Oracle® Enterprise Manager

Compliance Standards Reference

24ai Release 1 (24.1)
F97199-01
December 2024

Oracle Enterprise Manager Compliance Standards Reference, 24ai Release 1 (24.1)

F97199-01

Primary Author: Enterprise Manager Development Teams, Quality Assurance Teams, Customer Support Teams, and Product Management Teams.

Contributing Authors: Oracle Corporation

Contributors:

Contents

5 Host Compliance Standards

6 Oracle Access Management Server Compliance Standards

7 Oracle Database Machine Compliance Standards

8 Oracle Identity Manager Compliance Standards

12 Oracle Single Instance Database Compliance Standards

13 Oracle WebLogic Cluster Compliance Standards

14 Oracle WebLogic Domain Compliance Standards

15 Oracle WebLogic Server Compliance Standards

16 Pluggable Database Compliance Standards

19 Security Technical Implementation Guide (STIG) Compliance Standards

20 CIS Compliance Standards

Preface

Enterprise Manager 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 ships with compliance standards for Oracle hardware and software including Database, Exadata Database Machine, 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 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.

Convention	Meaning
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.

1

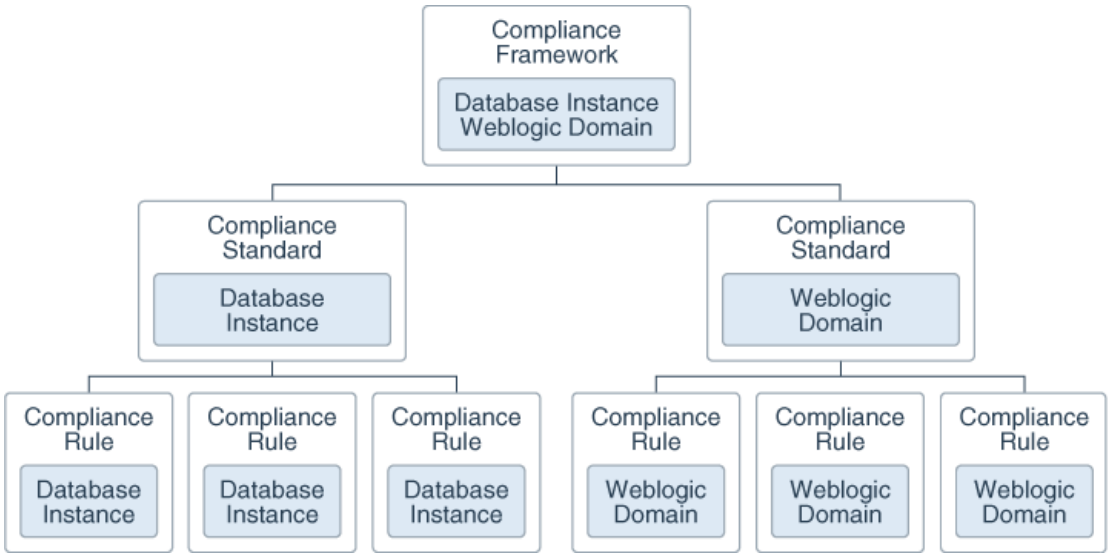
Introduction

This section provides an overview of compliance, how to use compliance standards, and how to view and understand compliance results.
Enterprise Manager 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 ships with compliance standards for Oracle hardware and software including Database, Exadata Database Machine, and more. These compliance standards validate conformance to Oracle configuration recommendations, best practices, and security recommendations.

Compliance Overview

The compliance framework in Enterprise Manager 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*.

Using Compliance Standards Provided by Oracle

Enterprise Manager 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 Using Monitoring Templates in *Oracle Enterprise Manager 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**.

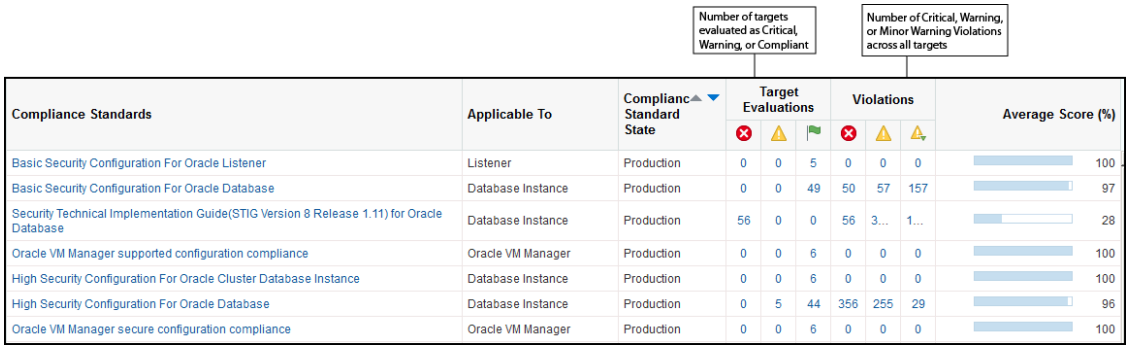
Viewing and Understanding Compliance Results

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.

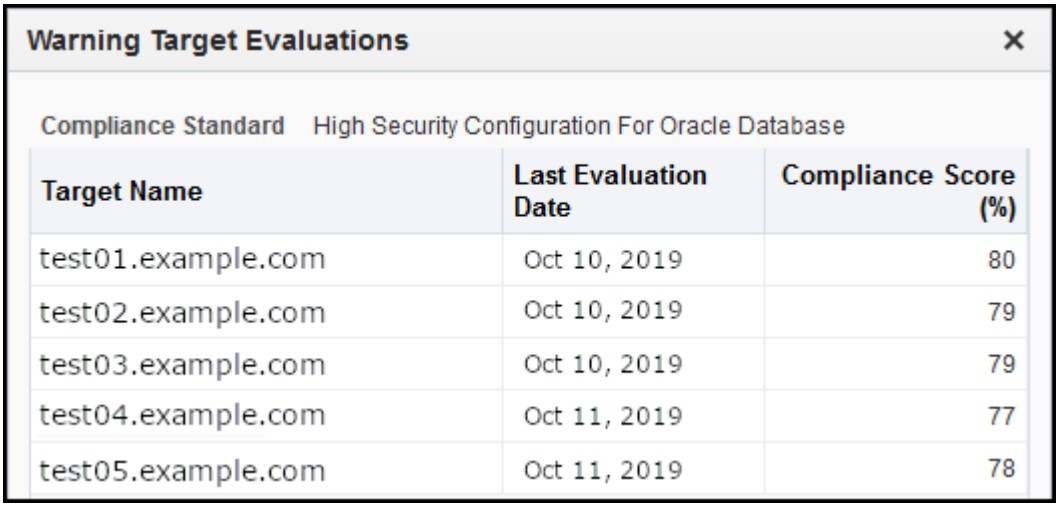
Target Evaluations

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

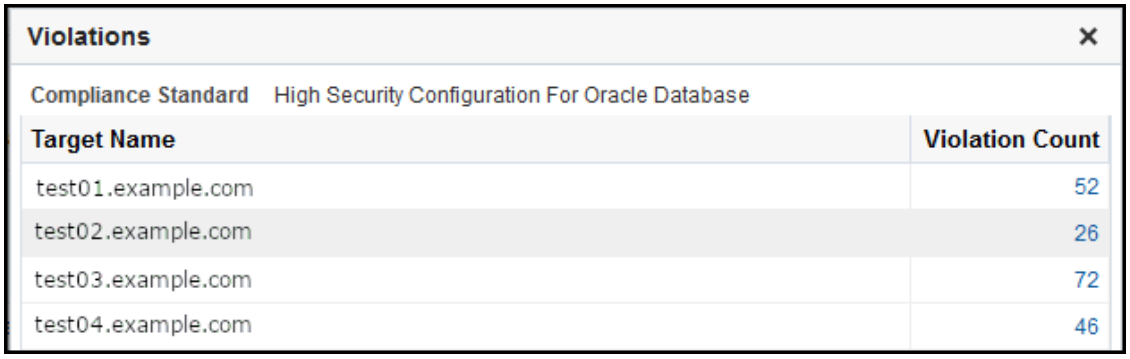
Target Name	Last Evaluation Date	Compliance Score (%)
test01.example.com	Oct 10, 2019	80
test02.example.com	Oct 10, 2019	79
test03.example.com	Oct 10, 2019	79
test04.example.com	Oct 11, 2019	77
test05.example.com	Oct 11, 2019	78

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



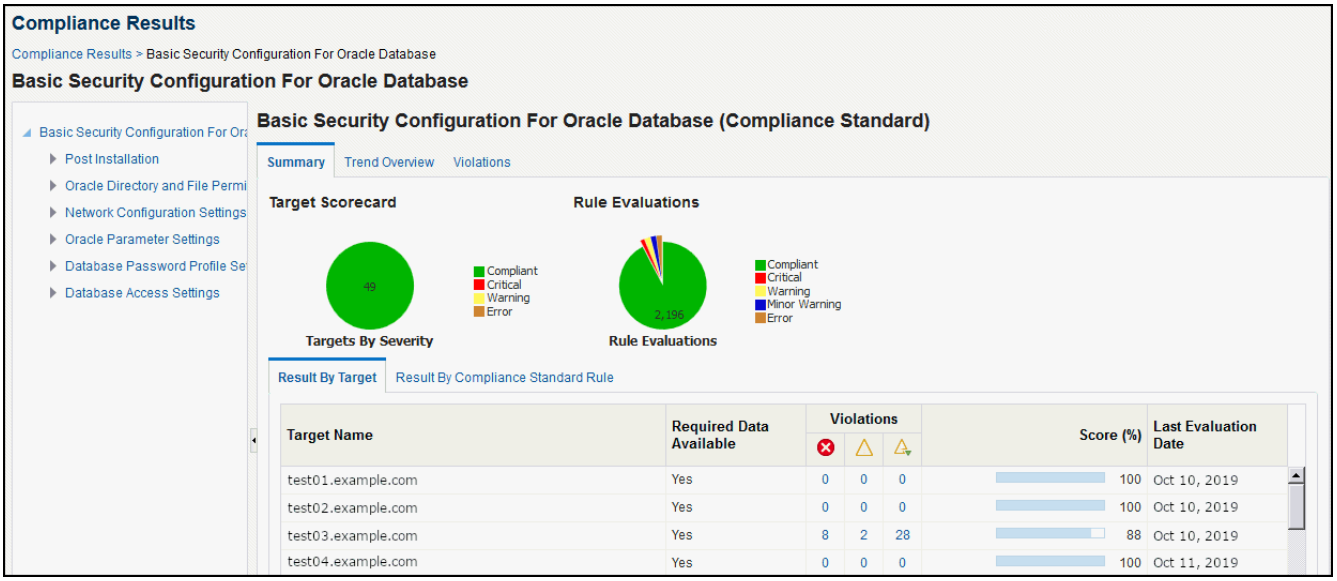
Violations

Compliance Standard High Security Configuration For Oracle Database

Target Name	Violation Count
test01.example.com	52
test02.example.com	26
test03.example.com	72
test04.example.com	46

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

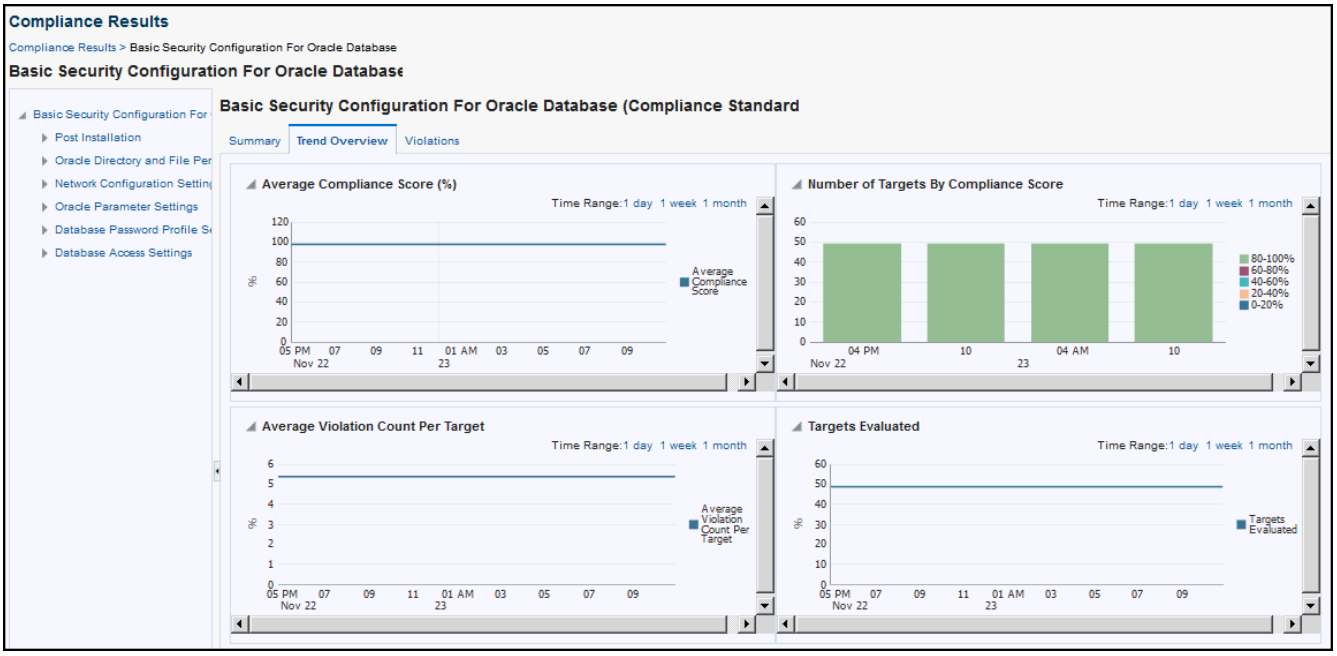
Figure 1-5 Compliance Standard Result Details - Summary



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.

