensure they are acceptable in your environment.

Enterprise Manager's compliance standard for STIG Version 1 for OHS 12.1.3 includes CAT I level rules from the DISA published STIG Version 1 for OHS 12.1.3. CAT II and CAT III rules are not included in the compliance standard and must consequently be tracked outside of Enterprise Manager Cloud Control. For a complete list of all rules in the DISA published STIG Version 1 for OHS 12.1.3, refer to http://iase.disa.mil/stigs/app-security/web-servers/Pages/index.aspx.

WBLC-01-000009 WebLogic cryptography for remote management session
WBLC-01-000010 WebLogic cryptography for remote session
WBLC-01-000011 WebLogic monitor and control remote session
WBLC-02-000062 WebLogic log particular user action
WBLC-02-000065 WebLogic log multiple components audit records
WBLC-02-000076 WebLogic log event time
WBLC-02-000077 WebLogic log event cause
WBLC-02-000078 WebLogic log process sources
WBLC-02-000079 WebLogic log outcome indicators
WBLC-02-000080 WebLogic log identity information
WBLC-02-000081 WebLogic log audit record content
WBLC-03-000129 WebLogic prevent program execution
WBLC-05-000160 WebLogic password use minimum password length
WBLC-05-000162 WebLogic password use upper case characters
WBLC-05-000163 WebLogic password use lower case characters
WBLC-05-000164 WebLogic password use numeric characters
WBLC-05-000165 WebLogic password use special characters
WBLC-05-000172 WebLogic PKI-based authentication with trust anchor
WBLC-06-000190 WebLogic cryptographic maintenance and diagnostic communications
WBLC-06-000191 WebLogic secure maintenance and diagnostic sessions

WBLC-08-000210 WebLogic session inactivity timeout
WBLC-08-000211 WebLogic trusted communications path
WBLC-08-000223 WebLogic session authentication
WBLC-08-000224 WebLogic session vulnerability
WBLC-08-000229 WebLogic unsafe state
WBLC-08-000231 WebLogic application confidentiality
WBLC-08-000235 WebLogic application data integrity
WBLC-08-000239 WebLogic secure cryptographic mechanism

22.7 Oracle HTTP Server STIG Compliance Standard

The Enterprise Manager implementation of the Security Technical Implementation Guide (STIG Version 1) for Oracle HTTP Server 12.1.3 contains automated rules. These rules check for Oracle HTTP Server configuration settings and generate violations. It is important that you review and understand implemented rules to ensure they are acceptable in your environment.

OH12-1X-000007 LoadModule ossl_module directive enabled to encrypt remote connections
OH12-1X-000008 SSLFIPS directive enabled to encrypt remote connections
OH12-1X-000010 SSLCipherSuite directive enabled to encrypt remote connections
OH12-1X-000011 LoadModule ossl_module directive enabled to protect the integrity of remote sessions
OH12-1X-000012 SSLFIPS directive enabled to protect the integrity of remote sessions
OH12-1X-000013 SSLEngine, SSLProtocol, and SSLWallet enabled and configured to protect the integrity of remote sessions
OH12-1X-000014 SSLCipherSuite directive enabled to protect the integrity of remote sessions
OH12-1X-000211 OHS version supported by vendor
OH12-1X-000234 mod_plsql directive PlsqlDatabasePassword obfuscated
OH12-1X-000240 LoadModule ossl_module directive enabled to encrypt passwords during transmission
OH12-1X-000241 SSLFIPS directive enabled to encrypt passwords during transmission
OH12-1X-000242 SSLEngine, SSLProtocol, and SSLWallet enabled and configured to encrypt passwords
OH12-1X-000243 SSLCipherSuite directive enabled to encrypt passwords during transmission
OH12-1X-000294 LoadModule ossl_module directive enabled to implement cryptographic protections
OH12-1X-000295 SSLFIPS directive enabled to implement cryptographic protections
OH12-1X-000296 SSLEngine, SSLProtocol, and SSLWallet enabled and configured to implement cryptographic protections
OH12-1X-000297 SSLCipherSuite directive enabled to implement cryptographic protections
OH12-1X-000308 LoadModule ossl_module directive enabled to prevent unauthorized disclosure of information
OH12-1X-000309 SSLFIPS directive enabled to prevent unauthorized disclosure of information

OH12-1X-000310 SSLEngine, SSLProtocol, and SSLWallet enabled and configured to prevent unauthorized disclosure of information.

OH12-1X-000311 SSLCipherSuite directive enabled to prevent unauthorized disclosure of information during transmission

23

Security Technical Implementation Guidelines (STIG) Rules Enhanced by Oracle

Security Technical Implementation Guidelines (STIG) rules enhanced by Oracle.

23.1 Oracle 12c Database STIG Variations

The following STIG database rules are enhanced by Oracle for Oracle 12c Database. **Bold** text in the Collection Query denotes the change.

23.1.1 SV-75899r1_rule

Description: Audit trail data must be retained for at least one year.

Automation Logic:

```
SELECT * FROM ( SELECT CASE WHEN ((SELECT count(*) from V$OPTION WHERE
PARAMETER='Unified Auditing' AND VALUE='FALSE')=1) THEN (SELECT name||' parameter is
set to '||value||'.' value from v$parameter where name='audit_trail' and
value='NONE')
    END AS VALUE FROM DUAL) WHERE VALUE IS NOT NULL
```

Change to STIG Rule: Combined the rule queries to check if audit is enabled by means of either Traditional or Unified system. Need to manually check if audit data is retained for at least one year.

23.1.2 SV-75903r1_rule

Description: Oracle instance names must not contain Oracle version numbers.

Automation Logic:

```
select 'Instance name contain version number' from v$instance where instance_name
LIKE '%12%';
```

Change to STIG Rule: Provided an even more specific query to check if instance name contains version number.

23.1.3 SV-75905r1_rule

Description: Fixed user and public database links must be authorized for use.

Automation Logic:

```
select 'Fixed user database link '||db_link||' found for '||owner value from
dba_db_links
where db_link not in (select master from sys.dba_repcatlog)
```

Change to STIG Rule: Combined the rule queries to return db_link as violations only if dba_repcatalog has records.

23.1.4 SV-75907r1_rule

Description: A minimum of two Oracle control files must be defined and configured to be stored on separate, archived physical disks or archived directories on a RAID device.

Automation Logic:

```
select 'A minimum of two oracle control files must be defined' value from v
$controlfile having count(*) < 2
```

Change to STIG Rule: Need to manually check if each file is located on a separate RAID device.

23.1.5 SV-75909r1_rule

Description: A minimum of two Oracle redo log groups or files must be defined and configured to be stored on separate, archived physical disks or archived directories on a RAID device.

Automation Logic:

```
select 'A minimum of two Oracle redo log groups/files must be defined ' value from v
$LOG where members > 1 having count(*) < 2
```

Change to STIG Rule: Used the more stricter query to get the violation. Need to manually check if a RAID device is used.

23.1.6 SV-75923r1_rule

Description: System privileges granted using the WITH ADMIN OPTION must not be granted to unauthorized user accounts.

Automation Logic:

```
select 'User '|| grantee||' granted system privilege ' ||privilege ||' WITH ADMIN
option' value from dba_sys_privs
where grantee not in
('SYS', 'SYSTEM', 'AQ_ADMINISTRATOR_ROLE', 'DBA',
'MDSYS', 'LBACSYS', 'SCHEDULER_ADMIN',
'WMSYS', 'APEX_030200', 'APEX_040200','DVSYS','SYSKM','DV_ACCTMGR')
and admin_option = 'YES'
and grantee not in
(select grantee from dba_role_privs where granted_role = 'DBA')
```

Change to STIG Rule: Added default users/roles to the query - 'APEX_030200', 'APEX_040200', 'DVSYS', 'SYSKM', and 'DV_ACCTMGR'.

23.1.7 SV-75927r1_rule

Description: Oracle roles granted using the WITH ADMIN OPTION must not be granted to unauthorized accounts.

Automation Logic:

```
select 'Role ' ||grantee||' granted '||granted_role||' WITH ADMIN OPTION' value from
dba_role_privs
where grantee not in
```

```
('ANONYMOUS','CTXSTS','EXFSYS','LBACSYS','MDSYS','OLAPSYS','OEDDATA','OWBSYS','ORDPLU
GINS','ORDSYS','OUTLN','SI_INFORMTN_SCHEMA','WK_TEST','WK_SYS','WKPROXY','WMSYS','XDB
','DBSNMP','MGMT_VIEW','SYS','SYSMAN','SYSTEM','DBA','DV_ACCTMGR','DV_OWNER','RECOVER
Y_CATALOG_OWNER','SPATIAL_CSW_ADMIN_USR','SPATIAL_WFS_ADMIN_USR')
and admin_option = 'YES'
and grantee not in
(select distinct owner from dba_objects)
and grantee not in
(select grantee from dba_role_privs
where granted_role = 'DBA')
order by grantee
```

Change to STIG Rule: Added default users/roles to the query: 'DBA', 'DV_ACCTMGR', 'DV_OWNER', 'RECOVERY_CATALOG_OWNER', 'SPATIAL_CSW_ADMIN_USR', and 'SPATIAL_WFS_ADMIN_USR'.

23.1.8 SV-75931r2_rule

Description: Listener must be configured for administration authentication.

Automation Logic:

```
perl %scriptsDir%/lsnrSecStatus.pl {OracleHome} {MachineName} {Port} {Protocol}
```

Change to STIG Rule: Script provided by Oracle.

23.1.9 SV-75937r2_rule

Description: Connections by mid-tier web and application systems to the Oracle DBMS from a DMZ or external network must be encrypted.

Automation Logic:

```
perl %scriptsDir%/encryptedCommCheck.pl {OracleHome}
```

Change to STIG Rule: Script provided by Oracle.

23.1.10 SV-75945r1_rule

Description: Application user privilege assignment must be reviewed monthly, or more frequently to ensure compliance with least privilege, and documented policy.

Automation Logic:

```
select 'No privilege analysis policy is defined/run to analyze unrequired
application user privilege assignment' value from SYS.DBA_UNUSED_SYSPRIVS having
count(*)=0
```

Change to STIG Rule: Added a query to check whether privilege analysis policy is defined/run to analyze non-required application user privilege assignment.

23.1.11 SV-75947r1_rule

Description: Audit trail data must be reviewed daily or more frequently.

Automation Logic:

```
SELECT * FROM ( SELECT CASE WHEN ((SELECT count(*) from SYS.V$OPTION WHERE
PARAMETER='Unified Auditing' AND VALUE='FALSE')=1) THEN
   (SELECT name||' parameter is set to '||value||'.' value from sys.v$parameter
where name='audit_trail' and value='NONE')
    END AS VALUE FROM DUAL) WHERE VALUE IS NOT NULL
```

Change to STIG Rule: Combined the rule queries to check if audit is enabled by means of either Traditional or Unified system.

23.1.12 SV-75953r1_rule

Description: The directories assigned to the LOG_ARCHIVE_DEST* parameters must be protected from unauthorized access.

Automation Logic:

```
perl %scriptsDir%/logArchiveDestPerm.pl {OracleHome} {MachineName} {Port} {Protocol}
{SID} {UserName} {password} {Role}
```

Change to STIG Rule: Script provided by Oracle.

23.1.13 SV-75957r1_rule

Description: Application object owner accounts must be disabled when installation or maintenance actions are not performed.

Automation Logic:

```
select distinct 'Application object owner account '||owner||' found' value from
dba_objects, dba_users
where owner not in
('ANONYMOUS','AURORA$JIS$UTILITY$',
'AURORA$ORB$UNAUTHENTICATED','CTXSYS','DBSNMP','DIP','DVF',
'DVSYS','EXFSYS','LBACSYS','MDDATA','MDSYS','MGMT_VIEW','ODM',
'ODM_MTR','OLAPSYS','ORDPLUGINS','ORDSYS','OSE$HTTP$ADMIN',
'OUTLN','PERFSTAT','PUBLIC','REPADMIN','RMAN',
'SI_INFORMTN_SCHEMA','SYS','SYSMAN','SYSTEM','TRACESVR',
'TSMSYS','WK_TEST','WKPROXY','WKSYS','WKUSER','WMSYS','XDB', 'HR', 'OE', 'PM', 'IX',
'SH','OJVMSYS','ORDDATA','APPQOSSYS','ORACLE_OCM','SCOTT','APEX_040200','AUDSYS','GSM
ADMIN_INTERNAL','FLOWS_FILES')
and owner in (select distinct owner from dba_objects
where object_type <> 'SYNONYM')
and owner = username
and upper(account_status) not like '%LOCKED%'
```

Change to STIG Rule: Changed the query to include more default users/roles which are not in the list.

23.1.14 SV-76001r1_rule

Description: Access to DBMS software files and directories must not be granted to unauthorized users.

Automation Logic:

```
perl %scriptsDir%/umaskCheck.pl {OracleHome} 022
```

Change to STIG Rule: Changed the query to include more default users/roles which are not in the list.