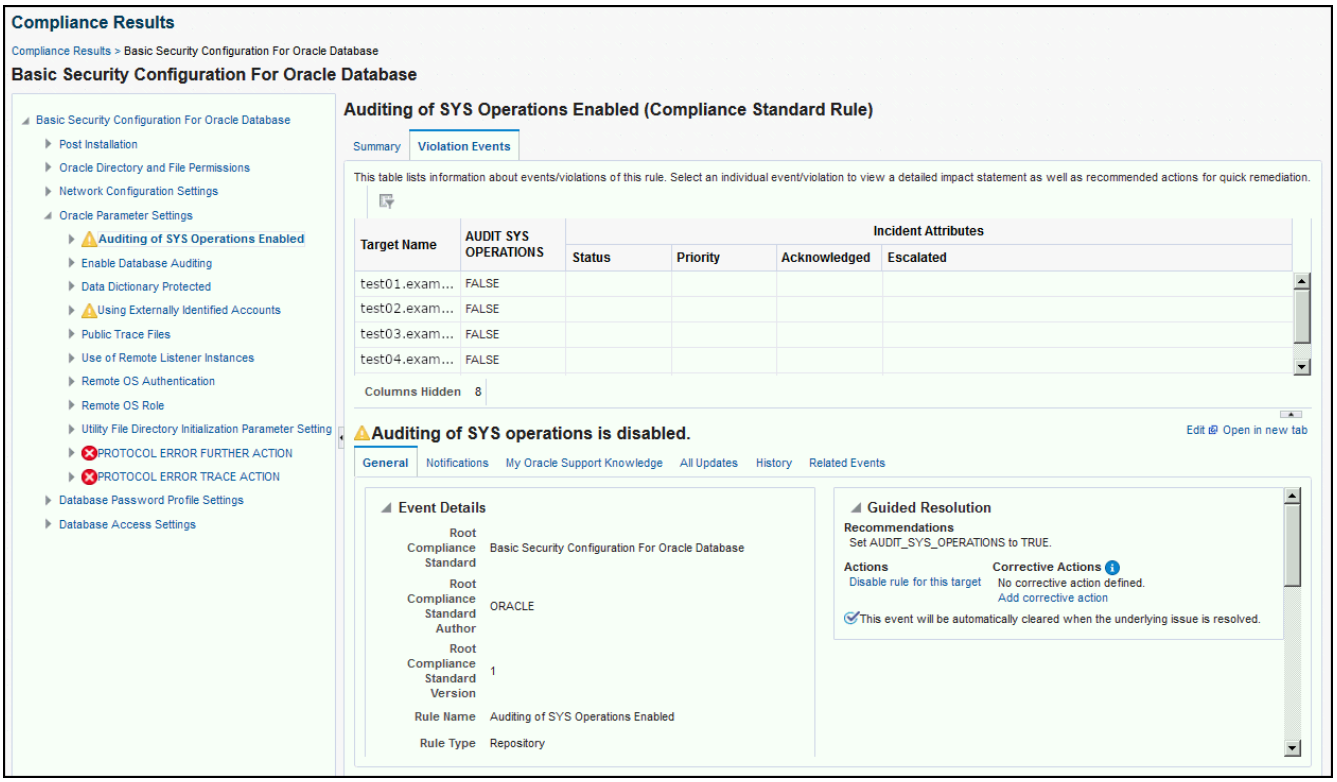
Figure 1-6 Compliance Standard Result Details - Trend Overview



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 click **Refresh** from the targets Last Collected configuration page.

Summary

Enterprise Manager 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.

Patchable Configuration For Asm

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

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

Storage Best Practices For Asm

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

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.

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.

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.

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

Patchable Configuration For Cluster

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

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

Storage Best Practices For Cluster Asm

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

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.

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.

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.

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

Host Compliance Standards

These are the compliance rules for the Host compliance standards

Configuration Monitoring For Core Linux Packages

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

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.

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.

Configuration Monitoring For Exadata Compute Node

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

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.

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.

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.

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.

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.

Configuration Monitoring For Exadata Compute Node Networking

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

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.

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.

Configuration Monitoring For Exadata Compute Node Time

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

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.

Configuration Monitoring For Network Time Linux Packages

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

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.

Configuration Monitoring For Networking Linux Packages

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

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.

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.

Configuration Monitoring For Security Linux Packages

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

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.

Configuration Monitoring For User Access Linux Packages

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

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.

File Integrity Monitoring For Exadata Compute Node

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

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.

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.

File Integrity Monitoring For Important Linux Packages

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

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.

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.

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.

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.

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.

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.

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.

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.

Secure Configuration For Host

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

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.

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.

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.

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.

Security Recommendations For Oracle Products

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

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.

6

Oracle Access Management Server Compliance Standards

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

Oracle Access Manager Server Agent Configuration Compliance

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

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.

Oracle Access Manager Server Configuration Compliance

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

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.

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

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.

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

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

7

Oracle Database Machine Compliance Standards

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

Db Machine Compliance

The compliance rules for the Db Machine Compliance standard follow.

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

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.

8

Oracle Identity Manager Compliance Standards

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

Oracle Identity Manager Server Configuration Compliance

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

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.

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.

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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

9

Oracle Identity Manager Cluster Compliance Standards

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

Oracle Identity Manager Cluster Configuration Compliance

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

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.

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

10

Oracle Listener Compliance Standards

These are the compliance rules for the Oracle Listener compliance standards

Basic Security Configuration For Oracle Listener

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

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.

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

High Security Configuration For Oracle Listener

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

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.

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

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.

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.

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.

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.

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.

Listener Logging Status

Description: Ensures that listener logging is enabled

Severity: Warning

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

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.

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.

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.

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.

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.

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.

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

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.

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.

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.

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.

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.

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

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.

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.

11

Oracle Real Application Cluster Database Compliance Standards

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

Basic Security Configuration For Oracle Cluster Database

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

Configuration Best Practices For Oracle Rac Database

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

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.

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.

High Security Configuration For Oracle Cluster Database

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

$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

$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

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.

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.

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.

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.

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.

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.

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.

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

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

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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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..

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

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.

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

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

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

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

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

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.

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.

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.

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.

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.

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.

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.

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

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.

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.

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.

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.

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.

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.

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.

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.

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

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.

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.

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.

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

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.

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.

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.

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

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.

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.

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.

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

Patchable Configuration For Rac Database

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

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

Storage Best Practices For Oracle Rac Database

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

12

Oracle Single Instance Database Compliance Standards

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

Basic Security Configuration For Oracle Cluster Database Instance

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

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

Basic Security Configuration For Oracle Database

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

Configuration Best Practices For Oracle Database

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

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.

Fast Recovery Area Location Not Set

Description: Checks whether recovery area is set

Severity: Warning

Rationale: NO_RECOVERY_AREA_IMPACT

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.

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.

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.'

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).

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.

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.

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.

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.

High Security Configuration For Oracle Cluster Database Instance

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

$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

$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

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

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.

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

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

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

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.

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.

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.

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.

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.

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.

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

High Security Configuration For Oracle Database

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

"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.

$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

$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

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.

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.

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.

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.

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.

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.

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.

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

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

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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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..

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

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.

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

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

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

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

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

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.

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.

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.

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.

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.

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.

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.

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.

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

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.

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.

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.

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

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.

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.

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.

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

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.

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.

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.

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

Patchable Configuration For Oracle Database

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

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

Storage Best Practices For Oracle Database

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

13

Oracle WebLogic Cluster Compliance Standards

These are the compliance rules for the Oracle WebLogic Cluster compliance standards

Weblogic Cluster Configuration Compliance

The compliance rules for the Weblogic Cluster Configuration Compliance standard follow.

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.

14

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.

WebLogic Domain Configuration Compliance

The compliance rules for the Weblogic Domain Configuration Compliance standard follow.

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.

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.

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.

15

Oracle WebLogic Server Compliance Standards

These are the compliance rules for the Oracle WebLogic Server compliance standards

Weblogic Server Configuration Compliance

The compliance rules for the Weblogic Server Configuration Compliance standard follow.

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.

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.

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

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.

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

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.

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.

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.

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.

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.

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.

16

Pluggable Database Compliance Standards

These are the compliance rules for the Pluggable Database compliance standards

Basic Security Configuration For Oracle Pluggable Database

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

Configuration Best Practices For Oracle Database

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

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.

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.'

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.

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.

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.

High Security Configuration For Oracle Pluggable Database

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

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.

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.

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.

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.

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.

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.

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.

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

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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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..

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

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

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

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.

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.

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.

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.

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.

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

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.

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

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.

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.

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.

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

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.

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.

Storage Best Practices For Oracle Database

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

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.

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.

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.

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.

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.

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.

17

Siebel Enterprise Compliance Standards

These are the compliance rules for the Siebel Enterprise compliance standards

Target Sync Info For Siebel

The compliance rules for the Target Sync Info For Siebel standard follow.

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.

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.

18

Systems Infrastructure Switch Compliance Standards

These are the compliance rules for the Systems Infrastructure Switch compliance standards

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.

Exadata Critical Issue Ib1-Ib3

Description: Exadata Critical Issue IB1-IB3

Severity: Critical

Rationale:

Exadata Software Version Compatibility With Infiniband Software Version

Description: Exadata software version compatibility with infiniband software version

Severity: Critical

Rationale:

Exadata Software Version Compatibility With Infiniband Software Version

Description: Exadata software version compatibility with infiniband software version

Severity: Critical

Rationale:

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.

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.

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:

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:

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:

Infiniband Switch Hostname Configuration

Description: Infiniband switch HOSTNAME configuration

Severity: Warning

Rationale:

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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).

Verify Switch Localtime Configuration Across Switches

Description: Verify switch localtime configuration across switches

Severity: Critical

Rationale:

Verify Switch Version Consistency Across Switches

Description: Verify switch version consistency across switches

Severity: Critical

Rationale:

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

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.

Exadata Software Version Compatibility With Infiniband Software Version

Description: Exadata software version compatibility with infiniband software version

Severity: Critical

Rationale:

Exadata Software Version Compatibility With Infiniband Software Version

Description: Exadata software version compatibility with infiniband software version

Severity: Critical

Rationale:

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.

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:

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:

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:

Infiniband Switch Hostname Configuration

Description: Infiniband switch HOSTNAME configuration

Severity: Warning

Rationale:

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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).

Verify Switch Localtime Configuration Across Switches

Description: Verify switch localtime configuration across switches

Severity: Critical

Rationale:

Verify Switch Version Consistency Across Switches

Description: Verify switch version consistency across switches

Severity: Critical

Rationale:

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

19

Security Technical Implementation Guide (STIG) Compliance Standards

This section explains how to use the Security Technical Implementation Guide (STIG) based compliance standards, as well as how to customize them to meet environmental-specific requirements.

About Security Technical Implementation Guide

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 Guide (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.

Table 19-1 Latest STIG Standards for Oracle Database and Oracle Cluster Database

Database Version	Latest STIG Version
19c	STIG - Version 2 Release 9 STIG - Version 2 Release 8

For detailed information on STIG, visit the Security Technical Implementation Guides (STIGs) website: https://public.cyber.mil/stigs/.

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.

> **Note:**
>
> STIG compliance standards cannot be associated with PDBs and do not include specific checks for them. Oracle recommends associating the RAC database (whether containerized or not) and its instances with STIG compliance standards. **It will not include PDBS.**

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.

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.
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**.

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 19c.

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

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.

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**.

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**.

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`.

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.

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.

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.

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

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

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. For a complete list of all rules in the DISA published STIG Version 1 for OHS 12.1.3, refer to https://public.cyber.mil/stigs/downloads/.

Oracle Database STIG Compliance Standard Modifications from Guide

The Enterprise Manager implementations of the Oracle Database 11g STIG and 12c STIG 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 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 19-2 Deviations from Oracle Database 12c, Version 1, Release 12 STIG

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.

Table 19-2 (Cont.) Deviations from Oracle Database 12c, Version 1, Release 12 STIG

STIG ID	Oracle Modification
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.
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 19-2 (Cont.) Deviations from Oracle Database 12c, Version 1, Release 12 STIG

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.
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.

Table 19-2 (Cont.) Deviations from Oracle Database 12c, Version 1, Release 12 STIG

STIG ID	Oracle Modification
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.
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 19-3 Deviations from Oracle Database 11g, V8, R8, and R11 STIG

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
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 19-4 Deviations from Oracle Database 11gR2, V1, Release 14, 15 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 19-4 (Cont.) Deviations from Oracle Database 11gR2, V1, Release 14, 15 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.
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.

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. For a complete list of all rules in the DISA published STIG Version 1 for OHS 12.1.3, refer to https://public.cyber.mil/stigs/downloads/.

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

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

STIG Rules Enhanced by Oracle

Security Technical Implementation Guidelines (STIG) rules enhanced by Oracle.

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.

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.

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.

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.

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.

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.

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'.

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','ORDPLUGINS
','ORDSYS','OUTLN','SI_INFORMTN_SCHEMA','WK_TEST','WK_SYS','WKPROXY','WMSYS','XDB','DBSNM
P','MGMT_VIEW','SYS','SYSMAN','SYSTEM','DBA','DV_ACCTMGR','DV_OWNER','RECOVERY_CATALOG_OW
NER','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'.

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.

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.

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.

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.

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.

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','GSMADMI
N_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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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'.

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'.

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.

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.

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.

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.

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.

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' ,'OLAPSY
S' ,'OUTLN' ,'OWBSYS' ,'SPATIAL_CSW_ADMIN_USR' ,'APEX_030200' ,'SCOTT' ,'APEX_PUBLIC_USER
' ,'MDDATA' ,'OE' ,'ORDPLUGINS' ,'PM' ,'SH' ,'SYSMAN' ,'BI' ,'IX' ,'ANONYMOUS' ,'SI_INFOR
MTN_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' ,'OLAPSY
```

```
S' ,'OUTLN' ,'OWBSYS' ,'SPATIAL_CSW_ADMIN_USR' ,'APEX_030200' ,'SCOTT' ,'APEX_PUBLIC_USER
' ,'MDDATA' ,'OE' ,'ORDPLUGINS' ,'PM' ,'SH' ,'SYSMAN' ,'BI' ,'IX' ,'ANONYMOUS' ,'SI_INFOR
MTN_SCHEMA','DVF','GSMADMIN_INTERNAL','APEX_040200','OJVMSYS','GSMCATUSER')
```

Change to STIG Rule: Changed query to exclude oracle default users/roles.

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.

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.

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.

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.

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.

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.

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.

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.

STIG Database Checks

The following STIG database rules are enhanced by Oracle. **Bold** text in the Collection Query denotes the change.

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

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.

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'.

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.

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.

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.

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.

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.

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.

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.

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.

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

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.

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.

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.

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.

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.

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.

STIG Installation Checks

Oracle provides scripts for the following STIG installation checks.

DG0009

Name: Access to DBMS software files and directories should not be granted to unauthorized users.

Comment: Script provided by Oracle

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

DG0019

Name: Application software should be owned by a Software Application account.

Comment: Script provided by Oracle

DG0102

Name: DBMS processes or services should run under custom, dedicated OS accounts.

Comment: Script provided by Oracle

DG0152

Name: DBMS network communications should comply with PPS usage restrictions.

Comment: Script provided by Oracle

DG0179

Name: The DBMS warning banner should meet Department of Defense (DoD) policy requirements.

Comment: Script provided by Oracle

DO0120

Name: The Oracle software installation account should not be granted excessive host system privileges.

Comment: Script provided by Oracle

DO0145

Name: OS DBA group membership should be restricted to authorized accounts.

Comment: Script provided by Oracle

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

DO0287

Name: The Oracle SQLNET.EXPIRE_TIME parameter should be set to a value greater than 0.

Comment: Script provided by Oracle

DO6740

Name: The Oracle Listener ADMIN_RESTRICTIONS parameter if present should be set to ON.

Comment: Script provided by Oracle

DO6746

Name: The Oracle listener.ora file should specify IP addresses rather than host names to identify hosts.

Comment: Script provided by Oracle

DO6751

Name: The SQLNet SQLNET.ALLOWED_LOGON_VERSION parameter should be set to a value of 10 or higher.

Comment: Script provided by Oracle.

20

CIS Compliance Standards

This section explains how to use the Center for Internet Security (CIS) Benchmarks in Enterprise Manager. CIS Benchmarks are the only consensus-based, best-practice security configuration guides both developed and accepted by government, business, industry, and academia.

About CIS Compliance Standards

Enterprise Manager supports an implementation in the form of compliance standards. These standards consist of CIS Profiles with traditional or unified auditing.

CIS Standards can be updated instantly via Self Update, for more information see: Self Update for Compliance Standards.

The currently available CIS based compliance standards are:

> **Note:**

Table 20-1 CIS Standards for Oracle Database 19c

CIS Version for Oracle Database 19c	CIS Standard Available for Enterprise Manager
CIS Oracle Database 19c Benchmark V1.2.0	• Oracle 19c Database CIS V1.2.0 - Level 1 - RDBMS using Traditional Auditing for Oracle Database • Oracle 19c Database CIS V1.2.0 - Level 1 - RDBMS using Traditional Auditing for Oracle Pluggable Database • Oracle 19c Database CIS V1.2.0 - Level 1 - RDBMS using Traditional Auditing for Oracle Cluster Database • Oracle 19c Database CIS V1.2.0 - Level 1 - RDBMS using Unified Auditing for Oracle Database • Oracle 19c Database CIS V1.2.0 - Level 1 - RDBMS using Unified Auditing for Oracle Pluggable Database • Oracle 19c Database CIS V1.2.0 - Level 1 - RDBMS using Unified Auditing for Oracle Cluster Database

Table 20-1 (Cont.) CIS Standards for Oracle Database 19c

CIS Version for Oracle Database 19c	CIS Standard Available for Enterprise Manager
CIS Oracle Database 19c Benchmark V1.1.0	• Oracle 19c Database CIS V1.1.0 - Level 1 - RDBMS using Traditional Auditing for Oracle Database • Oracle 19c Database CIS V1.1.0 - Level 1 - RDBMS using Traditional Auditing for Oracle Pluggable Database • Oracle 19c Database CIS V1.1.0 - Level 1 - RDBMS using Traditional Auditing for Oracle Cluster Database • Oracle 19c Database CIS V1.1.0 - Level 1 - RDBMS using Unified Auditing for Oracle Database • Oracle 19c Database CIS V1.1.0 - Level 1 - RDBMS using Unified Auditing for Oracle Pluggable Database • Oracle 19c Database CIS V1.1.0 - Level 1 - RDBMS using Unified Auditing for Oracle Cluster Database
CIS Oracle Database 19c Benchmark V1.0.0	• Oracle 19c Database CIS V1.0.0 - Level 1 - RDBMS using Traditional Auditing for Oracle Database • Oracle 19c Database CIS V1.0.0 - Level 1 - RDBMS using Traditional Auditing for Oracle Pluggable Database • Oracle 19c Database CIS V1.0.0 - Level 1 - RDBMS using Traditional Auditing for Oracle Cluster Database • Oracle 19c Database CIS V1.0.0 - Level 1 - RDBMS using Unified Auditing for Oracle Database • Oracle 19c Database CIS V1.0.0 - Level 1 - RDBMS using Unified Auditing for Oracle Pluggable Database • Oracle 19c Database CIS V1.0.0 - Level 1 - RDBMS using Unified Auditing for Oracle Cluster Database

Associating CIS Compliance Standards Targets

Associate the target to the CIS compliance standard to determine whether the target satisfies to the CIS compliance standard.

> **Note:**
>
> CIS compliance standards can provide checks for the PDBs, to associate ensure the following are met:
>
> - Minimum CIS compliance standard of Oracle 12c Database CIS v3.1.0, or Oracle 19c Database CIS V1.2.0
> - The RAC is a container:
>   - It is recommended to associate it with all instances in the RAC
>   - It is recommended to associate it with all PDBs in RAC

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Select the **Compliance Standards** tab and select the CIS standard.
3. Select the Oracle Database or RAC and click **Associate Targets**.
4. Click **Add** and select the targets you want to monitor. The targets appear in the table after you close the selector dialog.
5. Click **OK** then confirm that you want to save the association. The association internally deploys the necessary configuration extensions 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**.

Oracle Database Installation and Patching Requirements

One of the best ways to ensure secure Oracle security is to implement Critical Patch Updates (CPUs) as they come out, along with any applicable OS patches that will not interfere with system operations. It is additionally prudent to remove Oracle sample data from production environments.

Ensure All Default Passwords Are Changed (Scored)

Default passwords should not be used by Oracle database users.

Remediation

To remediate this recommendation, you may perform either of the following actions:

- Manually issue the following SQL statement for each USERNAME returned in the Audit Procedure:

```
PASSWORD <username>
```

- Execute the following SQL script to assign a randomly generated password to each account using a default password:

```
begin
    for r_user in
        (select username from dba_users_with_defpwd where username not like
'%XS$NULL%')
    loop
        DBMS_OUTPUT.PUT_LINE('Password for user '||r_user.username||' will be
changed.');
```

```
        execute immediate 'alter user "'||r_user.username||'" identified by "'||
DBMS_RANDOM.string('a',16)||'"account lock password expire';
    end loop;
end;
```

Ensure All Sample Data And Users Have Been Removed (Scored)

Oracle sample schemas can be used to create sample users (BI,HR,IX,OE,PM,SCOTT,SH), with well-known default passwords, particular views, and procedures/functions, in addition to tables and fictitious data. The sample schemas should be removed.

Remediation

To remediate this setting, execute the following SQL script:

```
$ORACLE_HOME/demo/schema/drop_sch.sql
```

Then, execute the following SQL statement.