23.1.15 SV-76017r1_rule

Description: Changes to DBMS security labels must be audited.

Automation Logic:

```
 SELECT * FROM (
SELECT CASE UPPER(value) WHEN 'FALSE'
```

```
     THEN
      (SELECT CASE UPPER(value) WHEN 'NONE'
            THEN
                name||' parameter is set to '||value||'.'
            ELSE
                (SELECT 'Changes to DBMS security labels must be audited.' value
from dba_sa_audit_options having count(*)=0)
            END AS VALUE FROM  v$parameter where name='audit_trail' )
     END AS value FROM v$option
           WHERE parameter  ='Unified Auditing') where VALUE IS NOT NULL;
```

Change to STIG Rule: Combined rule queries.

23.1.16 SV-76021r2_rule

Description: The /diag subdirectory under the directory assigned to the DIAGNOSTIC_DEST parameter must be protected from unauthorized access.

Automation Logic:

```
perl %scriptsDir%/diagDestPerm.pl {OracleHome} {MachineName} {Port} {Protocol} {SID}
{UserName} {password} {Role}
```

Change to STIG Rule: Script provided by Oracle.

23.1.17 SV-76023r1_rule

Description: Remote administration must be disabled for the Oracle connection manager.

Automation Logic:

```
perl %scriptsDir%/remoteAdminCheck.pl {OracleHome}
```

Change to STIG Rule: Script provided by Oracle.

23.1.18 SV-76025r1_rule

Description: Network client connections must be restricted to supported versions.

Automation Logic:

```
perl %scriptsDir%/allowedLogonVersion.pl {OracleHome} 11
```

Change to STIG Rule: Script provided by Oracle.

23.1.19 SV-76035r1_rule

Description: The DBMS must employ cryptographic mechanisms preventing the unauthorized disclosure of information during transmission unless the transmitted data is otherwise protected by alternative physical measures.

Automation Logic:

```
perl %scriptsDir%/encryptionCheck.pl {OracleHome}
```

Change to STIG Rule: Script provided by Oracle.

23.1.20 SV-76037r1_rule

Description: The DBMS must utilize approved cryptography when passing authentication data for remote access sessions.

Automation Logic:

```
perl %scriptsDir%/encryptionCheck.pl {OracleHome}
```

Change to STIG Rule: Script provided by Oracle.

23.1.21 SV-76039r1_rule

Description: A DBMS providing remote access capabilities must utilize organization-defined cryptography to protect the confidentiality of data passing over remote access sessions.

Automation Logic:

```
perl %scriptsDir%/encryptionCheck.pl {OracleHome}
```

Change to STIG Rule: Script provided by Oracle.

23.1.22 SV-76041r1_rule

Description: A DBMS providing remote access capabilities must utilize approved cryptography to protect the integrity of remote access sessions.

Automation Logic:

```
perl %scriptsDir%/encryptionCheck.pl {OracleHome}
```

Change to STIG Rule: Script provided by Oracle.

23.1.23 SV-76043r1_rule

Description: The DBMS must ensure remote sessions that access an organization-defined list of security functions and security-relevant information are audited.

Automation Logic:

```
SELECT * FROM ( SELECT CASE WHEN ((SELECT count(*) from SYS.V$OPTION WHERE
PARAMETER='Unified Auditing' AND VALUE='FALSE')=1) THEN
   (SELECT name||' parameter is set to '||value||'.' value from sys.v$parameter
where name='audit_trail' and value='NONE')
    END AS VALUE FROM DUAL) WHERE VALUE IS NOT NULL
```

Change to STIG Rule: Combined rule queries to check if audit is enabled by means of either Traditional or Unified system. Need to manually check if remote sessions that are accessing security information are being audited.

23.1.24 SV-76045r1_rule

Description: The DBMS must support the disabling of network protocols deemed as non-secure by the organization.

Automation Logic:

```
perl %scriptsDir%/secureProtocolCheck.pl {Protocol}
```

Change to STIG Rule: Script provided by Oracle.

23.1.25 SV-76051r1_rule

Description: The DBMS must provide a mechanism to automatically terminate accounts designated as temporary or emergency accounts after an organization-defined time period.

Automation Logic:

```
select 'User '||u.username||' is assigned profile '||p.profile||' with
PASSWORD_LIFE_TIME='||p.limit||'.'
value from dba_profiles p, dba_users u,
(select limit as def_pwd_life_tm
from dba_profiles
where profile = 'DEFAULT'
and resource_name = 'PASSWORD_LIFE_TIME')
where p.resource_name = 'PASSWORD_LIFE_TIME'
and ((replace(p.limit, 'DEFAULT', def_pwd_life_tm) in
('UNLIMITED', 'NULL'))
or (lpad(replace(p.limit, 'DEFAULT', def_pwd_life_tm),40,'0') >
lpad('35',40,'0')))
  AND u.profile = p.profile
```

Change to STIG Rule: A query added by Oracle.

23.1.26 SV-76053r1_rule

Description: The DBMS must automatically disable accounts after a 35 day period of account inactivity.

Automation Logic:

```
select 'User '||u.username||' is assigned profile '||p.profile||' with
PASSWORD_LIFE_TIME='||p.limit||'.'
value from dba_profiles p, dba_users u,
(select limit as def_pwd_life_tm
from dba_profiles
where profile = 'DEFAULT'
and resource_name = 'PASSWORD_LIFE_TIME')
where p.resource_name = 'PASSWORD_LIFE_TIME'
and ((replace(p.limit, 'DEFAULT', def_pwd_life_tm) in
('UNLIMITED', NULL))
or (lpad(replace(p.limit, 'DEFAULT', def_pwd_life_tm),40,'0') >
lpad('35',40,'0')))
  AND u.profile = p.profile
UNION ALL
select 'Table SYS.LOGIN_AUDIT_INFO_ALL is not used.' value FROM DUAL WHERE NOT
EXISTS (select table_name from dba_tables where table_name='LOGIN_AUDIT_INFO_ALL')
```

Change to STIG Rule: A query added by Oracle.

23.1.27 SV-76055r1_rule

Description: The DBMS must automatically audit account creation.

Automation Logic:

```
  SELECT * FROM (
     SELECT CASE UPPER(value) WHEN 'FALSE'
     THEN
      (SELECT CASE UPPER(value) WHEN 'NONE'
            THEN
```

```
               name||' parameter is set to '||value||'.'
            ELSE
               (SELECT 'Account creation is not being audited' value from
sys.dba_stmt_audit_opts where AUDIT_OPTION='CREATE USER' having count(*)=0)
            END AS VALUE FROM  v$parameter where name='audit_trail' )
     ELSE
        (SELECT CASE UPPER(value) WHEN 'NONE'
           THEN
        (SELECT 'Account creation is not being audited' from audit_unified_policies
where AUDIT_OPTION='CREATE USER' AND AUDIT_OPTION_TYPE='STANDARD ACTION' AND
AUDIT_CONDITION!='NONE' having count(*)=0)
     ELSE
              (SELECT DISTINCT value FROM (SELECT 'Account creation is not being
audited' value from audit_unified_policies where AUDIT_OPTION='CREATE USER' AND
AUDIT_OPTION_TYPE='STANDARD ACTION' AND AUDIT_CONDITION!='NONE' having count(*)=0
          UNION
      SELECT 'Account creation is not being audited' value from
sys.dba_stmt_audit_opts where AUDIT_OPTION='CREATE USER' having count(*)=0  ))
            END AS VALUE FROM  v$parameter where name='audit_trail' )
     END AS value FROM v$option WHERE parameter  ='Unified Auditing') where VALUE IS
NOT NULL;
```

Change to STIG Rule: Combined rule queries to check if audit is enabled by means of either Traditional or Unified system and to check if account creation is being audited.

23.1.28 SV-76059r1_rule

Description: The DBMS must automatically audit account modification.

Automation Logic:

```
  SELECT * FROM (
     SELECT CASE UPPER(value) WHEN 'FALSE'
     THEN
      (SELECT CASE UPPER(value) WHEN 'NONE'
            THEN
               name||' parameter is set to '||value||'.'
            ELSE
               (SELECT 'Account modification is not being audited' value from
sys.dba_stmt_audit_opts where AUDIT_OPTION='ALTER USER' having count(*)=0)
            END AS VALUE FROM  v$parameter where name='audit_trail' )
     ELSE
        (SELECT CASE UPPER(value) WHEN 'NONE'
           THEN
        (SELECT 'Account modification is not being audited' from
audit_unified_policies where AUDIT_OPTION='ALTER USER' AND
AUDIT_OPTION_TYPE='STANDARD ACTION' AND AUDIT_CONDITION!='NONE' having count(*)=0)
     ELSE
              (SELECT DISTINCT value FROM (SELECT 'Account modification is not being
audited' value from audit_unified_policies where AUDIT_OPTION='ALTER USER' AND
AUDIT_OPTION_TYPE='STANDARD ACTION' AND AUDIT_CONDITION!='NONE' having count(*)=0
          UNION
      SELECT 'Account modification is not being audited' value from
sys.dba_stmt_audit_opts where AUDIT_OPTION='ALTER USER' having count(*)=0  ))
            END AS VALUE FROM  v$parameter where name='audit_trail' )
     END AS value FROM v$option WHERE parameter  ='Unified Auditing') where VALUE IS
NOT NULL;
```

Change to STIG Rule: Combined rule queries to check if audit is enabled by means of either Traditional or Unified system and to check if account modification is being audited.

23.1.29 SV-76061r1_rule

Description: The DBMS must automatically audit account disabling actions.

Automation Logic:

```
SELECT * FROM (
     SELECT CASE UPPER(value) WHEN 'FALSE'
     THEN
      (SELECT CASE UPPER(value) WHEN 'NONE'
            THEN
                name||' parameter is set to '||value||'.'
            ELSE
                (SELECT 'Account disabling is not being audited' value from
sys.dba_stmt_audit_opts where AUDIT_OPTION='ALTER USER' having count(*)=0)
            END AS VALUE FROM  v$parameter where name='audit_trail' )
     ELSE
        (SELECT CASE UPPER(value) WHEN 'NONE'
           THEN
        (SELECT 'Account disabling is not being audited' from audit_unified_policies
where AUDIT_OPTION='ALTER USER' AND AUDIT_OPTION_TYPE='STANDARD ACTION' AND
AUDIT_CONDITION!='NONE' having count(*)=0)
     ELSE
              (SELECT DISTINCT value FROM (SELECT 'Account disabling is not being
audited' value from audit_unified_policies where AUDIT_OPTION='ALTER USER' AND
AUDIT_OPTION_TYPE='STANDARD ACTION' AND AUDIT_CONDITION!='NONE' having count(*)=0
          UNION
      SELECT 'Account disabling is not being audited' value from
sys.dba_stmt_audit_opts where AUDIT_OPTION='ALTER USER' having count(*)=0  ))
            END AS VALUE FROM  v$parameter where name='audit_trail' )
     END AS value FROM v$option WHERE parameter  ='Unified Auditing') where VALUE IS
NOT NULL;
```

Change to STIG Rule: Combined rule queries to check if audit is enabled by means of either Traditional or Unified system. Need to manually check if account disabling is being audited.

23.1.30 SV-76063r1_rule

Description: The DBMS must automatically audit account termination.

Automation Logic:

```
SELECT * FROM (
     SELECT CASE UPPER(value) WHEN 'FALSE'
     THEN
      (SELECT CASE UPPER(value) WHEN 'NONE'
            THEN
                name||' parameter is set to '||value||'.'
            ELSE
                (SELECT 'Account termination is not being audited' value from
sys.dba_stmt_audit_opts where AUDIT_OPTION='DROP USER' having count(*)=0)
            END AS VALUE FROM  v$parameter where name='audit_trail' )
     ELSE
        (SELECT CASE UPPER(value) WHEN 'NONE'
           THEN
        (SELECT 'Account termination is not being audited' from
audit_unified_policies where AUDIT_OPTION='DROP USER' AND
AUDIT_OPTION_TYPE='STANDARD ACTION' AND AUDIT_CONDITION!='NONE' having count(*)=0)
     ELSE
              (SELECT DISTINCT value FROM (SELECT 'Account termination is not being
```

```
audited' value from audit_unified_policies where AUDIT_OPTION='DROP USER' AND
AUDIT_OPTION_TYPE='STANDARD ACTION' AND AUDIT_CONDITION!='NONE' having count(*)=0
          UNION
      SELECT 'Account termination is not being audited' value from
sys.dba_stmt_audit_opts where AUDIT_OPTION='DROP USER' having count(*)=0  ))
            END AS VALUE FROM  v$parameter where name='audit_trail' )
     END AS value FROM v$option WHERE parameter  ='Unified Auditing') where VALUE IS
NOT NULL;
```

Change to STIG Rule: Combined rule queries to check if audit is enabled by means of either Traditional or Unified system and to check if account termination is being audited.

23.1.31 SV-76081r1_rule

Description: Administrative privileges must be assigned to database accounts through database roles.

Automation Logic:

```
select 'User '|| dsp.grantee ||' is granted '|| dsp.privilege ||' privilege' value
     from dba_sys_privs dsp, dba_users du
     where dsp.grantee in (SELECT username
     FROM dba_users
     WHERE username NOT IN
     (
     'XDB', 'SYSTEM', 'SYS', 'LBACSYS',
     'DVSYS', 'DVF', 'SYSMAN_RO',
     'SYSMAN_BIPLATFORM', 'SYSMAN_MDS',
     'SYSMAN_OPSS', 'SYSMAN_STB', 'DBSNMP',
     'SYSMAN', 'APEX_040200', 'WMSYS',
     'SYSDG', 'SYSBACKUP', 'SPATIAL_WFS_ADMIN_USR',
     'SPATIAL_CSW_ADMIN_US', 'GSMCATUSER',
     'OLAPSYS', 'SI_INFORMTN_SCHEMA',
     'OUTLN', 'ORDSYS', 'ORDDATA', 'OJVMSYS',
     'ORACLE_OCM', 'MDSYS', 'ORDPLUGINS',
     'GSMADMIN_INTERNAL', 'MDDATA', 'FLOWS_FILES',
     'DIP', 'CTXSYS', 'AUDSYS',
     'APPQOSSYS', 'APEX_PUBLIC_USER', 'ANONYMOUS',
     'SPATIAL_CSW_ADMIN_USR', 'SYSKM',
     'SYSMAN_TYPES', 'MGMT_VIEW',
     'EUS_ENGINE_USER', 'EXFSYS', 'SYSMAN_APM'
     )
     ) AND dsp.privilege NOT IN ('UNLIMITED TABLESPACE', 'REFERENCES', 'INDEX',
'SYSDBA','SYSOPER') and dsp.grantee=du.username and du.account_status not like
'%EXPIRED%LOCKED%' order by dsp.grantee
```

Change to STIG Rule: A query added by Oracle.

23.1.32 SV-76085r1_rule

Description: All usage of privileged accounts must be audited.

Automation Logic:

```
SELECT * FROM ( SELECT CASE WHEN ((SELECT count(*) from SYS.V$OPTION WHERE
PARAMETER='Unified Auditing' AND VALUE='FALSE')=1) THEN    (select 'audit_trail
parameter is set to '||value value from v$parameter where name='audit_trail' and
value = 'NONE')
 END AS VALUE FROM DUAL) WHERE VALUE IS NOT NULL
```

Change to STIG Rule: Combined rule queries to check if audit is enabled by means of either Traditional or Unified system. Need to manually check if all use of privileged accounts are audited.

23.1.33 SV-76093r1_rule

Description: The DBMS must verify if account lock-outs persist until reset by an administrator.

Automation Logic:

```
select p.resource_name||' is not set to UNLIMITED for user '||u.username||' through
profile '||p.profile AS value from dba_users u, dba_profiles p
where u.profile = p.profile
  and p.resource_name = 'PASSWORD_LOCK_TIME'
  and p.limit != 'UNLIMITED'
  and u.account_status not like '%EXPIRED%LOCKED%'
```

Change to STIG Rule: A query added by Oracle.

23.1.34 SV-76095r1_rule

Description: The DBMS must limit the number of consecutive failed logon attempts to 3.

Automation Logic:

```
select p.resource_name||' limit is set to '||p.limit||' for user '||u.username||'
through profile '||p.profile AS value from dba_profiles p, dba_users u,
(select limit as def_fld_lgn_atmt from dba_profiles
where profile = 'DEFAULT'
and resource_name = 'FAILED_LOGIN_ATTEMPTS')
where p.resource_name = 'FAILED_LOGIN_ATTEMPTS'
and ((replace(p.limit, 'DEFAULT', def_fld_lgn_atmt) in
('UNLIMITED', NULL))
or (lpad(replace(p.limit, 'DEFAULT', def_fld_lgn_atmt),40,'0') > lpad('3',40,'0')))
  AND u.profile = p.profile
AND u.account_status not like '%EXPIRED%LOCKED%'
```

Change to STIG Rule: A query added by Oracle.

23.1.35 SV-76097r1_rule

Description: The DBMS, when the maximum number of unsuccessful logon attempts is exceeded, must automatically lock the account/node until released by an administrator.

Automation Logic:

```
select p.resource_name||' is set to '||p.limit||' for user '||u.username||' through
profile '||p.profile AS
value from dba_profiles p, dba_users u,
(select limit as def_fld_lgn_atmt
from dba_profiles
where profile = 'DEFAULT'
and resource_name = 'FAILED_LOGIN_ATTEMPTS')
where p.resource_name = 'FAILED_LOGIN_ATTEMPTS'
and ((replace(p.limit, 'DEFAULT', def_fld_lgn_atmt) in
('UNLIMITED', NULL))
or (lpad(replace(p.limit, 'DEFAULT', def_fld_lgn_atmt),40,'0') >
lpad('3',40,'0')))
```

```
  AND u.profile = p.profile
AND u.account_status not like '%EXPIRED%LOCKED%'
```

Change to STIG Rule: A query added by Oracle.

23.1.36 SV-76099r1_rule

Description: The DBMS must retain the notification message or banner on the screen until users take explicit actions to log on to the database.

Automation Logic:

```
perl bannerText.pl {OracleHome}
```

Change to STIG Rule: Script provided by Oracle.

23.1.37 SV-76101r1_rule

Description: The DBMS must display the system use information when appropriate, before granting further access.

Automation Logic:

```
perl bannerText.pl {OracleHome}
```

Change to STIG Rule: Script provided by Oracle.

23.1.38 SV-76103r1_rule

Description: The DBMS must have its auditing configured to reduce the likelihood of storage capacity being exceeded.

Automation Logic:

```
select tablespace_name ||' tablespace used for logging '||table_name value from
sys.dba_tables where table_name in ('AUD$', 'FGA_LOG$')
 AND tablespace_name = 'SYSTEM' UNION ALL select tablespace_name ||' tablespace used
for unified adit '||table_name value from sys.dba_tables where owner='AUDSYS' and
tablespace_name='USERS'
```

Change to STIG Rule: A query added by Oracle.

23.1.39 SV-76105r1_rule

Description: The DBMS must have allocated audit record storage capacity.

Automation Logic:

```
select tablespace_name ||' tablespace used for logging '||table_name value from
sys.dba_tables where table_name in ('AUD$', 'FGA_LOG$')
 AND tablespace_name = 'SYSTEM' UNION ALL select tablespace_name ||' tablespace used
for unified adit '||table_name value from sys.dba_tables where owner='AUDSYS' and
tablespace_name='USERS'
```

Change to STIG Rule: A query added by Oracle.

23.1.40 SV-76111r1_rule

Description: The DBMS must provide audit record generation capability for organization-defined auditable events within the database.

Automation Logic:

```
SELECT * FROM ( SELECT CASE WHEN ((SELECT count(*) from SYS.V$OPTION WHERE
PARAMETER='Unified Auditing' AND VALUE='FALSE')=1) THEN    (select 'audit_trail
parameter is set to '||value value from v$parameter where name='audit_trail' and
value = 'NONE')
 END AS VALUE FROM DUAL) WHERE VALUE IS NOT NULL
```

Change to STIG Rule: Combined rule queries to check if audit is enabled by means of either Traditional or Unified system.

23.1.41 SV-76115r1_rule

Description: The DBMS must generate audit records for the DoD-selected list of auditable events.

Automation Logic:

```
SELECT * FROM ( SELECT CASE WHEN ((SELECT count(*) from SYS.V$OPTION WHERE
PARAMETER='Unified Auditing' AND VALUE='FALSE')=1) THEN (SELECT name||' parameter is
set to '||value||'.' value from sys.v$parameter where name='audit_trail' and
value='NONE')
    END AS VALUE FROM DUAL) WHERE VALUE IS NOT NULL
```

Change to STIG Rule: Combined rule queries to check if audit is enabled by means of either Traditional or Unified system.

23.1.42 SV-76117r1_rule

Description: The DBMS must produce audit records containing sufficient information to establish what type of events occurred.

Automation Logic:

```
SELECT * FROM ( SELECT CASE WHEN ((SELECT count(*) from SYS.V$OPTION WHERE
PARAMETER='Unified Auditing' AND VALUE='FALSE')=1) THEN    (select 'audit_trail
parameter is set to '||value value from v$parameter where name='audit_trail' and
value = 'NONE')
 END AS VALUE FROM DUAL) WHERE VALUE IS NOT NULL
```

Change to STIG Rule: Combined rule queries to check if audit is enabled by means of either Traditional or Unified system.

23.1.43 SV-76121r1_rule

Description: The DBMS must produce audit records containing sufficient information to establish when (date and time) the events occurred.

Automation Logic:

```
SELECT * FROM ( SELECT CASE WHEN ((SELECT count(*) from SYS.V$OPTION WHERE
PARAMETER='Unified Auditing' AND VALUE='FALSE')=1) THEN    (select 'audit_trail
parameter is set to '||value value from v$parameter where name='audit_trail' and
value = 'NONE')
 END AS VALUE FROM DUAL) WHERE VALUE IS NOT NULL
```

Change to STIG Rule: Combined rule queries to check if audit is enabled by means of either Traditional or Unified system.

23.1.44 SV-76123r1_rule

Description: The DBMS must produce audit records containing sufficient information to establish where the events occurred.

Automation Logic:

```
SELECT * FROM ( SELECT CASE WHEN ((SELECT count(*) from SYS.V$OPTION WHERE
PARAMETER='Unified Auditing' AND VALUE='FALSE')=1) THEN    (select 'audit_trail
parameter is set to '||value value from v$parameter where name='audit_trail' and
value = 'NONE')
 END AS VALUE FROM DUAL) WHERE VALUE IS NOT NULL
```

Change to STIG Rule: Combined rule queries to check if audit is enabled by means of either Traditional or Unified system.

23.1.45 SV-76125r1_rule

Description: The DBMS must produce audit records containing sufficient information to establish the sources (origins) of the events.

Automation Logic:

```
SELECT * FROM ( SELECT CASE WHEN ((SELECT count(*) from SYS.V$OPTION WHERE
PARAMETER='Unified Auditing' AND VALUE='FALSE')=1) THEN    (select 'audit_trail
parameter is set to '||value value from v$parameter where name='audit_trail' and
value = 'NONE')
 END AS VALUE FROM DUAL) WHERE VALUE IS NOT NULL
```

Change to STIG Rule: Combined rule queries to check if audit is enabled by means of either Traditional or Unified system.

23.1.46 SV-76127r1_rule

Description: The DBMS must produce audit records containing sufficient information to establish the outcome (success or failure) of the events.

Automation Logic:

```
SELECT * FROM ( SELECT CASE WHEN ((SELECT count(*) from SYS.V$OPTION WHERE
PARAMETER='Unified Auditing' AND VALUE='FALSE')=1) THEN    (select 'audit_trail
parameter is set to '||value value from v$parameter where name='audit_trail' and
value = 'NONE')
 END AS VALUE FROM DUAL) WHERE VALUE IS NOT NULL
```

Change to STIG Rule: Combined rule queries to check if audit is enabled by means of either Traditional or Unified system.

23.1.47 SV-76129r1_rule

Description: The DBMS must produce audit records containing sufficient information to establish the identity of any user/subject or process associated with the event.

Automation Logic:

```
SELECT * FROM ( SELECT CASE WHEN ((SELECT count(*) from SYS.V$OPTION WHERE
PARAMETER='Unified Auditing' AND VALUE='FALSE')=1) THEN    (select 'audit_trail
parameter is set to '||value value from v$parameter where name='audit_trail' and
value = 'NONE')
 END AS VALUE FROM DUAL) WHERE VALUE IS NOT NULL
```

Change to STIG Rule: Combined rule queries to check if audit is enabled by means of either Traditional or Unified system.

23.1.48 SV-76131r1_rule

Description: The DBMS must include organization-defined additional, more detailed information in the audit records for audit events identified by type, location, or subject.

Automation Logic:

```
SELECT * FROM ( SELECT CASE WHEN ((SELECT count(*) from SYS.V$OPTION WHERE
PARAMETER='Unified Auditing' AND VALUE='FALSE')=1) THEN    (select 'audit_trail
parameter is set to '||value value from v$parameter where name='audit_trail' and
value = 'NONE')
 END AS VALUE FROM DUAL) WHERE VALUE IS NOT NULL
```

Change to STIG Rule: Combined rule queries to check if audit is enabled by means of either Traditional or Unified system.

23.1.49 SV-76143r2_rule

Description: The system must protect audit information from any type of unauthorized access.