```
DROP USER SCOTT CASCADE;
```

> **Note:**
>
> The recyclebin is not set to OFF within the default drop script, which means that the data will still be present in your environment until the recyclebin is emptied.

Impact

The Oracle sample user names may be in use on a production basis. It is important that you first verify that `BI, HR, IX, OE, PM, SCOTT`, and/or `SH` are not valid production user names before executing the dropping SQL scripts. This may be particularly true with the `HR` and `BI` users. If any of these users are present, it is important to be cautious and confirm the schema present are, in fact, Oracle sample schema and not production schema being relied upon by business operations.

Oracle Parameter Settings

The operation of the Oracle database instance is governed by numerous parameters that are set in specific configuration files and are instance-specific in scope. As alterations of these parameters can cause problems ranging from denial-of-service to theft of proprietary information, these configurations should be carefully considered and maintained.

> **Note:**
>
> For all files that have parameters that can be modified with the OS and/or SQL commands/scripts, these will both be listed where appropriate.

Listener Settings

This section defines recommendations for the settings for the TNS Listener `listener.ora` file.

Ensure 'SECURE_CONTROL_' Is Set In 'listener.ora' (Scored)

The `SECURE_CONTROL_<listener_name>` setting determines the type of control connection the Oracle server requires for remote configuration of the listener.

Remediation

To remediate this recommendation:

Set the `SECURE_CONTROL_<listener_name>` for each defined listener in the `listener.ora` file.

Ensure 'extproc' Is Not Present in 'listener.ora' (Scored)

`extproc` should be removed from the `listener.ora` to mitigate the risk that OS libraries can be invoked by the Oracle instance.

Remediation

To remediate this recommendation:

Remove `extproc` from the `listener.ora` file.

Ensure 'ADMIN_RESTRICTIONS_' Is Set to 'ON' (Scored)

The `admin_restrictions_<listener_name>` setting in the `listener.ora` file can require that any attempted real-time alteration of the parameters in the `listener` via the `set` command file be refused unless the `listener.ora` file is manually altered, then restarted by a privileged user.

Remediation

To remediate this recommendation:

Use a text editor such as `vi` to set the `admin_restrictions_<listener_name>` to the value ON.

Ensure 'SECURE_REGISTER_' Is Set to 'TCPS' or 'IPC' (Scored)

The `SECURE_REGISTER_<listener_name>` setting specifies the protocols used to connect to the TNS listener. Each setting should have a value of either `TCPS` or `IPC` based on the needs for its protocol.

Remediation

To remediate this recommendation:

Use a text editor such as `vi` to set the `SECURE_REGISTER_<listener_name>=TCPS` or `SECURE_REGISTER_<listener_name>=IPC` for each listener found in `$ORACLE_HOME/network/admin/listener.ora`.

Database Settings

This section defines recommendations covering the general security configuration of the database instance. The recommendations ensure auditing is enabled, listeners are appropriately confined, and authentication is appropriately configured.

> **Note:**
>
> The remediation procedures assume the use of a server parameter file, which is often a preferred method of storing server initialization parameters.

For your environment, leaving off the SCOPE = SPFILE directive or substituting it with SCOPE = BOTH might be preferred depending on the recommendation.

Ensure 'AUDIT_SYS_OPERATIONS' Is Set to 'TRUE' (Scored)

The `AUDIT_SYS_OPERATIONS` setting provides for the auditing of all user activities conducted under the `SYSOPER` and `SYSDBA` accounts. The setting should be set to `TRUE` to enable this auditing.

Remediation

To remediate this setting, execute the following SQL statement:

```
ALTER SYSTEM SET AUDIT_SYS_OPERATIONS = TRUE SCOPE=SPFILE;
```

Ensure 'AUDIT_TRAIL' Is Set to 'DB', 'XML', 'OS', 'DB,EXTENDED', or 'XML,EXTENDED' (Scored)

The `audit_trail` setting determines whether or not Oracle's basic audit features are enabled. It can be set to "Operating System"(OS); `DB; DB,EXTENDED; XML;` or `XML,EXTENDED`. The value should be set according to the needs of the organization.

Remediation

To remediate this setting, execute one of the following SQL statements.

```
ALTER SYSTEM SET AUDIT_TRAIL = DB, EXTENDED SCOPE = SPFILE;

ALTER SYSTEM SET AUDIT_TRAIL = OS SCOPE = SPFILE;

ALTER SYSTEM SET AUDIT_TRAIL = XML, EXTENDED SCOPE = SPFILE;

ALTER SYSTEM SET AUDIT_TRAIL = DB SCOPE = SPFILE;

ALTER SYSTEM SET AUDIT_TRAIL = XML SCOPE = SPFILE;
```

Ensure 'GLOBAL_NAMES' Is Set to 'TRUE' (Scored)

The `global_names` setting requires that the name of a database link matches that of the remote database it will connect to. This setting should have a value of `TRUE`.

Remediation

To remediate this setting, execute the following SQL statement:

```
ALTER SYSTEM SET GLOBAL_NAMES = TRUE SCOPE = SPFILE;
```

Ensure 'O7_DICTIONARY_ACCESSIBILITY' Is Set to 'FALSE' (Scored)

The `O7_dictionary_accessibility` setting is a database initialization parameter that allows/disallows access to objects with the * `ANY` * privileges (`SELECT ANY TABLE, DELETE ANY TABLE, EXECUTE ANY PROCEDURE`, etc.). This functionality was created for the ease of migration from Oracle 7 databases to later versions. The setting should have a value of `FALSE`.

Remediation

To remediate this setting, execute the following SQL statement:

```
ALTER SYSTEM SET O7_DICTIONARY_ACCESSIBILITY=FALSE SCOPE = SPFILE;
```

> **Note:**
>
> The value for this is "O(oh)7" not "0(Zero)7" for O7. Also, for "Oracle Applications" up to version 11.5.9, this setting is reversed; the `O7_dictionary_accessibility=TRUE` value is required for correct operations.

Ensure 'OS_ROLES' Is Set to 'FALSE' (Scored)

The `os_roles` setting permits externally created groups to be applied to database management.

Remediation

To remediate this setting, execute the following SQL statement:

```
ALTER SYSTEM SET OS_ROLES = FALSE SCOPE = SPFILE;
```

Ensure 'REMOTE_LISTENER' Is Empty (Scored)

The `remote_listener` setting determines whether or not a valid listener can be established on a system separate from the database instance. This setting should be empty unless the organization specifically needs a valid listener on a separate system.

Remediation

To remediate this setting, execute the following SQL statement.

```
ALTER SYSTEM SET REMOTE_LISTENER = '' SCOPE = SPFILE;
```

> **Note:**
>
> If set as `remote_listener=true`, the address/address list is taken from the `TNSNAMES.ORA` file.

Ensure 'REMOTE_LOGIN_PASSWORDFILE' Is Set to 'NONE' (Scored)

The `remote_login_passwordfile` setting specifies whether or not Oracle checks for a password file during login and how many databases can use the password file. The setting should have a value of `NONE`.

Remediation

To remediate this setting, execute the following SQL statement.

```
ALTER SYSTEM SET REMOTE_LOGIN_PASSWORDFILE = 'NONE' SCOPE = SPFILE;
```

Ensure 'REMOTE_OS_AUTHENT' Is Set to 'FALSE' (Scored)

The `remote_os_authent` setting determines whether or not OS 'roles' with the attendant privileges are allowed for remote client connections. This setting should have a value of `FALSE`.

Remediation

To remediate this setting, execute the following SQL statement.

```
ALTER SYSTEM SET REMOTE_OS_AUTHENT = FALSE SCOPE = SPFILE;
```

Ensure 'REMOTE_OS_ROLES' Is Set to 'FALSE' (Scored)

The `remote_os_roles` setting permits remote users' OS roles to be applied to database management. This setting should have a value of `FALSE`.

Remediation

To remediate this setting, execute the following SQL statement.

```
ALTER SYSTEM SET REMOTE_OS_ROLES = FALSE SCOPE = SPFILE;
```

Ensure 'UTL_FILE_DIR' Is Empty (Scored)

The `utl_file_dir` setting allows packages like `utl_file` to access (read/write/modify/delete) files specified in `utl_file_dir`. This setting should have an empty value.

Remediation

To remediate this setting, execute the following SQL statement.

```
ALTER SYSTEM SET UTL_FILE_DIR = '' SCOPE = SPFILE;
```

Ensure 'SEC_CASE_SENSITIVE_LOGON' Is Set to 'TRUE' (Scored)

The `SEC_CASE_SENSITIVE_LOGON` information determines whether or not case-sensitivity is required for passwords during login.

Remediation

To remediate this setting, execute the following SQL statement.

```
ALTER SYSTEM SET SEC_CASE_SENSITIVE_LOGON = TRUE SCOPE = SPFILE;
```

Ensure 'SEC_MAX_FAILED_LOGIN_ATTEMPTS' Is '3' or Less (Scored)

The `SEC_MAX_FAILED_LOGIN_ATTEMPTS` parameter determines how many failed login attempts are allowed before Oracle closes the login connection.

Remediation

To remediate this setting, execute the following SQL statement.

```
ALTER SYSTEM SET SEC_MAX_FAILED_LOGIN_ATTEMPTS = 3 SCOPE = SPFILE;
```

Ensure 'SEC_PROTOCOL_ERROR_FURTHER_ACTION' Is Set to 'DROP,3' (Scored)

The `SEC_PROTOCOL_ERROR_FURTHER_ACTION` setting determines the Oracle's server's response to bad/malformed packets received from the client. This setting should have a value of `DROP,3`, which will cause a connection to be dropped after three bad/malformed packets.

Remediation

To remediate this setting, execute the following SQL statement.

```
ALTER SYSTEM SET SEC_PROTOCOL_ERROR_FURTHER_ACTION = 'DROP,3' SCOPE = SPFILE;
```

Ensure 'SEC_PROTOCOL_ERROR_TRACE_ACTION' Is Set to 'LOG' (Scored)

The `SEC_PROTOCOL_ERROR_TRACE_ACTION` setting determines the Oracle's server's logging response level to bad/malformed packets received from the client by generating `ALERT`, `LOG`, or `TRACE` levels of detail in the log files. This setting should have a value of `LOG` unless the organization has a compelling reason to use a different value because `LOG` should cause the necessary information to be logged. Setting the value as `TRACE` can generate an enormous amount of log output and should be reserved for debugging only.

Remediation

To remediate this setting, execute the following SQL statement.

```
ALTER SYSTEM SET SEC_PROTOCOL_ERROR_TRACE_ACTION=LOG SCOPE = SPFILE;
```

Ensure 'SEC_RETURN_SERVER_RELEASE_BANNER' Is Set to 'FALSE' (Scored)

The information about patch/update release number provides information about the exact patch/update release that is currently running on the database. This is sensitive information that should not be revealed to anyone who requests it.

Remediation

To remediate this setting, execute the following SQL statement.

```
ALTER SYSTEM SET SEC_RETURN_SERVER_RELEASE_BANNER = FALSE SCOPE = SPFILE;
```

Ensure 'SQL92_SECURITY' Is Set to 'TRUE' (Scored)

The SQL92_SECURITY parameter setting TRUE requires that a user must also be granted the SELECT object privilege before being able to perform UPDATE or DELETE operations on tables that have WHERE or SET clauses. The setting should have a value of TRUE.

Remediation

To remediate this setting, execute the following SQL statement.

```
ALTER SYSTEM SET SQL92_SECURITY = TRUE SCOPE = SPFILE;
```

Ensure '_trace_files_public' Is Set to 'FALSE' (Scored)

The _trace_files_public setting determines whether or not the system's trace file is world readable. This setting should have a value of FALSE to restrict trace file access.

Remediation

To remediate this setting, execute the following SQL statement.

```
ALTER SYSTEM SET "_trace_files_public" = FALSE SCOPE = SPFILE;
```

Ensure 'RESOURCE_LIMIT' Is Set to 'TRUE' (Scored)

RESOURCE_LIMIT determines whether resource limits are enforced in database profiles. This setting should have a value of TRUE.

Remediation

To remediate this setting, execute the following SQL statement.

```
ALTER SYSTEM SET RESOURCE_LIMIT = TRUE SCOPE = SPFILE;
```

Default Value: FALSE

Oracle Connection and Login Restrictions

The restrictions on Client/User connections to the Oracle database help block unauthorized access to data and services by setting access rules. These security measures help to ensure that successful logins cannot be easily made through brute-force password attacks or intuited by clever social engineering exploits. Settings are generally recommended to be applied to all defined profiles rather than by using only the DEFAULT profile. All values assigned below are the recommended minimums or maximums; higher, more restrictive values can be applied at the discretion of the organization by creating a separate profile to assign to a different user group.

Ensure 'FAILED_LOGIN_ATTEMPTS' Is Less than or Equal to '5' (Scored)

The FAILED_LOGIN_ATTEMPTS setting determines how many failed login attempts are permitted before the system locks the user's account. While different profiles can have different

and more restrictive settings, such as USERS and APPS, the minimum(s) recommended here should be set on the DEFAULT profile.

Remediation

Remediate this setting by executing the following SQL statement for each PROFILE returned by the audit procedure.

```
ALTER PROFILE <profile_name> LIMIT FAILED_LOGIN_ATTEMPTS 5;
```

> **Note:**
>
> One great concern with the above is the possibility of this setting being exploited to craft a DDoS attack by using the row-locking delay between failed login attempts (see _Oracle Bug 7715339 – Logon failures causes “row cache lock” waits – Allow disable of logon delay [ID 7715339.8], so the configuration of this setting depends on using the bug workaround). Also, while the setting for the FAILED_LOGIN_ATTEMPTS value can also be set in sqlnet.ora, this only applies to listed users. The similar setting used to block a DDoS, the SEC_MAX_FAILED_LOGIN_ATTEMPTS initialization parameter, can be used to protect unauthorized intruders from attacking the server processes for applications, but this setting does not protect against unauthorized attempts via valid usernames.

Ensure 'PASSWORD_LOCK_TIME' Is Greater than or Equal to '1' (Scored)

The PASSWORD_LOCK_TIME setting determines how many days must pass for the user's account to be unlocked after the set number of failed login attempts has occurred. The suggested value for this is one day or greater.

Remediation

Remediate this setting by executing the following SQL statement for each PROFILE returned by the audit procedure.

```
ALTER PROFILE <profile_name> LIMIT PASSWORD_LOCK_TIME 1;
```

Ensure 'PASSWORD_LIFE_TIME' Is Less than or Equal to '90' (Scored)

The PASSWORD_LIFE_TIME setting determines how long a password may be used before the user is required to be change it. The suggested value for this is 90 days or less.

Remediation

Remediate this setting by executing the following SQL statement for each PROFILE returned by the audit procedure.

```
ALTER PROFILE <profile_name> LIMIT PASSWORD_LIFE_TIME 90;
```

Ensure 'PASSWORD_REUSE_MAX' Is Greater than or Equal to '20' (Scored)

The `PASSWORD_REUSE_MAX` setting determines how many different passwords must be used before the user is allowed to reuse a prior password. The suggested value for this is 20 passwords or greater.

Remediation

Remediate this setting by executing the following SQL statement for each `PROFILE` returned by the audit procedure.

```
ALTER PROFILE <profile_name> LIMIT PASSWORD_REUSE_MAX 20;
```

Ensure 'PASSWORD_REUSE_TIME' Is Greater than or Equal to '365' (Scored)

The `PASSWORD_REUSE_TIME` setting determines the amount of time in days that must pass before the same password may be reused. The suggested value for this is 365 days or greater.

Remediation

Remediate this setting by executing the following SQL statement for each `PROFILE` returned by the audit procedure.

```
ALTER PROFILE <profile_name> LIMIT PASSWORD_REUSE_TIME 365;
```

Ensure 'PASSWORD_GRACE_TIME' Is Less than or Equal to '5' (Scored)

The `PASSWORD_GRACE_TIME` setting determines how many days can pass after the user's password expires before the user's login capability is automatically locked out. The suggested value for this is five days or less.

Remediation

Remediate this setting by executing the following SQL statement for each `PROFILE` returned by the audit procedure.

```
ALTER PROFILE <profile_name> LIMIT PASSWORD_GRACE_TIME 5;
```

Ensure 'DBA_USERS.PASSWORD' Is Not Set to 'EXTERNAL' for Any User (Scored)

The `password='EXTERNAL'` setting determines whether or not a user can be authenticated by a remote OS to allow access to the database with full authorization. This setting should not be used.

Remediation

Remediate this setting by executing the following SQL statement for each `PROFILE` returned by the audit procedure.

```
ALTER USER <username> INDENTIFIED BY <password>;
```

> **Note:**
>
> The PASSWORD keyword (column) used in the SQL for prior Oracle versions has been deprecated from version 11.2 onward in favor of the new AUTHENTICATION_TYPE keyword (column) for the DBA_USERS table. However, the PASSWORD column has still been retained for backward compatibility.

Ensure 'PASSWORD_VERIFY_FUNCTION' Is Set for All Profiles (Scored)

The PASSWORD_VERIFY_FUNCTION determines password settings requirements when a user password is changed at the SQL command prompt. It should be set for all profiles. Note that this setting does not apply for users managed by the Oracle password file.

Remediation

Create a custom password verification function which fulfills the password requirements of the organization.

Ensure 'SESSIONS_PER_USER' Is Less than or Equal to '10' (Scored)

The SESSIONS_PER_USER setting determines the maximum number of user sessions that are allowed to be open concurrently. The suggested value for this is 10 or less.

Remediation

To remediate this setting, execute the following SQL statement for each PROFILE returned by the audit procedure.

```
ALTER PROFILE <profile_name> LIMIT SESSIONS_PER_USER 10;
```

> **Note:**
>
> The SESSIONS_PER_USER profile management capability was created to prevent resource(s) exhaustion at a time when resource usage was very expensive. As current database design may require much higher limits on this parameter if one "user" handles all processing for specific types of batch/customer connections, this must be handled via a new user profile.

Oracle User Access and Authorization Restrictions

The capability to use database resources at a given level, or user authorization rules, allows for user manipulation of the various parts of the Oracle database. These authorizations must be structured to block unauthorized use and/or corruption of vital data and services by setting restrictions on user capabilities, particularly those of the user PUBLIC. Such security measures help to ensure successful logins cannot be easily redirected.

> **Note:**
>
> Use caution when revoking privileges from PUBLIC. Oracle and third-party products explicitly require default grants to PUBLIC for commonly used functions, objects, and in view definitions. After revoking any privilege from PUBLIC, verify that applications keep running properly and recompile invalid database objects. Specific grants to users and roles may be needed to make all objects valid. Please see the following Oracle support document which provides further information and SQL statements that can be used to determine dependencies that require explicit grants: Be Cautious When Revoking Privileges Granted to PUBLIC (Doc ID 247093.1) Always test database changes in development and test environments before making changes to production databases.

Default Public Privileges for Packages and Object Types

This section contains recommendations that revoke default public execute privileges from powerful packages and object types.

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'DBMS_ADVISOR' (Scored)

The Oracle database DBMS_ADVISOR package can be used to write files located on the server where the Oracle instance is installed. The user PUBLIC should not be able to execute DBMS_ADVISOR.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON DBMS_ADVISOR FROM PUBLIC;
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'DBMS_CRYPTO' (Scored)

The DBMS_CRYPTO settings provide a toolset that determines the strength of the encryption algorithm used to encrypt application data and is part of the SYS schema. The DES (56-bit key), 3DES (168-bit key), 3DES-2KEY (112-bit key), AES (128/192/256-bit keys), and RC4 are available. The user PUBLIC should not be able to execute DBMS_CRYPTO.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON DBMS_CRYPTO FROM PUBLIC;
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'DBMS_JAVA' (Scored)

The Oracle database DBMS_JAVA package can run Java classes (e.g. OS commands) or grant Java privileges. The user PUBLIC should not be able to execute DBMS_JAVA.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON DBMS_JAVA FROM PUBLIC;
```

> **Note:**
>
> DBMS_JAVA_TEST is an undocumented PL/SQL package, but the public grant should be revoked.

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'DBMS_JAVA_TEST' (Scored)

The Oracle database DBMS_JAVA_TEST package can run Java classes (e.g. OS commands) or grant Java privileges. The user PUBLIC should not be able to execute DBMS_JAVA_TEST.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON DBMS_JAVA_TEST FROM PUBLIC;
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'DBMS_JOB' (Scored)

The Oracle database DBMS_JOB package schedules and manages the jobs sent to the job queue and has been superseded by the DBMS_SCHEDULER package, even though DBMS_JOB has been retained for backwards compatibility. The user PUBLIC should not be able to execute DBMS_JOB.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON DBMS_JOB FROM PUBLIC
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'DBMS_LDAP' (Scored)

The Oracle database DBMS_LDAP package contains functions and procedures that enable programmers to access data from LDAP servers. The user PUBLIC should not be able to execute DBMS_LDAP.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON DBMS_LDAP FROM PUBLIC;
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'DBMS_LOB' (Scored)

The Oracle database DBMS_LOB package provides subprograms that can manipulate and read/write on BLOBs, CLOBs, NCLOBs, BFILEs, and temporary LOBs. The user PUBLIC should not be able to execute DBMS_LOB.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON DBMS_LOB FROM PUBLIC;
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'DBMS_OBFUSCATION_TOOLKIT' (Scored)

The DBMS_OBFUSCATION_TOOLKIT provides one of the tools that determine the strength of the encryption algorithm used to encrypt application data and is part of the SYS schema. The DES (56-bit key) and 3DES (168-bit key) are the only two types available. The user PUBLIC should not be able to execute DBMS_OBFUSCATION_TOOLKIT.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON DBMS_OBFUSCATION_TOOLKIT FROM PUBLIC;
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'DBMS_RANDOM' (Scored)

The Oracle database DBMS_RANDOM package is used for generating random numbers but should not be used for cryptographic purposes. The user PUBLIC should not be able to execute DBMS_RANDOM.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON DBMS_RANDOM FROM PUBLIC;
```

> **Note:**
>
> The OEM cautions that removing this from PUBLIC may break certain applications.

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'DBMS_SCHEDULER' (Scored)

The Oracle database DBMS_SCHEDULER package schedules and manages the database and operating system jobs. The user PUBLIC should not be able to execute DBMS_SCHEDULER.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON DBMS_SCHEDULER FROM PUBLIC;
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'DBMS_SQL' (Scored)

The Oracle database DBMS_SQL package is used for running dynamic SQL statements. The user PUBLIC should not be able to execute DBMS_SQL.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON DBMS_SQL FROM PUBLIC;
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'DBMS_XMLGEN' (Scored)

The DBMS_XMLGEN package takes an arbitrary SQL query as input, converts it to XML format, and returns the result as a CLOB. The user PUBLIC should not be able to execute DBMS_XMLGEN.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON DBMS_XMLGEN FROM PUBLIC;
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'DBMS_XMLQUERY' (Scored)

The Oracle package DBMS_XMLQUERY takes an arbitrary SQL query, converts it to XML format, and returns the result. This package is similar to DBMS_XMLGEN. The user PUBLIC should not be able to execute DBMS_XMLQUERY.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON DBMS_XMLQUERY FROM PUBLIC;
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'UTL_FILE' (Scored)

The Oracle database UTL_FILE package can be used to read/write files located on the server where the Oracle instance is installed. The user PUBLIC should not be able to execute UTL_FILE.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON UTL_FILE FROM PUBLIC;
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'UTL_INADDR' (Scored)

The Oracle database UTL_INADDR package can be used to create specially crafted error messages or send information via DNS to the outside. The user PUBLIC should not be able to execute UTL_INADDR.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON UTL_INADDR FROM PUBLIC;
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'UTL_TCP' (Scored)

The Oracle database UTL_TCP package can be used to read/write file to TCP sockets on the server where the Oracle instance is installed. The user PUBLIC should not be able to execute UTL_TCP.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON UTL_TCP FROM PUBLIC;
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'UTL_MAIL' (Scored)

The Oracle database `UTL_MAIL` package can be used to send email from the server where the Oracle instance is installed. The user `PUBLIC` should not be able to execute `UTL_MAIL`.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON UTL_MAIL FROM PUBLIC;
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'UTL_SMTP' (Scored)

The Oracle database `UTL_SMTP` package can be used to send email from the server where the Oracle instance is installed. The user `PUBLIC` should not be able to execute `UTL_SMTP`.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON UTL_SMTP FROM PUBLIC;
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'UTL_DBWS' (Scored)

The Oracle database `UTL_DBWS` package can be used to read/write file to web-based applications on the server where the Oracle instance is installed. This package is not automatically installed for security reasons. The user `PUBLIC` should not be able to execute `UTL_DBWS`.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON UTL_DBWS FROM PUBLIC;
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'UTL_ORAMTS' (Scored)

The Oracle database `UTL_ORAMTS` package can be used to perform HTTP requests. This could be used to send information to the outside. The user `PUBLIC` should not be able to execute `UTL_ORAMTS`.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON UTL_ORAMTS FROM PUBLIC;
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'UTL_HTTP' (Scored)

The Oracle database `UTL_HTTP` package can be used to perform HTTP requests. This could be used to send information to the outside. The user `PUBLIC` should not be able to execute `UTL_HTTP`.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON UTL_HTTP FROM PUBLIC;
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'HTTPURITYPE' (Scored)

The Oracle database `HTTPURITYPE` object type can be used to perform HTTP requests. The user `PUBLIC` should not be able to execute `HTTPURITYPE`.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON HTTPURITYPE FROM PUBLIC;
```

Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_XMLSTORE' (Scored)

The `DBMS_XLMSTORE` package provides XML functionality. It accepts a table name and XML as input to perform DML operations against the table. The user `PUBLIC` should not be able to execute `DBMS_XLMSTORE`.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON DBMS_XMLSTORE FROM PUBLIC;
```

Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_XMLSAVE' (Scored)

The `DBMS_XLMSTORE` package provides XML functionality. It accepts a table name and XML as input and then inserts into or updates that table. The user `PUBLIC` should not be able to execute `DBMS_XLMSAVE`.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON DBMS_XMLSAVE FROM PUBLIC;
```

Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_REDACT' (Scored)

The `DBMS_REDACT` package provides an interface to Oracle Data Redaction, which enables you to mask (redact) data that is returned from queries issued by low-privileged users or an application. The user `PUBLIC` should not be able to execute `DBMS_REDACT`.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON DBMS_REDACT FROM PUBLIC;
```

Revoke Non-Default Privileges for Packages and Object Types

The recommendations within this section revoke excessive privileges for packages and object types.

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'DBMS_SYS_SQL' (Scored)

The Oracle database DBMS_SYS_SQL package is shipped as undocumented. The user PUBLIC should not be able to execute DBMS_SYS_SQL.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON DBMS_SYS_SQL FROM PUBLIC;
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'DBMS_BACKUP_RESTORE' (Scored)

The Oracle database DBMS_BACKUP_RESTORE package is used for applying PL/SQL commands to the native RMAN sequences. The user PUBLIC should not be able to execute DBMS_BACKUP_RESTORE.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON DBMS_BACKUP_RESTORE FROM PUBLIC;
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'DBMS_AQADM_SYSCALLS' (Scored)

The Oracle database DBMS_AQADM_SYSCALLS package is shipped as undocumented. The user PUBLIC should not be able to execute DBMS_AQADM_SYSCALLS.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON DBMS_AQADM_SYSCALLS FROM PUBLIC;
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'DBMS_REPCAT_SQL_UTL' (Scored)

The Oracle database DBMS_REPCAT_SQL_UTL package is shipped as undocumented and allows to run SQL commands as user SYS. The user PUBLIC should not be able to execute DBMS_REPCAT_SQL_UTL.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON DBMS_REPCAT_SQL_UTL FROM PUBLIC;
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'INITJVMAUX' (Scored)

The Oracle database INITJVMAUX package is shipped as undocumented and allows to run SQL commands as user SYS. The user PUBLIC should not be able to execute INITJVMAUX.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON INITJVMAUX FROM PUBLIC;
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'DBMS_STREAMS_ADM_UTL' (Scored)

The Oracle database `DBMS_STREAMS_ADM_UTL` package is shipped as undocumented and allows to run SQL commands as user SYS. The user `PUBLIC` should not be able to execute `DBMS_STREAMS_ADM_UTL`.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON DBMS_STREAMS_ADM_UTL FROM PUBLIC;
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'DBMS_AQADM_SYS' (Scored)

The Oracle database `DBMS_AQADM_SYS` package is shipped as undocumented and allows to run SQL commands as user SYS. The user `PUBLIC` should not be able to execute `DBMS_AQADM_SYS`.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON DBMS_AQADM_SYS FROM PUBLIC;
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'DBMS_STREAMS_RPC' (Scored)

The Oracle database `DBMS_STREAMS_RPC` package is shipped as undocumented and allows to run SQL commands as user SYS. The user `PUBLIC` should not be able to execute `DBMS_STREAMS_RPC`.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON DBMS_STREAMS_RPC FROM PUBLIC;
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'LTADM' (Scored)

The Oracle database `LTADM` package is shipped as undocumented. It allows privilege escalation if granted to unprivileged users. The user `PUBLIC` should not be able to execute `LTADM`.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON LTADM FROM PUBLIC;
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'WWV_DBMS_SQL' (Scored)

The Oracle database `WWV_DBMS_SQL` package is shipped as undocumented. It allows Oracle Application Express to run dynamic SQL statements.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON WWV_DBMS_SQL FROM PUBLIC;
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'WWV_EXECUTE_IMMEDIATE' (Scored)

The Oracle database `WWV_EXECUTE_IMMEDIATE` package is shipped as undocumented. It allows Oracle Application Express to run dynamic SQL statements. The user `PUBLIC` should not be able to execute `WWV_EXECUTE_IMMEDIATE`.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON WWV_EXECUTE_IMMEDIATE FROM PUBLIC;
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'DBMS_IJOB' (Scored)

The Oracle database `DBMS_IJOB` package is shipped as undocumented. It allows a user to run database jobs in the context of another user. The user `PUBLIC` should not be able to execute `DBMS_IJOB`.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON DBMS_IJOB FROM PUBLIC;
```

Ensure 'EXECUTE' Is Revoked from 'PUBLIC' on 'DBMS_FILE_TRANSFER' (Scored)

The Oracle database `DBMS_FILE_TRANSFER` package allows a user to transfer files from one database server to another. The user `PUBLIC` should not be able to execute `DBMS_FILE_TRANSFER`.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ON DBMS_FILE_TRANSFER FROM PUBLIC;
```

Revoke Excessive System Privileges

The recommendations within this section revoke excessive system privileges.

Ensure 'SELECT ANY DICTIONARY' Is Revoked from Unauthorized 'GRANTEE' (Scored)

The Oracle database `SELECT ANY DICTIONARY` privilege allows the designated user to access `SYS` schema objects. Unauthorized grantees should not have that privilege.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE SELECT_ANY_DICTIONARY FROM <grantee>;
```

Ensure 'SELECT ANY TABLE' Is Revoked from Unauthorized 'GRANTEE' (Scored)

The Oracle database `SELECT ANY TABLE` privilege allows the designated user to open any table, except `SYS`, to view it. Unauthorized grantees should not have that privilege.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE SELECT ANY TABLE FROM <grantee>;
```

> **Note:**
>
> If `O7_DICTIONARY_ACCESSIBILITY` has been set to `TRUE` (non-default setting) then the `SELECT ANY TABLE` privilege provides access to `SYS` objects.

Ensure 'AUDIT SYSTEM' Is Revoked from Unauthorized 'GRANTEE' (Scored)

The Oracle database AUDIT SYSTEM privilege allows changes to auditing activities on the system. Unauthorized grantees should not have that privilege.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE AUDIT SYSTEM FROM <grantee>;
```

Ensure 'EXEMPT ACCESS POLICY' Is Revoked from Unauthorized 'GRANTEE' (Scored)

The Oracle database `EXEMPT ACCESS POLICY` keyword provides the user the capability to access all the table rows regardless of row-level security lockouts. Unauthorized grantees should not have that keyword assigned to them.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXEMPT ACCESS POLICY FROM <grantee>;
```

Ensure 'BECOME USER' Is Revoked from Unauthorized 'GRANTEE' (Scored)

The Oracle database `BECOME USER` privilege allows the designated user to inherit the rights of another user. Unauthorized grantees should not have that privilege.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE BECOME USER FROM <grantee>;
```

Ensure 'CREATE_PROCEDURE' Is Revoked from Unauthorized 'GRANTEE' (Scored)

The Oracle database `CREATE PROCEDURE` privilege allows the designated user to create a stored procedure that will fire when given the correct command sequence. Unauthorized grantees should not have that privilege.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE CREATE PROCEDURE FROM <grantee>;
```

Ensure 'ALTER SYSTEM' Is Revoked from Unauthorized 'GRANTEE' (Scored)

The Oracle database `ALTER SYSTEM` privilege allows the designated user to dynamically alter the instance's running operations. Unauthorized grantees should not have that privilege.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE ALTER SYSTEM FROM <grantee>;
```

Ensure 'CREATE ANY LIBRARY' Is Revoked from Unauthorized 'GRANTEE' (Scored)

The Oracle database `CREATE ANY LIBRARY` privilege allows the designated user to create objects that are associated to the shared libraries. Unauthorized grantees should not have that privilege.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE CREATE ANY LIBRARY FROM <grantee>;
```

> **Note:**
>
> Oracle has two identical privileges: `CREATE LIBRARY` and `CREATE ANY LIBRARY`.

Ensure 'CREATE LIBRARY' Is Revoked from Unauthorized 'GRANTEE' (Scored)

The Oracle database `CREATE LIBRARY` privilege allows the designated user to create objects that are associated to the shared libraries. Unauthorized grantees should not have that privilege.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE CREATE LIBRARY FROM <grantee>;
```

> **Note:**
>
> Oracle has two identical privileges: `CREATE LIBRARY` and `CREATE ANY LIBRARY`.

Ensure 'GRANT ANY OBJECT PRIVILEGE' Is Revoked from Unauthorized 'GRANTEE' (Scored)

The Oracle database `GRANT ANY OBJECT PRIVILEGE` keyword provides the grantee the capability to grant access to any single or multiple combinations of objects to any grantee in the catalog of the database. Unauthorized grantees should not have that keyword assigned to them.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE GRANT ANY OBJECT PRIVILEGE FROM <grantee>;
```

Ensure 'GRANT ANY ROLE' Is Revoked from Unauthorized 'GRANTEE' (Scored)

The Oracle database `GRANT ANY ROLE` keyword provides the grantee the capability to grant any single role to any grantee in the catalog of the database. Unauthorized grantees should not have that keyword assigned to them.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE GRANT ANY ROLE FROM <grantee>;
```

Ensure 'GRANT ANY PRIVILEGE' Is Revoked from Unauthorized 'GRANTEE' (Scored)

The Oracle database `GRANT ANY PRIVILEGE` keyword provides the grantee the capability to grant any single privilege to any item in the catalog of the database. Unauthorized grantees should not have that privilege.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE GRANT ANY PRIVILEGE FROM <grantee>;
```

Revoke Role Privileges

The recommendations within this section intend to revoke powerful roles where they are likely not needed.

Ensure 'DELETE_CATALOG_ROLE' Is Revoked from Unauthorized 'GRANTEE' (Scored)

The Oracle database `DELETE_CATALOG_ROLE` provides `DELETE` privileges for the records in the system's audit table (`AUD$`). Unauthorized grantees should not have that role.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE DELETE_CATALOG_ROLE FROM <grantee>;
```

Ensure 'SELECT_CATALOG_ROLE' Is Revoked from Unauthorized 'GRANTEE' (Scored)

The Oracle database SELECT_CATALOG_ROLE provides SELECT privileges on all data dictionary views held in the SYS schema. Unauthorized grantees should not have that role.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE SELECT_CATALOG_ROLE FROM <grantee>;
```

Ensure 'EXECUTE_CATALOG_ROLE' Is Revoked from Unauthorized 'GRANTEE' (Scored)

The Oracle database EXECUTE_CATALOG_ROLE provides EXECUTE privileges for a number of packages and procedures in the data dictionary in the SYS schema. Unauthorized grantees should not have that role.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE_CATALOG_ROLE FROM <grantee>;
```

Ensure 'DBA' Is Revoked from Unauthorized 'GRANTEE' (Scored)

The Oracle database DBA role is the default database administrator role provided for the allocation of administrative privileges. Unauthorized grantees should not have that role.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE DBA FROM <grantee>;
```

Revoke Excessive Table and View Privileges

The recommendations within this section intend to revoke excessive table and view privileges.

Ensure 'ALL' Is Revoked from Unauthorized 'GRANTEE' on 'AUD$' (Scored)

The Oracle database SYS.AUD$ table contains all the audit records for the database of the non-Data Manipulation Language (DML) events, such as ALTER, DROP, and CREATE, and so forth. (DML changes need trigger-based audit events to record data alterations.) Unauthorized grantees should not have full access to that table.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE ALL ON AUD$ FROM <grantee>;
```