Automation Logic:

```
SELECT GRANTEE||' has '||PRIVILEGE||' on '|| TABLE_NAME AS VALUE FROM
sys.DBA_TAB_PRIVS where (table_name = 'AUD$' or table_name='FGA_LOG$') AND grantee
not in ('SYS','SYSTEM', 'DELETE_CATALOG_ROLE') UNION ALL  SELECT GRANTEE|| ' has '||
PRIVILEGE|| ' on '||TABLE_NAME AS VALUE FROM sys.DBA_TAB_PRIVS where owner='AUDSYS'
AND grantee not in ('SYS', 'SYSTEM', 'DELETE_CATALOG_ROLE')
```

Change to STIG Rule: A query added by Oracle.

23.1.50 SV-76145r1_rule

Description: The system must protect audit information from unauthorized modification.

Automation Logic:

```
SELECT GRANTEE||' has '||PRIVILEGE||' on '|| TABLE_NAME AS VALUE FROM
sys.DBA_TAB_PRIVS where (table_name = 'AUD$' or table_name='FGA_LOG$') AND PRIVILEGE
IN ('DELETE','INSERT','UPDATE') AND grantee not in ('SYS','SYSTEM',
'DELETE_CATALOG_ROLE') UNION ALL  SELECT GRANTEE|| ' has '||PRIVILEGE|| ' on '||
TABLE_NAME AS VALUE FROM sys.DBA_TAB_PRIVS where owner='AUDSYS' AND PRIVILEGE IN
('DELETE','INSERT','UPDATE') AND grantee not in ('SYS','SYSTEM',
'DELETE_CATALOG_ROLE')
```

Change to STIG Rule: A query added by Oracle.

23.1.51 SV-76147r1_rule

Description: The system must protect audit information from unauthorized deletion.

Automation Logic:

```
SELECT GRANTEE||' has '||PRIVILEGE||' on '|| TABLE_NAME AS VALUE FROM
sys.DBA_TAB_PRIVS where (table_name = 'AUD$' or table_name='FGA_LOG$') AND
PRIVILEGE='DELETE' AND grantee not in ('SYS','SYSTEM', 'DELETE_CATALOG_ROLE') UNION
ALL  SELECT GRANTEE|| ' has '||PRIVILEGE|| ' on '||TABLE_NAME AS VALUE FROM
sys.DBA_TAB_PRIVS where owner='AUDSYS' AND PRIVILEGE='DELETE' AND grantee not in
('SYS','SYSTEM', 'DELETE_CATALOG_ROLE')
```

Change to STIG Rule: A query added by Oracle.

23.1.52 SV-76157r1_rule

Description: The DBMS must protect audit data records and integrity by using cryptographic mechanisms.

Automation Logic:

```
SELECT 'Tablespace '||t.tablespace_name ||' holding audit data in '||t.table_name||'
is not encrypted.' value
      FROM dba_tables t, dba_tablespaces ts
   WHERE (t.table_name ='AUD$' OR t.table_name='FGA_LOG$' OR t.owner= 'AUDSYS')
         AND t.tablespace_name = ts.tablespace_name
         AND ts.encrypted = 'NO'
        AND EXISTS (SELECT PARAMETER as value1 from SYS.V$OPTION WHERE
PARAMETER='Unified Auditing' AND VALUE='TRUE' UNION select name as value1 from v
$parameter where name='audit_trail' and UPPER(value) != 'NONE')
```

Change to STIG Rule: A query added by Oracle.

23.1.53 SV-76159r1_rule

Description: The DBMS must protect the audit records generated, as a result of remote access to privileged accounts, and the execution of privileged functions.

Automation Logic:

```
SELECT GRANTEE||' has '||PRIVILEGE||' on '|| TABLE_NAME AS VALUE FROM
sys.DBA_TAB_PRIVS where (table_name = 'AUD$' or table_name='FGA_LOG$') AND grantee
not in ('SYS','SYSTEM', 'DELETE_CATALOG_ROLE') UNION ALL  SELECT GRANTEE|| ' has '||
PRIVILEGE|| ' on '||TABLE_NAME AS VALUE FROM sys.DBA_TAB_PRIVS where owner='AUDSYS'
AND grantee not in ('SYS','SYSTEM', 'DELETE_CATALOG_ROLE') UNION ALL  SELECT GRANTEE
|| ' has been granted with '||GRANTED_ROLE AS VALUE FROM sys.DBA_ROLE_PRIVS WHERE
GRANTED_ROLE IN ('AUDIT_ADMIN','AUDIT_VIEWER','DELETE_CATALOG_ROLE') AND GRANTEE NOT
IN ('SYS','SYSTEM','DBA')
```

Change to STIG Rule: Combined rule queries to check if audit records are being protected.

23.1.54 SV-76161r1_rule

Description: The DBMS must support enforcement of logical access restrictions associated with changes to the DBMS configuration and to the database itself.

Automation Logic:

```
perl %scriptsDir%/umaskCheck.pl {OracleHome} 022
```

Change to STIG Rule: Script provided by Oracle.

23.1.55 SV-76163r1_rule

Description: Database objects must be owned by accounts authorized for ownership.

Automation Logic:

```
SELECT 'Database objects are owned by unauthorized user '||OWNER value FROM ( SELECT
OWNER, COUNT(*)  FROM DBA_OBJECTS
WHERE OWNER NOT IN ('PUBLIC', 'OUTLN', 'CTXSYS', 'SYSTEM', 'EXFSYS', 'DBSNMP',
'ORDSYS', 'ORDPLUGINS', 'APPQOSYS', 'XDB', 'IX', 'ORDDATA', 'SYS', 'WMSYS', 'MDSYS',
'OLAPSYS', 'SYSMAN', 'APEX_030200', 'FLOWS_FILES', 'SI_INFORMTN_SCHEMA',
```

```
'ORACLE_OCM', 'APPQOSSYS', 'PM', 'OE', 'SH', 'HR', 'ORACLE_OCM', 'SCOTT',
'OWBSYS_AUDIT', 'OWBSYS',
'BI','APEX_040200','DVF','DVSYS','LBACSYS','AUDSYS','GSMADMIN_INTERNAL','OJVMSYS')
GROUP BY OWNER )
```

Change to STIG Rule: A query added by Oracle.

23.1.56 SV-76167r1_rule

Description: Default demonstration and sample databases, database objects, and applications must be removed.

Automation Logic:

```
select distinct 'Demonstration account '||username||' found in database' value from
dba_users where username in ('BI', 'HR', 'OE', 'PM', 'IX', 'SH', 'SCOTT')
```

Change to STIG Rule: A query added by Oracle.

23.1.57 SV-76173r1_rule

Description: Use of external executables must be authorized.

Automation Logic:

```
SELECT owner||'.'||library_name||' is a library containing external procedure.' AS
VALUE FROM ( select library_name,owner, '' grantee, '' privilege
from dba_libraries where file_spec is not null
minus
(
select library_name,o.name owner, '' grantee, '' privilege
 from dba_libraries l,
 sys.user$ o,
 sys.user$ ge,
 sys.obj$ obj,
 sys.objauth$ oa
 where l.owner=o.name
 and obj.owner#=o.user#
 and obj.name=l.library_name
 and oa.obj#=obj.obj#
 and ge.user#=oa.grantee#
 and l.file_spec is not null
))
union all

SELECT grantee||' has been granted with '||privilege||' on '||owner||'.'||
library_name||' the library containing external procedures.' AS VALUE FROM (
select library_name,o.name owner, --obj.obj#,oa.privilege#,
 ge.name grantee,
 tpm.name privilege
 from dba_libraries l,
 sys.user$ o,
 sys.user$ ge,
 sys.obj$ obj,
 sys.objauth$ oa,
 sys.table_privilege_map tpm
 where l.owner=o.name
 and obj.owner#=o.user#
 and obj.name=l.library_name
 and oa.obj#=obj.obj#
 and ge.user#=oa.grantee#
 and tpm.privilege=oa.privilege#
```

```
and l.file_spec is not null
)
```

Change to STIG Rule: Made to be operated manually as query cannot be executed successfully because of special characters being added.

23.1.58 SV-76175r1_rule

Description: Access to external executables must be disabled or restricted.

Automation Logic:

```
perl %scriptsDir%/externalExecs.pl {OracleHome}
```

Change to STIG Rule: Script provided by Oracle.

23.1.59 SV-76181r1_rule

Description: The DBMS must have transaction journaling enabled.

Automation Logic:

```
select 'Database is in NOARCHIVELOG mode' value from v$database where log_mode !=
'ARCHIVELOG'
```

Change to STIG Rule: A query added by Oracle.

23.1.60 SV-76193r1_rule

Description: The DBMS must use multifactor authentication for network access to privileged accounts.

Automation Logic:

```
perl %scriptsDir%/multiFactorAuth.pl {OracleHome}
```

Change to STIG Rule: Script provided by Oracle.

23.1.61 SV-76195r1_rule

Description: The DBMS must use multifactor authentication for network access to non-privileged accounts.

Automation Logic:

```
perl %scriptsDir%/multiFactorAuth.pl {OracleHome}
```

Change to STIG Rule: Script provided by Oracle.

23.1.62 SV-76197r1_rule

Description: The DBMS must use multifactor authentication for local access to privileged accounts.

Automation Logic:

```
perl %scriptsDir%/multiFactorAuth.pl {OracleHome}
```

Change to STIG Rule: Script provided by Oracle.

23.1.63 SV-76199r1_rule

Description: The DBMS must use multifactor authentication for local access to non-privileged accounts.

Automation Logic:

```
perl %scriptsDir%/multiFactorAuth.pl {OracleHome}
```

Change to STIG Rule: Script provided by Oracle.

23.1.64 SV-76203r1_rule

Description: The DBMS must use organization-defined replay-resistant authentication mechanisms for network access to privileged accounts.

Automation Logic:

```
perl %scriptsDir%/replayResistantAuthCheck.pl {OracleHome}
```

Change to STIG Rule: Script provided by Oracle.

23.1.65 SV-76205r1_rule

Description: The DBMS must use organization-defined replay-resistant authentication mechanisms for network access to non-privileged accounts.

Automation Logic:

```
perl %scriptsDir%/replayResistantAuthCheck.pl {OracleHome}
```

Change to STIG Rule: Script provided by Oracle.

23.1.66 SV-76207r1_rule

Description: The DBMS must support organizational requirements to disable user accounts after an organization-defined time period of inactivity.

Automation Logic:

```
select p.resource_name||' limit is set to '||p.limit||' for user '||u.username||'
through profile '||p.profile AS
value from dba_profiles p, dba_users u,
(select limit as def_pwd_life_tm
from dba_profiles
where profile = 'DEFAULT'
and resource_name = 'PASSWORD_LIFE_TIME')
where p.resource_name = 'PASSWORD_LIFE_TIME'
and ((replace(p.limit, 'DEFAULT', def_pwd_life_tm) in
('UNLIMITED', 'NULL'))
or (lpad(replace(p.limit, 'DEFAULT', def_pwd_life_tm),40,'0') >
lpad('35',40,'0')))
  AND u.profile = p.profile
  AND u.account_status not like '%EXPIRED%LOCKED%' AND u.AUTHENTICATION_TYPE NOT IN
('GLOBAL','EXTERNAL')
UNION ALL
select 'Table SYS.LOGIN_AUDIT_INFO_ALL is not used' value FROM DUAL WHERE NOT EXISTS
(select table_name from dba_tables where table_name='LOGIN_AUDIT_INFO_ALL')
```

Change to STIG Rule: A query added by Oracle.

23.1.67 SV-76209r1_rule

Description: The DBMS must support organizational requirements to enforce minimum password length.

Automation Logic:

```
select p.resource_name||' is not set for user '||u.username||' through profile '||
p.profile||' to check minimum password length' AS
value from sys.dba_profiles p, sys.dba_users u,
(select limit as def_pwd_verify_func
from sys.dba_profiles
where profile = 'DEFAULT'
and resource_name = 'PASSWORD_VERIFY_FUNCTION')
where p.resource_name = 'PASSWORD_VERIFY_FUNCTION'
and ((replace(p.limit, 'DEFAULT', def_pwd_verify_func) in ('', 'NULL'))) AND
u.profile = p.profile
AND u.account_status not like '%EXPIRED%LOCKED%' and u.AUTHENTICATION_TYPE NOT IN
('EXTERNAL', 'GLOBAL')
```

Change to STIG Rule: A query added by Oracle.

23.1.68 SV-76211r2_rule

Description: The DBMS must support organizational requirements to prohibit password reuse for the organization-defined number of generations.