Ensure 'ALL' Is Revoked from Unauthorized 'GRANTEE' on 'USER_HISTORY$' (Scored)

The Oracle database SYS.USER_HISTORY$ table contains all the audit records for the user's password change history. (This table gets updated by password changes if the user has an

assigned profile that has a password reuse limit set, e.g., PASSWORD_REUSE_TIME set to other than UNLIMITED.) Unauthorized grantees should not have full access to that table.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE ALL ON USER_HISTORY$ FROM <grantee>;
```

> **Note:**
>
> USER_HISTORY$ contains only the old, case-insensitive passwords.

Ensure 'ALL' Is Revoked from Unauthorized 'GRANTEE' on 'LINK$' (Scored)

The Oracle database SYS.LINK$ table contains all the user's password information and data table link information. Unauthorized grantees should not have full access to that table.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE ALL ON LINK$ FROM <grantee>;
```

Ensure 'ALL' Is Revoked from Unauthorized 'GRANTEE' on 'SYS.USER$' (Scored)

The Oracle database SYS.USER$ table contains the users' hashed password information. Unauthorized grantees should not have full access to that table.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE ALL ON SYS.USER$ FROM <grantee>;
```

Ensure 'ALL' Is Revoked from Unauthorized 'GRANTEE' on 'DBA_%' (Scored)

The Oracle database DBA_% views show all information which is relevant to administrative accounts. Unauthorized grantees should not have full access to those views.

Remediation

Replace <Non-DBA/SYS grantee> in the query below, with the Oracle login(s) or role(s) returned from the associated audit procedure and execute:

```
REVOKE ALL ON DBA_ FROM <NON-DBA/SYS grantee>;
```

Ensure 'ALL' Is Revoked from Unauthorized 'GRANTEE' on 'SYS.SCHEDULER$_CREDENTIAL' (Scored)

The Oracle database SCHEDULER$_CREDENTIAL table contains the database scheduler credential information. Unauthorized grantees should not have full access to that table.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE ALL ON SYS.SCHEDULER4_CREDENTIAL FROM <username>;
```

> **Note:**
>
> *_SCHEDULER_CREDENTIALS is deprecated in Oracle Database 12c, but remains available for reasons of backward compatibility.

Ensure 'SYS.USER$MIG' Has Been Dropped (Scored)

The table sys.user$mig is created during migration and contains the Oracle password hashes before the migration starts. This table should be dropped.

Remediation

To remediate this setting, execute the following SQL statement.

```
DROP TABLE SYS.USER$MIG;
```

Ensure '%ANY%' Is Revoked from Unauthorized 'GRANTEE' (Scored)

The Oracle database ANY keyword provides the user the capability to alter any item in the catalog of the database. Unauthorized grantees should not have that keyword assigned to them.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE '<ANY Privilege>' FROM <grantee>;
```

Ensure 'DBA_SYS_PRIVS.%' Is Revoked from Unauthorized 'GRANTEE' with 'ADMIN_OPTION' Set to 'YES' (Scored)

The Oracle database WITH_ADMIN privilege allows the designated user to grant another user the same privileges. Unauthorized grantees should not have that privilege.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE <privilege> FROM <grantee>;
```

Ensure Proxy Users Have Only 'CONNECT' Privilege (Scored)

Do not grant privileges other than CONNECT directly to proxy users.

Remediation

To remediate this setting execute the following SQL statement for each [PRIVILEGE] returned (other than CONNECT) by running the audit procedure.

```
REVOKE <privilege> FROM <proxy_user>;
```

Ensure 'EXECUTE ANY PROCEDURE' Is Revoked from 'OUTLN' (Scored)

Remove unneeded `EXECUTE ANY PROCEDURE` privileges from `OUTLN`.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ANY PROCEDURE FROM OUTLN;
```

Ensure 'EXECUTE ANY PROCEDURE' Is Revoked from 'DBSNMP' (Scored)

Remove unneeded `EXECUTE ANY PROCEDURE` privileges from `DBSNMP`.

Remediation

To remediate this setting, execute the following SQL statement.

```
REVOKE EXECUTE ANY PROCEDURE FROM DBSNMP;
```

Audit/Logging Policies and Procedures

The ability to audit database activities is among the most important of all database security features. Decisions must be made regarding the scope of auditing since auditing has costs - in storage for the audit trail and in performance impact on audited operations - and perhaps even the database or system in general. There is also the additional cost to manage (store, backup, secure) and review the data in the audit trail.

Measures must be taken to protect the audit trail itself, for it may be targeted for alteration or destruction to hide unauthorized activity. For an audit destination outside the database, the recommendations are elsewhere in this document. Auditing recommendations for potential database audit destinations are below.

Auditing "by session" typically creates fewer (until 11g) and slightly smaller audit records, but is discouraged in most situations since there is some loss of fidelity (e.g. object privilege `GRANTEE`). More detailed auditing creates larger audit records. The `AUDIT_TRAIL` initialization parameter (for DB|XML, extended - or not) is the main determining factor for the size of a given audit record - and a notable factor in the performance cost, although the largest of the latter is DB versus OS or XML.

This section deals with standard Oracle auditing since auditing of privileged connections (as `sysdba` or `sysoper`) is configured via the `AUDIT_SYS_OPERATIONS` initialization parameter and is otherwise not configurable. The basic types of standard auditing are object, statement and privilege auditing, and each behaves differently.

Object auditing applies to specific objects for which it is invoked and always applies to all users. This type of auditing is usually employed to audit application-specific sensitive objects, but can also be used to protect the audit trail in the database.

Privilege auditing audits the use of specific system privileges, but typically only if the user actually possesses the audited privilege. Attempts that fail for lack of the audited privilege are typically not audited. This is the main weakness of privilege auditing and why statement auditing is usually preferred, if the option exists.

Statement auditing audits the issuance of certain types of statements, usually without regard to privilege or lack thereof. Both privilege and statement audits may be specified for specific users or all users (the default).

Traditional Auditing

The recommendations in this section should be followed if traditional auditing is implemented.

Ensure the 'USER' Audit Option Is Enabled (Scored)

The `USER` object allows for creating accounts that can interact with the database according to the roles and privileges allotted to the account. It may also own database objects. Enabling the audit option causes auditing of all activities and requests to create, drop or alter a user, including a user changing their own password. (The latter is not audited by audit `ALTER USER`.)

Remediation

Execute the following SQL statement to remediate this setting.

```
AUDIT USER;
```

Ensure the 'ROLE' Audit Option Is Enabled (Scored)

The `ROLE` object allows for the creation of a set of privileges that can be granted to users or other roles. Enabling the audit option causes auditing of all attempts, successful or not, to create, drop, alter or set roles.

Remediation

Execute the following SQL statement to remediate this setting.

```
AUDIT ROLE;
```

Ensure the 'SYSTEM GRANT' Audit Option Is Enabled (Scored)

Enabling the audit option for the `SYSTEM GRANT` object causes auditing of any attempt, successful or not, to grant or revoke any system privilege or role, regardless of privilege held by the user attempting the operation.

Remediation

Execute the following SQL statement to remediate this setting.

```
AUDIT SYSTEM GRANT;
```

Ensure the 'PROFILE' Audit Option Is Enabled (Scored)

The `PROFILE` object allows for the creation of a set of database resource limits that can be assigned to a user, so that user cannot exceed those resource limitations. Enabling the audit option causes auditing of all attempts, successful or not, to create, drop or alter any profile.

Remediation

Execute the following SQL statement to remediate this setting.

```
AUDIT PROFILE;
```

> **Note:**
>
> The statement auditing option audit `PROFILE` audits everything that the three privilege audits audit `CREATE PROFILE`, audit `DROP PROFILE` and audit `ALTER PROFILE` do, but also audits:
>
> 1. Attempts to create a profile by a user without the `CREATE PROFILE` system privilege.
> 2. Attempts to drop a profile by a user without the `DROP PROFILE` system privilege
> 3. Attempts to alter a profile by a user without the `ALTER PROFILE` system privilege.

Ensure the 'DATABASE LINK' Audit Option Is Enabled (Scored)

Enabling the audit option for the `DATABASE LINK` object causes all activities on database links to be audited.

Remediation

Execute the following SQL statement to remediate this setting.

```
AUDIT DATABASE LINK;
```

Ensure the 'PUBLIC DATABASE LINK' Audit Option Is Enabled (Scored)

The `PUBLIC DATABASE LINK` object allows for the creation of a public link for an application-based "user" to access the database for connections/session creation. Enabling the audit option causes all user activities involving the creation, alteration, or dropping of public links to be audited.

Remediation

Execute the following SQL statement to remediate this setting.

```
AUDIT PUBLIC DATABASE LINK;
```

Ensure the 'PUBLIC SYNONYM' Audit Option Is Enabled (Scored)

The `PUBLIC SYNONYM` object allows for the creation of an alternate description of an object. Public synonyms are accessible by all users that have the appropriate privileges to the underlying object. Enabling the audit option causes all user activities involving the creation or dropping of public synonyms to be audited.

Remediation

Execute the following SQL statement to remediate this setting.

```
AUDIT PUBLIC SYNONYM;
```

Ensure the 'SYNONYM' Audit Option Is Enabled (Scored)

The `SYNONYM` operation allows for the creation of an alternative name for a database object such as a Java class schema object, materialized view, operator, package, procedure, sequence, stored function, table, view, user-defined object type, or even another synonym. This synonym puts a dependency on its target and is rendered invalid if the target object is

changed/dropped. Enabling the audit option causes all user activities involving the creation or dropping of synonyms to be audited.

Remediation

Execute the following SQL statement to remediate this setting.

```
AUDIT SYNONYM;
```

Ensure the 'DIRECTORY' Audit Option Is Enabled (Scored)

The `DIRECTORY` object allows for the creation of a directory object that specifies an alias for a directory on the server file system, where the external binary file `LOBs` (`BFILEs`)/ table data are located. Enabling this audit option causes all user activities involving the creation or dropping of a directory alias to be audited.

Remediation

Execute the following SQL statement to remediate this setting.

```
AUDIT DIRECTORY;
```

Ensure the 'SELECT ANY DICTIONARY' Audit Option Is Enabled (Scored)

The `SELECT ANY DICTIONARY` capability allows the user to view the definitions of all schema objects in the database. Enabling the audit option causes all user activities involving this capability to be audited.

Remediation

Execute the following SQL statement to remediate this setting.

```
AUDIT SELECT ANY DICTIONARY;
```

Ensure the 'GRANT ANY OBJECT PRIVILEGE' Audit Option Is Enabled (Scored)

`GRANT ANY OBJECT PRIVILEGE` allows the user to grant or revoke any object privilege, which includes privileges on tables, directories, mining models, etc. Enabling this audit option causes auditing of all uses of that privilege.

Remediation

Execute the following SQL statement to remediate this setting.

```
AUDIT GRANT ANY OBJECT PRIVILEGE;
```

> **Note:**
>
> This does NOT audit all attempts to grant or revoke object privileges since this can also be done by anyone who was granted an object privilege with the grant option. Also, this never creates an audit record for anyone who does not hold the `GRANT ANY OBJECT PRIVILEGE` system privilege. Therefore, many attempts, successful or not, to grant and revoke object privileges are not audited by this.

Ensure the 'GRANT ANY PRIVILEGE' Audit Option Is Enabled (Scored)

`GRANT ANY PRIVILEGE` allows a user to grant any system privilege, including the most powerful privileges typically available only to administrators - to change the security infrastructure, to drop/add/modify users and more.

Remediation

Execute the following SQL statement to remediate this setting.

```
AUDIT GRANT ANY PRIVILEGE;
```

> **Note:**
>
> This does NOT audit all attempts to grant or revoke system privileges since this can also be done by anyone who was granted a system privilege with the admin option. Also, this never creates an audit record for anyone who does not hold the `GRANT ANY PRIVILEGE` system privilege. Thus, many attempts, successful or not, to grant and revoke system privileges are not audited by this.

Ensure the 'DROP ANY PROCEDURE' Audit Option Is Enabled (Scored)

The `AUDIT DROP ANY PROCEDURE` command is auditing the dropping of procedures. Enabling the option causes auditing of all such activities.

Remediation

Execute the following SQL statement to remediate this setting.