Automation Logic:

```
elect profile|| ' profile has PASSWORD_REUSE_TIME set to '||limit
value from dba_profiles p,
(select limit as def_pwd_reuse_tm
from dba_profiles
where profile = 'DEFAULT'
and resource_name = 'PASSWORD_REUSE_TIME')
where p.resource_name = 'PASSWORD_REUSE_TIME'
and ((replace(p.limit, 'DEFAULT', def_pwd_reuse_tm) in
('UNLIMITED', NULL))
or (lpad(replace(p.limit, 'DEFAULT', def_pwd_reuse_tm),40,'0') <
lpad('6',40,'0')))
UNION
SELECT profile|| ' profile has PASSWORD_REUSE_MAX set to '||limit value FROM
dba_profiles
 WHERE resource_name = 'PASSWORD_REUSE_MAX'
   AND (limit IS NULL
        OR limit = 'UNLIMITED')
```

Change to STIG Rule: A query added by Oracle.

23.1.69 SV-76213r1_rule

Description: The DBMS must support organizational requirements to enforce password complexity by the number of upper-case characters used.

Automation Logic:

```
select p.resource_name||' is not set for user '||u.username||' through profile '||
p.profile||' to check number of upper-case characters used' AS value from
sys.dba_profiles p, sys.dba_users u, (select limit as def_pwd_verify_func from
sys.dba_profiles where profile = 'DEFAULT' and resource_name =
'PASSWORD_VERIFY_FUNCTION') where p.resource_name = 'PASSWORD_VERIFY_FUNCTION' and
```

```
((replace(p.limit, 'DEFAULT', def_pwd_verify_func) in ('', 'NULL'))) AND u.profile =
p.profile AND u.account_status not like '%EXPIRED%LOCKED%' and u.AUTHENTICATION_TYPE
NOT IN ('EXTERNAL', 'GLOBAL')
```

Change to STIG Rule: A query added by Oracle.

23.1.70 SV-76215r1_rule

Description: The DBMS must support organizational requirements to enforce password complexity by the number of lower-case characters used.

Automation Logic:

```
select p.resource_name||' is not set for user '||u.username||' through profile '||
p.profile||' to check number of lower-case characters used' AS
value from sys.dba_profiles p, sys.dba_users u,
(select limit as def_pwd_verify_func
from sys.dba_profiles
where profile = 'DEFAULT'
and resource_name = 'PASSWORD_VERIFY_FUNCTION')
where p.resource_name = 'PASSWORD_VERIFY_FUNCTION'
and ((replace(p.limit, 'DEFAULT', def_pwd_verify_func) in ('', 'NULL'))) AND
u.profile = p.profile
AND u.account_status not like '%EXPIRED%LOCKED%' and u.AUTHENTICATION_TYPE NOT IN
('EXTERNAL', 'GLOBAL')
```

Change to STIG Rule: A query added by Oracle.

23.1.71 SV-76217r1_rule

Description: The DBMS must support organizational requirements to enforce password complexity by the number of numeric characters used.

Automation Logic:

```
select p.resource_name||' is not set for user '||u.username||' through profile '||
p.profile||' to check number of numeric characters used' AS
value from sys.dba_profiles p, sys.dba_users u,
(select limit as def_pwd_verify_func
from sys.dba_profiles
where profile = 'DEFAULT'
and resource_name = 'PASSWORD_VERIFY_FUNCTION')
where p.resource_name = 'PASSWORD_VERIFY_FUNCTION'
and ((replace(p.limit, 'DEFAULT', def_pwd_verify_func) in ('', 'NULL'))) AND
u.profile = p.profile
AND u.account_status not like '%EXPIRED%LOCKED%' and u.AUTHENTICATION_TYPE NOT IN
('EXTERNAL', 'GLOBAL')
```

Change to STIG Rule: A query added by Oracle.

23.1.72 SV-76219r1_rule

Description: The DBMS must support organizational requirements to enforce password complexity by the number of special characters used.

Automation Logic:

```
select p.resource_name||' is not set for user '||u.username||' through profile '||
p.profile||' to check number of special characters used' AS
value from sys.dba_profiles p, sys.dba_users u,
(select limit as def_pwd_verify_func
from sys.dba_profiles
```

```
where profile = 'DEFAULT'
and resource_name = 'PASSWORD_VERIFY_FUNCTION')
where p.resource_name = 'PASSWORD_VERIFY_FUNCTION'
and ((replace(p.limit, 'DEFAULT', def_pwd_verify_func) in ('', 'NULL'))) AND
u.profile = p.profile
AND u.account_status not like '%EXPIRED%LOCKED%' and u.AUTHENTICATION_TYPE NOT IN
('EXTERNAL', 'GLOBAL')
```

Change to STIG Rule: A query added by Oracle.

23.1.73 SV-76221r1_rule

Description: The DBMS must support organizational requirements to enforce the number of characters that get changed when passwords are changed.

Automation Logic:

```
select p.resource_name||' is not set for user '||u.username||' through profile '||
p.profile||' to check number of characters changed on password reset' AS
value from sys.dba_profiles p, sys.dba_users u,
(select limit as def_pwd_verify_func
from sys.dba_profiles
where profile = 'DEFAULT'
and resource_name = 'PASSWORD_VERIFY_FUNCTION')
where p.resource_name = 'PASSWORD_VERIFY_FUNCTION'
and ((replace(p.limit, 'DEFAULT', def_pwd_verify_func) in ('', 'NULL'))) AND
u.profile = p.profile
AND u.account_status not like '%EXPIRED%LOCKED%' and u.AUTHENTICATION_TYPE NOT IN
('EXTERNAL', 'GLOBAL')
```

Change to STIG Rule: A query added by Oracle.

23.1.74 SV-76229r1_rule

Description: The DBMS must enforce maximum lifetime restrictions on password.

Automation Logic:

```
select p.profile||' has PASSWORD_LIFE_TIME set to '||p.limit||'.'
value from dba_profiles p,
(select limit as def_pwd_life_tm
from dba_profiles
where profile = 'DEFAULT'
and resource_name = 'PASSWORD_LIFE_TIME')
where p.resource_name = 'PASSWORD_LIFE_TIME'
and ((replace(p.limit, 'DEFAULT', def_pwd_life_tm) in
('UNLIMITED', NULL))
or (lpad(replace(p.limit, 'DEFAULT', def_pwd_life_tm),40,'0') >
lpad('35',40,'0')))
```

Change to STIG Rule: A query added by Oracle.

23.1.75 SV-76237r1_rule

Description: The DBMS must use NIST-validated FIPS 140-2-compliant cryptography for authentication mechanisms.

Automation Logic:

```
perl %scriptsDir%/fipsCompliantCheck.pl {OracleHome}
```

Change to STIG Rule: Script provided by Oracle.

23.1.76 SV-76245r1_rule

Description: The DBMS must support organizational requirements to encrypt information stored in the database and information extracted or derived from the database and stored on digital media.

Automation Logic:

```
select 'Parameter '||name||' is set to '||value  AS VALUE from  SYS.V$PARAMETER
where name='DBFIPS_140' and value='FALSE'
UNION SELECT 'DBMS must support organizational requirements to encrypt information
stored in the database and information extracted or derived from the database' as
value FROM DUAL WHERE NOT EXISTS(SELECT NAME FROM SYS.V$PARAMETER where
name='DBFIPS_140')
```

Change to STIG Rule: A query added by Oracle.

23.1.77 SV-76247r2_rule

Description: The DBMS must terminate the network connection associated with a communications session at the end of the session or 15 minutes of inactivity.

Automation Logic:

```
select p.resource_name||' is set to '||p.limit||' for user '||u.username||' through
profile '||p.profile AS value from sys.DBA_PROFILES p, sys.dba_users u,(SELECT limit
as def_idle_time FROM sys.DBA_PROFILES where profile='DEFAULT' AND
RESOURCE_NAME='IDLE_TIME') d where p.resource_name ='IDLE_TIME' and (DECODE
(p.limit, 'DEFAULT', d.def_idle_time, limit) = 'UNLIMITED' OR (lpad(replace(p.limit,
'DEFAULT', d.def_idle_time),40,'0') > lpad('15',40,'0'))) and u.profile = p.profile
and u.account_status not like '%EXPIRED%LOCKED%'
```

Change to STIG Rule: A query added by Oracle.

23.1.78 SV-76249r1_rule

Description: The DBMS must implement required cryptographic protections using cryptographic modules complying with applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance.

Automation Logic:

```
perl %scriptsDir%/cryptoProtectionCheck.pl {OracleHome} {MachineName} {Port}
{Protocol} {SID} {UserName} {password} {Role}
```

Change to STIG Rule: Script provided by Oracle.

23.1.79 SV-76251r1_rule

Description: Database data files containing sensitive information must be encrypted.

Automation Logic:

```
select 'Parameter '||name||' is set to '||value  AS VALUE from  SYS.V$PARAMETER
where name='DBFIPS_140' and value='FALSE'
UNION SELECT 'Database data files containing sensitive information must be
encrypted.' as value FROM DUAL WHERE NOT EXISTS(SELECT NAME FROM SYS.V$PARAMETER
where name='DBFIPS_140')
```

Change to STIG Rule: A query added by Oracle.

23.1.80 SV-76253r1_rule

Description: The DBMS must protect the integrity of publicly available information and applications.

Automation Logic:

```
SELECT TABLESPACE_NAME||' tablespace is not READ ONLY. ' AS VALUE FROM
sys.DBA_TABLESPACES WHERE STATUS != 'READ ONLY' AND TABLESPACE_NAME NOT IN
('SYSTEM','SYSAUX','UD1','TEMP','SYSEXT','UNDOTBS')
```

Change to STIG Rule: A query added by Oracle.

23.1.81 SV-76255r1_rule

Description: The DBMS must terminate user sessions upon user logoff or any other organization or policy-defined session termination events, such as exceeding idle time limit.

Automation Logic:

```
SELECT resource_name||' is set to '||limit||' for user '||username||' through
profile '||profile AS value FROM (select
u.username,p.profile,p.resource_name,p.limit,u.account_status from sys.DBA_PROFILES
p, sys.dba_users u,(SELECT limit as def_idle_time FROM sys.DBA_PROFILES where
profile='DEFAULT' AND RESOURCE_NAME='IDLE_TIME') d where p.resource_name
='IDLE_TIME' and (DECODE (p.limit, 'DEFAULT', d.def_idle_time, limit) = 'UNLIMITED'
OR (lpad(replace(p.limit, 'DEFAULT', d.def_idle_time),40,'0') > lpad('15',40,'0')))
and u.profile = p.profile
UNION ALL
select u.username,p.profile, p.resource_name, p.limit,u.account_status from
sys.DBA_PROFILES p, sys.dba_users u where p.resource_name='CONNECT_TIME' and DECODE
(limit, 'DEFAULT', (SELECT limit from DBA_PROFILES d where
d.resource_name=p.resource_name and profile='DEFAULT'), limit) = 'UNLIMITED' and
u.profile = p.profile) where account_status not like '%EXPIRED%LOCKED%'
```

Change to STIG Rule: A query added by Oracle.

23.1.82 SV-76257r1_rule

Description: The DBMS must fail to a known safe state for defined types of failures.

Automation Logic:

```
select 'Database is in NOARCHIVELOG mode' value from v$database where log_mode !=
'ARCHIVELOG'
```

Change to STIG Rule: A query added by Oracle.

23.1.83 SV-76261r1_rule

Description: The DBMS must take needed steps to protect data at rest and ensure confidentiality and integrity of application data.

Automation Logic:

```
SELECT 'Table '||a.owner||'.'||a.table_name||' in tablespace '||a.tablespace_name||'
is not protected by means of encryption.' AS VALUE
 FROM dba_tables a WHERE a.tablespace_name NOT IN (select t.name from v$tablespace
t, v$encrypted_tablespaces e where t.ts# = e.ts# ) AND a.tablespace_name NOT IN
('SYSTEM','SYSAUX','UD1','TEMP','SYSEXT','UNDOTBS') AND ROWNUM < 200
```

Change to STIG Rule: Modified the query to exclude -'SYSTEM', 'SYSAUX', 'UD1', 'TEMP', 'SYSEXT', and 'UNDOTBS'.

23.1.84 SV-76263r1_rule

Description: The DBMS must employ cryptographic mechanisms preventing the unauthorized disclosure of information at rest unless the data is otherwise protected by alternative physical measures.

Automation Logic:

```
SELECT 'Table '||a.owner||'.'||a.table_name||' in tablespace '||a.tablespace_name||'
is not protected by means of encryption.' AS VALUE
 FROM dba_tables a WHERE a.tablespace_name NOT IN (select t.name from v$tablespace
t, v$encrypted_tablespaces e where t.ts# = e.ts# ) AND a.tablespace_name NOT IN
('SYSTEM','SYSAUX','UD1','TEMP','SYSEXT','UNDOTBS') AND ROWNUM < 200
```

Change to STIG Rule: Modified the query to exclude -'SYSTEM', 'SYSAUX', 'UD1', 'TEMP', 'SYSEXT', and 'UNDOTBS'.

23.1.85 SV-76275r1_rule

Description: The DBMS must check the validity of data inputs.

Automation Logic:

```
select owner, 'Constraint '||owner ||'.'||constraint_name || ' is '|| status||' '||
validated value from dba_constraints where (status='DISABLED' or validated='NOT
VALIDATED') and owner not in ('SYS', 'SYSMAN', 'SH', 'SYSTEM', 'PM', 'OE', 'SH',
'HR', 'IX', 'OLAPSYS', 'ORDDATA', 'CTXSYS', 'WMSYS')
```

Change to STIG Rule: A query added by Oracle.

23.1.86 SV-76287r2_rule

Description: The DBMS must notify appropriate individuals when accounts are created.

Automation Logic:

```
SELECT * FROM (
     SELECT CASE UPPER(value) WHEN 'FALSE'
     THEN
      (SELECT CASE UPPER(value) WHEN 'NONE'
            THEN
                name||' parameter is set to '||value||'.'
            ELSE
                (SELECT 'Account creation is not being audited' value from
sys.dba_stmt_audit_opts where AUDIT_OPTION='CREATE USER' having count(*)=0)
            END AS VALUE FROM  v$parameter where name='audit_trail' )
     ELSE
        (SELECT CASE UPPER(value) WHEN 'NONE'
           THEN
        (SELECT 'Account creation is not being audited' from audit_unified_policies
where AUDIT_OPTION='CREATE USER' AND AUDIT_OPTION_TYPE='STANDARD ACTION' AND
AUDIT_CONDITION!='NONE' having count(*)=0)
     ELSE
              (SELECT DISTINCT value FROM (SELECT 'Account creation is not being
audited' value from audit_unified_policies where AUDIT_OPTION='CREATE USER' AND
AUDIT_OPTION_TYPE='STANDARD ACTION' AND AUDIT_CONDITION!='NONE' having count(*)=0
          UNION
```

```
      SELECT 'Account creation is not being audited' value from
sys.dba_stmt_audit_opts where AUDIT_OPTION='CREATE USER' having count(*)=0  ))
            END AS VALUE FROM  v$parameter where name='audit_trail' )
     END AS value FROM v$option WHERE parameter  ='Unified Auditing') where VALUE IS
NOT NULL;
```

Change to STIG Rule: Combined to check if audit is enabled by means of either Traditional or Unified system and to check if account creation is being audited. Need to manually check if they are being notified.

23.1.87 SV-76289r2_rule

Description: The DBMS must notify appropriate individuals when accounts are modified.

Automation Logic:

```
SELECT * FROM (
     SELECT CASE UPPER(value) WHEN 'FALSE'
     THEN
      (SELECT CASE UPPER(value) WHEN 'NONE'
            THEN
                name||' parameter is set to '||value||'.'
            ELSE
                (SELECT 'Account modification is not being audited' value from
sys.dba_stmt_audit_opts where AUDIT_OPTION='ALTER USER' having count(*)=0)
            END AS VALUE FROM  v$parameter where name='audit_trail' )
     ELSE
        (SELECT CASE UPPER(value) WHEN 'NONE'
           THEN
        (SELECT 'Account modification is not being audited' from
audit_unified_policies where AUDIT_OPTION='ALTER USER' AND
AUDIT_OPTION_TYPE='STANDARD ACTION' AND AUDIT_CONDITION!='NONE' having count(*)=0)
     ELSE
              (SELECT DISTINCT value FROM (SELECT 'Account modification is not being
audited' value from audit_unified_policies where AUDIT_OPTION='ALTER USER' AND
AUDIT_OPTION_TYPE='STANDARD ACTION' AND AUDIT_CONDITION!='NONE' having count(*)=0
          UNION
      SELECT 'Account modification is not being audited' value from
sys.dba_stmt_audit_opts where AUDIT_OPTION='ALTER USER' having count(*)=0  ))
            END AS VALUE FROM  v$parameter where name='audit_trail' )
     END AS value FROM v$option WHERE parameter  ='Unified Auditing') where VALUE IS
NOT NULL;
```

Change to STIG Rule: Combined to check if audit is enabled by means of either Traditional or Unified system and to check if account modification is being audited. Need to manually check if it is notified.

23.1.88 SV-76291r2_rule

Description: The DBMS must notify appropriate individuals when account disabling actions are taken.

Automation Logic:

```
SELECT * FROM (
     SELECT CASE UPPER(value) WHEN 'FALSE'
     THEN
      (SELECT CASE UPPER(value) WHEN 'NONE'
            THEN
                name||' parameter is set to '||value||'.'
```

```
            ELSE
                (SELECT 'Account disabling is not being audited' value from
sys.dba_stmt_audit_opts where AUDIT_OPTION='ALTER USER' having count(*)=0)
            END AS VALUE FROM  v$parameter where name='audit_trail' )
     ELSE
        (SELECT CASE UPPER(value) WHEN 'NONE'
           THEN
        (SELECT 'Account disabling is not being audited' from audit_unified_policies
where AUDIT_OPTION='ALTER USER' AND AUDIT_OPTION_TYPE='STANDARD ACTION' AND
AUDIT_CONDITION!='NONE' having count(*)=0)
     ELSE
              (SELECT DISTINCT value FROM (SELECT 'Account disabling is not being
audited' value from audit_unified_policies where AUDIT_OPTION='ALTER USER' AND
AUDIT_OPTION_TYPE='STANDARD ACTION' AND AUDIT_CONDITION!='NONE' having count(*)=0
          UNION
      SELECT 'Account disabling is not being audited' value from
sys.dba_stmt_audit_opts where AUDIT_OPTION='ALTER USER' having count(*)=0  ))
            END AS VALUE FROM  v$parameter where name='audit_trail' )
     END AS value FROM v$option WHERE parameter  ='Unified Auditing') where VALUE IS
NOT NULL;
```

Change to STIG Rule: Combined to check if audit is enabled by means of either Traditional or Unified system and to check if account disabling is being audited. Need to manually check if it is notified.

23.1.89 SV-76293r2_rule

Description: The DBMS must notify appropriate individuals when accounts are terminated.

Automation Logic:

```
SELECT * FROM (
     SELECT CASE UPPER(value) WHEN 'FALSE'
     THEN
      (SELECT CASE UPPER(value) WHEN 'NONE'
            THEN
                name||' parameter is set to '||value||'.'
            ELSE
                (SELECT 'Account termination is not being audited' value from
sys.dba_stmt_audit_opts where AUDIT_OPTION='DROP USER' having count(*)=0)
            END AS VALUE FROM  v$parameter where name='audit_trail' )
     ELSE
        (SELECT CASE UPPER(value) WHEN 'NONE'
           THEN
        (SELECT 'Account termination is not being audited' from
audit_unified_policies where AUDIT_OPTION='DROP USER' AND
AUDIT_OPTION_TYPE='STANDARD ACTION' AND AUDIT_CONDITION!='NONE' having count(*)=0)
     ELSE
              (SELECT DISTINCT value FROM (SELECT 'Account termination is not being
audited' value from audit_unified_policies where AUDIT_OPTION='DROP USER' AND
AUDIT_OPTION_TYPE='STANDARD ACTION' AND AUDIT_CONDITION!='NONE' having count(*)=0
          UNION
      SELECT 'Account termination is not being audited' value from
sys.dba_stmt_audit_opts where AUDIT_OPTION='DROP USER' having count(*)=0  ))
            END AS VALUE FROM  v$parameter where name='audit_trail' )
     END AS value FROM v$option WHERE parameter  ='Unified Auditing') where VALUE IS
NOT NULL;
```

Change to STIG Rule: Combined to check if audit is enabled by means of either Traditional or Unified system and to check if account termination is being audited. Need to manually check if it is notified.

23.1.90 SV-76299r1_rule

Description: The DBMS must support organizational requirements to implement separation of duties through assigned information access authorizations.

Automation Logic:

```
select grantee ||' has '||privilege||' privilege on '|| table_name value
FROM dba_tab_privs
WHERE grantee NOT IN (
SELECT role
FROM dba_roles)
  and grantee not in ('SYSKM', 'PUBLIC', 'SYSBACKUP', 'CTXSYS', 'EXFSYS', 'DVSYS',
'SYSTEM', 'AUDSYS', 'DBSNMP', 'ORDSYS',
                      'XDB', 'SYSDG', 'ORDDATA', 'APPQOSSYS', 'SYS', 'WMSYS',
'LBACSYS', 'MDSYS', 'ORACLE_OCM',
'OWBSYS_AUDIT' ,'DIP' ,'SPATIAL_WFS_ADMIN_USR' ,'FLOWS_FILES' ,'HR' ,'MGMT_VIEW' ,'OL
APSYS' ,'OUTLN' ,'OWBSYS' ,'SPATIAL_CSW_ADMIN_USR' ,'APEX_030200' ,'SCOTT' ,'APEX_PUB
LIC_USER' ,'MDDATA' ,'OE' ,'ORDPLUGINS' ,'PM' ,'SH' ,'SYSMAN' ,'BI' ,'IX' ,'ANONYMOUS
' ,'SI_INFORMTN_SCHEMA','DVF','GSMADMIN_INTERNAL','APEX_040200','OJVMSYS','GSMCATUSER
')
UNION
select 'User '|| grantee ||' is granted '||privilege||' privilege ' value
 from dba_sys_privs
where grantee not in ( select role from dba_roles)
  and grantee not in ('SYSKM', 'PUBLIC', 'SYSBACKUP', 'CTXSYS', 'EXFSYS', 'DVSYS',
'SYSTEM', 'AUDSYS', 'DBSNMP', 'ORDSYS',
                      'XDB', 'SYSDG', 'ORDDATA', 'APPQOSSYS', 'SYS', 'WMSYS',
'LBACSYS', 'MDSYS', 'ORACLE_OCM',
'OWBSYS_AUDIT' ,'DIP' ,'SPATIAL_WFS_ADMIN_USR' ,'FLOWS_FILES' ,'HR' ,'MGMT_VIEW' ,'OL
APSYS' ,'OUTLN' ,'OWBSYS' ,'SPATIAL_CSW_ADMIN_USR' ,'APEX_030200' ,'SCOTT' ,'APEX_PUB
LIC_USER' ,'MDDATA' ,'OE' ,'ORDPLUGINS' ,'PM' ,'SH' ,'SYSMAN' ,'BI' ,'IX' ,'ANONYMOUS
' ,'SI_INFORMTN_SCHEMA','DVF','GSMADMIN_INTERNAL','APEX_040200','OJVMSYS','GSMCATUSER
')
```

Change to STIG Rule: Changed query to exclude oracle default users/roles.

23.1.91 SV-76301r1_rule

Description: The DBMS must display an approved system use notification message or banner before granting access to the database.

Automation Logic:

```
perl %scriptsDir%/bannerText.pl {OracleHome}
```

Change to STIG Rule: Script provided by Oracle.

23.1.92 SV-76307r1_rule

Description: The DBMS must manage excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of Denial of Service (DoS) attacks.

Automation Logic:

```
select p.resource_name||' is set to '||p.limit||' for user '||u.username||' through
profile '||p.profile AS value from sys.DBA_PROFILES p, sys.dba_users u,(SELECT limit
as def_limit, resource_name FROM sys.DBA_PROFILES where profile='DEFAULT' ) d where
p.resource_name IN
('CPU_PER_SESSION','LOGICAL_READS_PER_SESSION','CONNECT_TIME','PRIVATE_SGA') and
(DECODE (p.limit, 'DEFAULT', d.def_limit, limit) = 'UNLIMITED' OR
(p.resource_name='CPU_PER_SESSION' AND (lpad(replace(p.limit, 'DEFAULT',
d.def_limit),40,'0') > lpad('6000',40,'0'))) OR
(p.resource_name='LOGICAL_READS_PER_SESSION' AND (lpad(replace(p.limit, 'DEFAULT',
d.def_limit),40,'0') > lpad('1000',40,'0'))) OR (p.resource_name='CONNECT_TIME' AND
(lpad(replace(p.limit, 'DEFAULT', d.def_limit),40,'0') > lpad('30',40,'0'))) OR
(p.resource_name='PRIVATE_SGA' AND (lpad(replace(p.limit, 'DEFAULT', d.def_limit),
40,'0') > lpad('102400',40,'0'))) and u.profile = p.profile AND
d.RESOURCE_NAME=p.resource_name AND u.account_status not like '%EXPIRED%LOCKED%'
```

Change to STIG Rule: A query added by Oracle.

23.1.93 SV-76309r1_rule

Description: The DBMS must limit the use of resources by priority and not impede the host from servicing processes designated as a higher-priority.

Automation Logic:

```
select p.resource_name||' is set to '||p.limit||' for user '||u.username||' through
profile '||p.profile AS value from DBA_PROFILES p, dba_users u
where p.resource_name IN ('SESSIONS_PER_USER', 'CPU_PER_SESSION', 'CPU_PER_CALL',
'CONNECT_TIME', 'IDLE_TIME', 'LOGICAL_READS_PER_SESSION', 'LOGICAL_READS_PER_CALL',
'PRIVATE_SGA', 'COMPOSITE_LIMIT')
  and DECODE (p.limit, 'DEFAULT', (SELECT d.limit from DBA_PROFILES d where
d.resource_name=p.resource_name and d.profile='DEFAULT'), p.limit) = 'UNLIMITED' and
u.profile = p.profile and u.account_status not like '%EXPIRED%LOCKED%'
```

Change to STIG Rule: A query added by Oracle.

23.1.94 SV-76339r1_rule

Description: DBMS default accounts must be protected from misuse.

Automation Logic:

```
SELECT 'Account '||username||' is OPEN.' as value FROM sys.dba_users where
ACCOUNT_STATUS NOT LIKE '%LOCKED%' AND USERNAME NOT IN ('SYS','SYSTEM','SYSMAN') AND
ROWNUM < 200
```

Change to STIG Rule: A query added by Oracle.

23.1.95 SV-76365r1_rule

Description: Database software directories, including DBMS configuration files, must be stored in dedicated directories, or DASD pools, separate from the host OS and other applications.

Automation Logic:

```
perl %scriptsDir%/oracleFiles.pl {OracleHome}
```

Change to STIG Rule: Script provided by Oracle.

23.1.96 SV-76377r1_rule

Description: The DBMS must protect against an individual who uses a shared account falsely denying having performed a particular action.

Automation Logic:

```
SELECT * FROM ( SELECT CASE WHEN ((SELECT count(*) from SYS.V$OPTION WHERE
PARAMETER='Unified Auditing' AND VALUE='FALSE')=1) THEN (SELECT name||' parameter is
set to '||value||'.' value from sys.v$parameter where name='audit_trail' and
value='NONE')
    END AS VALUE FROM DUAL) WHERE VALUE IS NOT NULL
```

Change to STIG Rule: A query added by Oracle.

23.1.97 SV-76455r1_rule

Description: The directory assigned to the AUDIT_FILE_DEST parameter must be protected from unauthorized access and must be stored in a dedicated directory or disk partition separate from software or other application files.

Automation Logic:

```
perl %scriptsDir%/auditFileDestPerm.pl {OracleHome} {MachineName} {Port} {Protocol}
{SID} {UserName} {password} {Role}
```

Change to STIG Rule: Script provided by Oracle.

23.1.98 SV-76457r1_rule

Description: The DBMS must limit the number of concurrent sessions for each system account to an organization-defined number of sessions.

Automation Logic:

```
select p.resource_name||' is set to '||p.limit||' for user '||u.username||' through
profile '||p.profile AS value from sys.DBA_PROFILES p, sys.dba_users u,(SELECT limit
as def_limit FROM sys.DBA_PROFILES where profile='DEFAULT' AND
RESOURCE_NAME='SESSIONS_PER_USER') d where p.resource_name ='SESSIONS_PER_USER' and
DECODE (p.limit, 'DEFAULT', d.def_limit, limit) = 'UNLIMITED' and u.profile =
p.profile and u.account_status not like '%EXPIRED%LOCKED%'
```

Change to STIG Rule: A query added by Oracle.

23.2 STIG Database Checks

The following STIG database rules are enhanced by Oracle. **Bold** text in the Collection Query denotes the change.

23.2.1 DG0008

Name: Application objects should be owned by accounts authorized for ownership

Collection Query:

```
(select distinct 'Unauthorized user '||owner||' owns application objects in the
database.'  from dba_objects
where owner not in
('ANONYMOUS','AURORA$JIS$UTILITY$',
'AURORA$ORB$UNAUTHENTICATED',
```

```
'CTXSYS','DBSNMP','DIP','DVF','DVSYS','EXFSYS','LBACSYS','MDDATA',
'MDSYS','MGMT_VIEW','ODM','ODM_MTR',
'OLAPSYS','ORDPLUGINS', 'ORDSYS',
'OSE$HTTP$ADMIN','OUTLN','PERFSTAT',
'PUBLIC','REPADMIN','RMAN','SI_INFORMTN_SCHEMA',
'SYS','SYSMAN','SYSTEM','TRACESVR',
'TSMSYSWK_TEST','WKPROXY','WKSYS',
'WKUSER','WMSYS','XDB', 'OWBSYS', 'SCOTT', 'ORACLE_OCM', 'ORDDATA', 'APEX_030200',
'OWBSYS_AUDIT', 'APPQOSSYS', 'FLOWS_FILES')
and owner not in
(select grantee from dba_role_privs where granted_role='DBA'))
```

Change to STIG Rule: Added Default Users/Roles

23.2.2 DG0077

Name: Production databases should be protected from unauthorized access by developers on shared production/development host systems.

Collection Query:

```
select 'User/Role '||grantee||' granted '||privilege||' on production system' from
dba_sys_privs
where (privilege like 'CREATE%' or privilege like 'ALTER%'
or privilege like 'DROP%')
and privilege <> 'CREATE SESSION'
and grantee not in
('ANONYMOUS','AURORA$JIS$UTILITY$',
'AURORA$ORB$UNAUTHENTICATED','CTXSYS','DBSNMP','DIP',
'DVF','DVSYS','EXFSYS','LBACSYS','MDDATA','MDSYS','MGMT_VIEW',
'ODM','ODM_MTR','OLAPSYS','ORDPLUGINS','ORDSYS',
'OSE$HTTP$ADMIN','OUTLN','PERFSTAT','PUBLIC','REPADMIN',
'RMAN','SI_INFORMTN_SCHEMA','SYS','SYSMAN','SYSTEM',
'TRACESVR','TSMSYSWK_TEST','WKPROXY','WKSYS','WKUSER',
'WMSYS','XDB', 'APEX_030200', 'APPQOSSYS',
'AQ_ADMINISTRATOR_ROLE','DATAPUMP_EXP_FULL_DATABASE',
'DBA', 'EXP_FULL_DATABASE', 'FLOWS_FILES', 'IMP_FULL_DATABASE',
'DATAPUMP_IMP_FULL_DATABASE', 'OEM_ADVISOR', 'OEM_MONITOR', 'OLAP_DBA',
'OLAP_USER', 'OWB$CLIENT', 'OWBSYS', 'OWBSYS_AUDIT', 'RECOVERY_CATALOG_OWNER',
'RESOURCE', 'SCHEDULER_ADMIN', 'SPATIAL_CSW_ADMIN_USR', 'SPATIAL_WFS_ADMIN_USR')
order by 1;
```

Change to STIG Rule: Added Default Users/Roles.

23.2.3 DG0079

Name: DBMS login accounts require passwords to meet complexity requirements.

Collection Query:

```
select profile||': '||limit
from dba_profiles,
(select limit as def_pwd_verify_func
from dba_profiles
where resource_name='PASSWORD_VERIFY_FUNCTION'
and profile='DEFAULT')
where resource_name='PASSWORD_VERIFY_FUNCTION'
and replace(limit, 'DEFAULT', def_pwd_verify_func) in
('UNLIMITED', 'NULL')
```

Change to STIG Rule: Incorrect query. Replaced NULL with string 'NULL'.

23.2.4 DG0091

Name: Custom and GOTS application source code stored in the database should be protected with encryption or encoding.

Collection Query:

```
(select 'Application source code of '||owner||'.'||name||' is not encrypted.'
from dba_source
where line=1 and owner not in('SYS', 'CTXSYS', 'MDSYS', 'ODM', 'OE', 'OLAPSYS',
'ORDPLUGINS',
'ORDSYS', 'OUTLN', 'PM', 'QS_ADM', 'RMAN', 'SYSTEM', 'WKSYS',
'WMSYS', 'XDB', 'APEX_030200', 'SYSMAN', 'ORACLE_OCM', 'DBSNMP', 'EXFSYS' )
and owner not like 'OEM%'
and text not like '%wrapped%'
and type in ('PROCEDURE', 'FUNCTION', 'PACKAGE BODY'))
```

Change to STIG Rule: Added default users.

23.2.5 DG0116

Name: Database privileged role assignments should be restricted to IAO-authorized DBMS accounts.

Collection Query:

```
select 'Privileged role '||granted_role||' is assigned to user '||grantee details
from dba_role_privs
where grantee not in
('ANONYMOUS','AURORA$JIS$UTILITY$',
'AURORA$ORB$UNAUTHENTICATED','CTXSYS','DBSNMP','DIP',
'DMSYS','DVF','DVSYS','EXFSYS','LBACSYS','MDDATA','MDSYS',
'MGMT_VIEW','ODM','ODM_MTR','OLAPSYS','ORDPLUGINS','ORDSYS',
'OSE$HTTP$ADMIN','OUTLN','PERFSTAT','REPADMIN','RMAN',
'SI_INFORMTN_SCHEMA','SYS','SYSMAN','SYSTEM','TRACESVR',
'TSMSYS','WK_TEST','WKPROXY','WKSYS','WKUSER','WMSYS','XDB', 'OEM_MONITOR')
and grantee not in
('DBA', 'OLAP_USER', 'IP', 'ORASSO_PUBLIC',
'PORTAL_PUBLIC', 'DATAPUMP_EXP_FULL_DATABASE',
'DATAPUMP_IMP_FULL_DATABASE', 'EXP_FULL_DATABASE',
'IMP_FULL_DATABASE', 'OLAP_DBA', 'EXECUTE_CATALOG_ROLE',
'SELECT_CATALOG_ROLE', 'JAVASYSPRIV')
and grantee not in
(select grantee from dba_role_privs where granted_role = 'DBA')
and grantee not in (select distinct owner from dba_objects)
and granted_role in
('AQ_ADMINISTRATOR_ROLE','AQ_USER_ROLE',
'CTXAPP',
'DELETE_CATALOG_ROLE','EJBCLIENT','EXECUTE_CATALOG_ROLE',
'EXP_FULL_DATABASE','GATHER_SYSTEM_STATISTICS',
'GLOBAL_AQ_USER_ROLE','HS_ADMIN_ROLE', 'IMP_FULL
DATABASE','JAVADEBUGPRIV','JAVAIDPRIV',
'JAVASYSPRIV','JAVAUSERPRIV','JAVA_ADMIN','JAVA_DEPLOY',
'LOGSTDBY_ADMINISTRATOR','OEM_MONITOR','OLAP_DBA',
'RECOVERY_CATALOG_OWNER',
'SALES_HISTORY_ROLE','SELECT_CATALOG_ROLE','WKUSER',
'WM_ADMIN_ROLE','XDBADMIN')
and granted_role not in ('CONNECT', 'RESOURCE', 'AUTHENTICATEDUSER')
order by 1;
```

Change to STIG Rule: Added default users.

23.2.6 DG0117

Name: Administrative privileges should be assigned to database accounts via database roles.

Collection Query:

```
select 'Grantee '||grantee||' is directly granted '||privilege||' privilege. The
privilege should be granted via a role.'
from dba_sys_privs
where grantee not in
('SYS', 'SYSTEM', 'SYSMAN', 'CTXSYS', 'MDSYS', 'WKSYS', 'ANONYMOUS', 'APEX_030200',
'APEX_PUBLIC_USER', 'FLOWS_FILES', 'OUTLN', 'DIP', 'APPQOSSYS', 'WMSYS',
'OLAPSYS', 'ORACLE_OCM', 'OWBSYS_AUDIT', 'DBSNMP', 'XDB', 'EXFSYS',
'SPATIAL_WFS_ADMIN_USR', 'SPATIAL_CSW_ADMIN_USR', 'OWBSYS', 'OWBSYS_AUDIT')
and grantee not in
(select distinct granted_role from dba_role_privs)
and privilege <> 'UNLIMITED TABLESPACE'
order by 1
```

Change to STIG Rule: Added Default Users.

23.2.7 DG0119

Name: DBMS application users should not be granted administrative privileges to the DBMS.

Collection Query:

```
select 'Application user '||grantee||' has administrative privilege  '||privilege||'
on '||owner||'.'|| table_name from dba_tab_privs
where privilege in ('ALTER', 'REFERENCES', 'INDEX')
and grantee not in ('DBA', 'SYS', 'SYSTEM', 'LBACSYS', 'XDBADMIN', 'ANONYMOUS',
'APEX_PUBLIC_USER', 'CSW_USR_ROLE', 'WFS_USR_ROLE', 'SPATIAL_WFS_ADMIN',
'SPATIAL_WFS_ADMIN_USR', 'SPATIAL_CSW_ADMIN', 'SPATIAL_CSW_ADMIN_USR')
and table_name not in
('SDO_IDX_TAB_SEQUENCE', 'XDB$ACL', 'XDB_ADMIN')
and grantee not in
(select grantee from dba_role_privs where granted_role = 'DBA')
and grantee not in (select distinct owner from dba_objects) order by 1
```

Change to STIG Rule: Added default users.

23.2.8 DG0121

Name: Application users privileges should be restricted to assignment using application user roles.

Collection Query:

```
select 'User '||grantee||' has direct privilege '||privilege||' on the table '||
owner||'.'||table_name||'. The privilege should be granted via a role.'
from dba_tab_privs where grantee not in
(select role from dba_roles)
and grantee not in
('APEX_PUBLIC_USER', 'AURORA$JIS$UTILITY$', 'CTXSYS',
'DBSNMP', 'EXFSYS', 'FLOWS_030000', 'FLOWS_FILES',
'LBACSYS', 'MDSYS', 'MGMT_VIEW', 'ODM', 'OLAPSYS',
'ORACLE_OCM', 'ORDPLUGINS', 'ORDSYS',
'OSE$HTTP$ADMIN', 'OUTLN', 'OWBSYS', 'PERFSTAT',
```

```
'PUBLIC', 'REPADMIN', 'SYS', 'SYSMAN', 'SYSTEM',
'WKSYS', 'WMSYS', 'XDB', 'ANONYMOUS', 'APEX_030200', 'APEX_PUBLIC_USER',
'APPQOSSYS', 'CSW_USR_ROLE', 'WFS_USR_ROLE', 'SPATIAL_WFS_ADMIN',
'SPATIAL_WFS_ADMIN_USR', 'SPATIAL_CSW_ADMIN', 'SPATIAL_CSW_ADMIN_USR')
and table_name<>'DBMS_REPCAT_INTERNAL_PACKAGE'
and table_name not like '%RP'
and grantee not in
(select grantee from dba_tab_privs
where table_name in ('DBMS_DEFER', 'DEFLOB'))
```

Change to STIG Rule: Added default users.

23.2.9 DG0123

Name: Access to DBMS system tables and other configuration or metadata should be restricted to DBAs.

Collection Query:

```
select 'Application user '|| grantee||' is granted '||privilege||' on system table
'|| owner||'.'|| table_name from dba_tab_privs
where (owner='SYS' or table_name like 'DBA_%')
and privilege <> 'EXECUTE'
and grantee not in
('PUBLIC', 'AQ_ADMINISTRATOR_ROLE', 'AQ_USER_ROLE',
'AURORA$JIS$UTILITY$', 'OSE$HTTP$ADMIN', 'TRACESVR',
'CTXSYS', 'DBA', 'DELETE_CATALOG_ROLE',
'EXECUTE_CATALOG_ROLE', 'EXP_FULL_DATABASE',
'GATHER_SYSTEM_STATISTICS', 'HS_ADMIN_ROLE',
'IMP_FULL_DATABASE', 'LOGSTDBY_ADMINISTRATOR', 'MDSYS',
'ODM', 'OEM_MONITOR', 'OLAPSYS', 'ORDSYS', 'OUTLN',
'RECOVERY_CATALOG_OWNER', 'SELECT_CATALOG_ROLE',
'SNMPAGENT', 'SYSTEM', 'WKSYS', 'WKUSER', 'WMSYS', 'WM_ADMIN_ROLE', 'XDB',
'LBACSYS', 'PERFSTAT', 'XDBADMIN', 'ADM_PARALLEL_EXECUTE_TASK', 'APEX_030200',
'APPQOSSYS', 'DBFS_ROLE', 'EXFSYS', 'HS_ADMIN_SELECT_ROLE', 'OLAP_XS_ADMIN',
'ORACLE_OCM', 'OWB$CLIENT', 'OWBSYS', 'SYSMAN')
and grantee not in
(select grantee from dba_role_privs where granted_role='DBA')
order by 1
```

Change to STIG Rule: Added default users.

23.2.10 DO0155

Name: Only authorized system accounts should have the SYSTEM tablespace specified as the default tablespace.

Collection Query:

```
(select 'User '||username||' is using SYSTEM as temporary or default tablespace.'
from dba_users
where (default_tablespace = 'SYSTEM' or temporary_tablespace = 'SYSTEM')
and username not in
('AURORA$JIS$UTILITY$','AURORA$ORB$UNAUTHENTICATED',
'DBSNMP','MDSYS','ORDPLUGINS','ORDSYS','OSE$HTTP$ADMIN',
'OUTLN','REPADMIN','SYS','SYSTEM','TRACESVR','MTSSYS','DIP', 'MGMT_VIEW'))
```

Change to STIG Rule: Added default users.

23.2.11 DO0231

Name: Application owner accounts should have a dedicated application tablespace.

Collection Query:

```
select distinct tablespace_name||' tablespace used by '||owner||' is not a dedicated
tablespace.' from (
select distinct owner, tablespace_name
from dba_tables
where owner not in
('SYS','SYSTEM','OUTLN','OLAPSYS','CTXSYS','WKSYS','ODM','ODM_MTR'
'MDSYS','ORDSYS','WMSYS','RMAN','XDB', 'APEX_030200', 'APPQOSSYS', 'DBSNMP',
'EXFSYS', 'FLOWS_FILES', 'ORDDATA', 'OWBSYS', 'SYSMAN', 'SCOTT')
and tablespace_name is not NULL
and (owner, table_name) not in
(select owner, table_name from dba_external_tables)
order by 1)
```

Change to STIG Rule: Added default users.

23.2.12 DO0250

Name: Fixed user and public database links should be authorized for use.

Collection Query:

```
select 'Fixed user database link '||db_link||' found for '||owner value from
dba_db_links
where db_link not in (select master from sys.dba_repcatlog)
```

Comment: Combined the rule queries to return db_link as violations only if dba_repcatalog has records

23.2.13 DO0270

Name: A minimum of two Oracle redo log groups/files should be defined and configured to be stored on separate, archived physical disks or archived directories on a RAID device.

Collection Query:

```
select 'redo_logs_count', log_count from
(select count(*) log_count from  V$LOG where members > 1)
where log_count < 2
```

Comment: Used the more strict query to get the violation. Need to manually check if a RAID device is used.

23.2.14 DO0340

Name: Oracle application administration roles should be disabled if not required and authorized.

Collection Query:

```
select 'Oracle Administration role '||granted_role||' granted to '||grantee||'.'
from dba_role_privs
where default_role='YES'
and granted_role in
(select grantee from dba_sys_privs where upper(privilege) like '%USER%')
```

```
and grantee not in
('DBA', 'SYS', 'SYSTEM', 'CTXSYS', 'DBA', 'IMP_FULL_DATABASE',
'DATAPUMP_IMP_FULL_DATABASE','MDSYS', 'SYS', 'WKSYS')
and grantee not in (select distinct owner from dba_tables)
and grantee not in
(select distinct username from dba_users where upper(account_status) like
'%LOCKED%')
```

Change to STIG Rule: Added default users.

23.2.15 DO0350

Name: Oracle system privileges should not be directly assigned to unauthorized accounts.

Collection Query:

```
select 'User/Role '||grantee||' granted system privilege '||PRIVILEGE from
dba_sys_privs
where privilege<>'CREATE SESSION' and grantee not in
('PUBLIC', 'AQ_ADMINISTRATOR_ROLE', 'AQ_USER_ROLE', 'CTXSYS',
'DBA', 'DELETE_CATALOG_ROLE', 'EXECUTE_CATALOG_ROLE',
'EXP_FULL_DATABASE', 'GATHER_SYSTEM_STATISTICS',
'HS_ADMIN_ROLE', 'IMP_FULL_DATABASE',
'LOGSTDBY_ADMINISTRATOR', 'MDSYS', 'ODM', 'OEM_MONITOR',
'OLAPSYS', 'ORDSYS', 'OUTLN', 'MTSSYS',
'RECOVERY_CATALOG_OWNER', 'SELECT_CATALOG_ROLE',
'SNMPAGENT', 'SYSTEM', 'WKSYS', 'WKUSER', 'WMSYS',
'WM_ADMIN_ROLE', 'XDB', 'ANONYMOUS', 'CONNECT', 'DBSNMP',
'JAVADEBUGPRIV', 'ODM_MTR', 'OLAP_DBA', 'ORDPLUGINS',
'RESOURCE', 'RMAN', 'SYS', 'WKPROXY', 'AURORA$JIS$UTILITY$',
'AURORA$ORB$UNAUTHENTICATED', 'OSE$HTTP$ADMIN',
'TIMESERIES_DBA', 'TIMESERIES_DEVELOPER', 'OLAP_USER', 'DATAPUMP_EXP_FULL_DATABASE',
'DATAPUMP_IMP_FULL_DATABASE', 'OEM_ADVISOR', 'OWB$CLIENT', 'SCHEDULER_ADMIN',
'SYSMAN')
and grantee not in
(select grantee from dba_role_privs where granted_role='DBA')
and grantee not in
(select username from dba_users where upper(account_status) like
'%LOCKED%') order by 1
```

Change to STIG Rule: Added default users and roles.

23.2.16 DO3536

Name: The IDLE_TIME profile parameter should be set for Oracle profiles IAW DoD policy.

Collection Query:

```
select 'IDLE_TIME set to '||limit||' for profile '||profile||'.' from (
select profile, limit from DBA_PROFILES
where profile = 'DEFAULT'
and resource_name = 'IDLE_TIME')
where TO_NUMBER(DECODE (limit, 'UNLIMITED', 1000, limit)) > 15
UNION
select profile, limit from (
select profile, limit from DBA_PROFILES
where profile <> 'DEFAULT'
and resource_name = 'IDLE_TIME')
where TO_NUMBER(DECODE (limit, 'UNLIMITED', 1000, 'DEFAULT', (SELECT DECODE(limit,
```

```
'UNLIMITED', 1000, limit)
 from DBA_PROFILES where resource_name='IDLE_TIME' and profile='DEFAULT'), limit))
> 60
```

Comment: Combined the queries. De-referenced the DEFAULT value for the limit.

23.2.17 DO3609

Name: System privileges granted using the WITH ADMIN OPTION should not be granted to unauthorized user accounts.

Collection Query:

```
select 'User '||grantee||' granted '||privilege||' privilege WITH ADMIN OPTION.'
from dba_sys_privs
where grantee not in
('SYS', 'SYSTEM', 'AQ_ADMINISTRATOR_ROLE', 'DBA',
'MDSYS', 'LBACSYS', 'SCHEDULER_ADMIN',
'WMSYS', 'APEX_030200', 'OWBSYS')
and admin_option = 'YES'
and grantee not in
(select grantee from dba_role_privs where granted_role = 'DBA') order by 1
```

Change to STIG Rule: Added default users and roles.

23.2.18 DO3689

Name: Object permissions granted to PUBLIC should be restricted.

Collection Query:

```
select privilege||' on '||owner ||'.'|| table_name ||' is granted to PUBLIC.' from
dba_tab_privs
where grantee = 'PUBLIC'
and owner not in
('SYS', 'CTXSYS', 'MDSYS', 'ODM', 'OLAPSYS', 'MTSSYS',
'ORDPLUGINS', 'ORDSYS', 'SYSTEM', 'WKSYS', 'WMSYS',
'XDB', 'LBACSYS', 'PERFSTAT', 'SYSMAN', 'DMSYS',
'EXFSYS','APEX_030200', 'DBSNMP', 'ORDDATA')
```

Change to STIG Rule: Added default users and roles.

23.3 STIG Installation Checks

Oracle provides scripts for the following STIG installation checks.

23.3.1 DG0009

Name: Access to DBMS software files and directories should not be granted to unauthorized users.

Comment: Script provided by Oracle

23.3.2 DG0012

Name: Database software directories including DBMS configuration files are stored in dedicated directories separate from the host OS and other applications.

Comment: Script provided by Oracle

23.3.3 DG0019

Name: Application software should be owned by a Software Application account.

Comment: Script provided by Oracle

23.3.4 DG0102

Name: DBMS processes or services should run under custom, dedicated OS accounts.

Comment: Script provided by Oracle

23.3.5 DG0152

Name: DBMS network communications should comply with PPS usage restrictions.

Comment: Script provided by Oracle

23.3.6 DG0179

Name: The DBMS warning banner should meet Department of Defense (DoD) policy requirements.

Comment: Script provided by Oracle

23.3.7 DO0120

Name: The Oracle software installation account should not be granted excessive host system privileges.

Comment: Script provided by Oracle

23.3.8 DO0145

Name: OS DBA group membership should be restricted to authorized accounts.

Comment: Script provided by Oracle

23.3.9 DO0286

Name: The Oracle INBOUND_CONNECT_TIMEOUT and SQLNET.INBOUND_CONNECT_TIMEOUT parameters should be set to a value greater than 0.

Comment: Script provided by Oracle

23.3.10 DO0287

Name: The Oracle SQLNET.EXPIRE_TIME parameter should be set to a value greater than 0.

Comment: Script provided by Oracle

23.3.11 DO6740

Name: The Oracle Listener ADMIN_RESTRICTIONS parameter if present should be set to ON.

Comment: Script provided by Oracle

23.3.12 DO6746

Name: The Oracle listener.ora file should specify IP addresses rather than host names to identify hosts.

Comment: Script provided by Oracle

23.3.13 DO6751

Name: The SQLNet SQLNET.ALLOWED_LOGON_VERSION parameter should be set to a value of 10 or higher.

Comment: Script provided by Oracle.