```
AUDIT DROP ANY PROCEDURE;
```

Ensure the 'ALL' Audit Option on 'SYS.AUD$' Is Enabled (Scored)

The logging of attempts to alter the audit trail in the `SYS.AUD$` table (open for read/update/delete/view) will provide a record of any activities that may indicate unauthorized attempts to access the audit trail. Enabling the audit option will cause these activities to be audited.

Remediation

Execute the following SQL statement to remediate this setting.

```
AUDIT ALL ON SYS.AUD$ BY ACCESS;
```

Ensure the 'PROCEDURE' Audit Option Is Enabled (Scored)

In this statement audit, `PROCEDURE` means any procedure, function, package or library. Enabling this audit option causes any attempt, successful or not, to create or drop any of these types of objects to be audited, regardless of privilege or lack thereof. Java schema objects (sources, classes, and resources) are considered the same as procedures for the purposes of auditing SQL statements.

Remediation

Execute the following SQL statement to remediate this setting.

```
AUDIT PROCEDURE;
```

> **Note:**
>
> Not all auditing options work alike. In particular, the statement auditing option audit `PROCEDURE` does indeed audit create and drop library as well as all types of procedures and java schema objects. However, privilege audits do not work this way. So, for example, none of audit `CREATE ANY PROCEDURE`, audit `DROP ANY PROCEDURE`, or audit `CREATE PROCEDURE` will audit create or drop library activities. In statement auditing, `PROCEDURE` has a larger scope than in privilege auditing, where it is specific to functions, packages and procedures, but excludes libraries and perhaps other object types. Audit `PROCEDURE` does not audit altering procedures, either in your own schema or in another via the `ALTER ANY PROCEDURE` system privilege. There seems to be no statement audit that is a better replacement for Audit `ALTER ANY PROCEDURE`, but beware that will not create any audit records for users that do not have the privilege. Thus, attempts to alter procedures in one's own schema are never audited, and attempts to alter procedures in another's schema that fail for lack of the `ALTER ANY PROCEDURE` privilege are not audited. This is simply a weakness in the current state of Oracle auditing. Fortunately, though, all that the `ALTER` command can be used for regarding procedures, functions, packages and libraries is compile options, so the inability to comprehensively audit alter procedure activities and requests is not as bad as it would be for other object types (`USER`, `PROFILE`, etc.)

Ensure the 'ALTER SYSTEM' Audit Option Is Enabled (Scored)

`ALTER SYSTEM` allows one to change instance settings, including security settings and auditing options. Additionally, `ALTER SYSTEM` can be used to run operating system commands using undocumented Oracle functionality. Enabling the audit option will audit all attempts to perform `ALTER SYSTEM`, whether successful or not and regardless of whether or not the `ALTER SYSTEM` privilege is held by the user attempting the action.

Remediation

Execute the following SQL statement to remediate this setting.

```
AUDIT ALTER SYSTEM;
```

Ensure the 'TRIGGER' Audit Option Is Enabled (Scored)

A `TRIGGER` may be used to modify `DML` actions or invoke other (recursive) actions when some types of user-initiated actions occur. Enabling this audit option will cause auditing of any attempt, successful or not, to create, drop, enable or disable any schema trigger in any schema regardless of privilege or lack thereof. For enabling and disabling a trigger, it covers both `ALTER TRIGGER` and `ALTER TABLE`.

Remediation

Execute the following SQL statement to remediate this setting.

```
AUDIT TRIGGER;
```

Note:

There is no current CIS recommendation to audit the use of the system privilege `CREATE TRIGGER`, as there is for `CREATE SYNONYM`, `CREATE PROCEDURE` and some other types of objects, so this is actually a scope escalation also - to audit such actions in one's own schema. However, this is the only way to comprehensively audit things like attempts to create, drop or alter triggers in another's schema if the user attempting to operation does not hold the required ANY privilege - and these are exactly the sorts of things that should raise a large red flag. The statement auditing option audit `TRIGGER` audits almost everything that the three privilege audits audit `CREATE ANY TRIGGER`, audit `ALTER ANY TRIGGER` and audit `DROP ANY TRIGGER` do, but also audits:

1. Statements to create, drop, enable or disable a trigger in the user's own schema.
2. 2. Attempts to create a trigger by a user without the `CREATE TRIGGER` system privilege.
3. 3. Attempts to create a trigger in another schema by users without the `CREATE ANY TRIGGER` privilege.
4. 4. Attempts to drop a trigger in another schema by users without the `DROP ANY TRIGGER` privilege.
5. 5. Attempts to disable or enable a trigger in another schema by users without the `ALTER ANY TRIGGER` privilege.

The one thing is audited by any of the three privilege audits that is not audited by this is `ALTER TRIGGER ...COMPILE` if the trigger is in another's schema, which is audited by audit `ALTER ANY TRIGGER`, but only if the user attempting the alteration actually holds the `ALTER ANY TRIGGER` system privilege. Audit `TRIGGER` only audits `ALTER TABLE` or `ALTER TRIGGER` statements used to enable or disable triggers. It does not audit `ALTER TRIGGER` or `ALTER TABLE` statements used only with compile options.

Ensure the 'CREATE SESSION' Audit Option Is Enabled (Scored)

Enabling this audit option will cause auditing of all attempts to connect to the database, whether successful or not, as well as audit session disconnects/logoffs. The commands to audit `SESSION`, `CONNECT` or `CREATE SESSION` all accomplish the same thing - they initiate statement auditing of the connect statement used to create a database session.

Remediation

Execute the following SQL statement to remediate this setting.

```
AUDIT SESSION;
```

> **Note:**
>
> Although listed in the documentation as a privilege audit, audit `CREATE SESSION` actually audits the `CONNECT` statement. This is evidenced by the undocumented audit `CONNECT` which has the same result as audit `SESSION` or audit `CREATE SESSION`. There is no system privilege named either `SESSION` or `CONNECT` (`CONNECT` is a role, not a system privilege). Also, it behaves as statement auditing rather than privilege auditing in that it audits all attempts to create a session, even if the user does not hold the `CREATE SESSION` system privilege.

PDB Specific Remediation

The recommendations in this section should be followed if a PDB with traditional auditing is used.

3.10 Ensure No Users Are Assigned the 'DEFAULT' Profile

Will continue to display a violation even after performing remediation action.

This is because a user "PDBADMIN" is created for each PDB and assigned DEFAULT Profile

5.1.14 Ensure the 'ALL' Audit Option on 'SYS.AUD$' Is Enabled

This cannot be remediated for PDB by executing the command specified in CIS documentation. It will continue to show a violation.

Rules to Remediate from a CDB

The following rules cannot be remediated from inside the PDB. The user must remediate them by connecting to CDB and performing the remediation action specified in CIS documentation:

- Rule 2.2.1 Ensure 'AUDIT_SYS_OPERATIONS' Is Set to 'TRUE' (Compliance Standard Rule)
- Rule 2.2.2 Ensure 'AUDIT_TRAIL' Is Set to 'DB', 'XML', 'OS', 'DB,EXTENDED', or 'XML,EXTENDED' (Compliance Standard Rule)
- Rule 2.2.5 Ensure 'OS_ROLES' Is Set to 'FALSE' (Compliance Standard Rule)
- Rule 2.2.6 Ensure 'REMOTE_LISTENER' Is Empty (Compliance Standard Rule)
- Rule 2.2.8 Ensure 'REMOTE_OS_AUTHENT' Is Set to 'FALSE' (Compliance Standard Rule)
- Rule 2.2.9 Ensure 'REMOTE_OS_ROLES' Is Set to 'FALSE' (Compliance Standard Rule)
- Rule 2.2.10 Ensure 'UTL_FILE_DIR' Is Empty (Compliance Standard Rule)
- Rule 2.2.11 Ensure 'SEC_CASE_SENSITIVE_LOGON' Is Set to 'TRUE' (Compliance Standard Rule)
- Rule 2.2.12 Ensure 'SEC_MAX_FAILED_LOGIN_ATTEMPTS' Is '3' or Less (Compliance Standard Rule)
- Rule 2.2.15 Ensure 'SEC_RETURN_SERVER_RELEASE_BANNER' Is Set to 'FALSE' (Compliance Standard Rule)
- Rule 2.2.17 Ensure '_trace_files_public' Is Set to 'FALSE' (Compliance Standard Rule)
- Rule 2.2.13 Ensure 'SEC_PROTOCOL_ERROR_FURTHER_ACTION' Is Set to 'DROP,3' (Compliance Standard Rule)

- Rule 2.2.14 Ensure 'SEC_PROTOCOL_ERROR_TRACE_ACTION' Is Set to 'LOG' (Compliance Standard Rule)
- Rule 2.2.16 Ensure 'SQL92_SECURITY' Is Set to 'TRUE' (Compliance Standard Rule)

Unified Auditing

The recommendations in this section should be followed if unified auditing is implemented.

Ensure the 'CREATE USER' Action Audit Is Enabled (Scored)

The CREATE USER statement is used to create Oracle database accounts and assign database properties to them. Enabling this unified action audit causes logging of all CREATE USER statements, whether successful or unsuccessful, issued by the users regardless of the privileges held by the users to issue such statements.

Remediation

Execute the following SQL statement to remediate this setting.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD
ACTIONS
CREATE USER;
```

> **Note:**
>
> If you do not have CIS_UNIFIED_AUDIT_POLICY, please create one using the CREATE AUDIT POLICY statement.

Ensure the 'ALTER USER' Action Audit Is Enabled (Scored)

The ALTER USER statement is used to change database users' password, lock accounts, and expire passwords. In addition, this statement is used to change database properties of user accounts such as database profiles, default and temporary tablespaces, and tablespace quotas. This unified audit action enables logging of all ALTER USER statements, whether successful or unsuccessful, issued by the users regardless of the privileges held by the users to issue such statements.

Remediation

Execute the following SQL statement to remediate this setting.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD
ACTIONS
ALTER USER;
```

> **Note:**
>
> If you do not have CIS_UNIFIED_AUDIT_POLICY, please create one using the CREATE AUDIT POLICY statement.

Ensure the 'DROP USER' Audit Option Is Enabled (Scored)

The DROP USER statement is used to drop Oracle database accounts and schemas associated with them. Enabling this unified action audit enables logging of all DROP USER statements, whether successful or unsuccessful, issued by the users regardless of the privileges held by the users to issue such statements.

Remediation

Execute the following SQL statement to remediate this setting.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD
ACTIONS
DROP USER;
```

> **Note:**
>
> If you do not have CIS_UNIFIED_AUDIT_POLICY, please create one using the CREATE AUDIT POLICY statement.

Ensure the 'CREATE ROLE' Action Audit Is Enabled (Scored)

An Oracle database role is a collection or set of privileges that can be granted to users or other roles. Roles may include system privileges, object privileges or other roles. Enabling this unified audit action enables logging of all CREATE ROLE statements, whether successful or unsuccessful, issued by the users regardless of the privileges held by the users to issue such statements.

Remediation

Execute the following SQL statement to remediate this setting.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD
ACTIONS
CREATE ROLE;
```

> **Note:**
>
> If you do not have CIS_UNIFIED_AUDIT_POLICY, please create one using the CREATE AUDIT POLICY statement.

Ensure the 'ALTER ROLE' Action Audit Is Enabled (Scored)

An Oracle database role is a collection or set of privileges that can be granted to users or other roles. Roles may include system privileges, object privileges or other roles. The ALTER ROLE statement is used to change the authorization needed to enable a role. Enabling this unified action audit causes logging of all ALTER ROLE statements, whether successful or

unsuccessful, issued by the users regardless of the privileges held by the users to issue such statements.

Remediation

Execute the following SQL statement to remediate this setting.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD
ACTIONS
ALTER ROLE;
```

> **Note:**
>
> If you do not have CIS_UNIFIED_AUDIT_POLICY, please create one using the CREATE AUDIT POLICY statement.

Ensure the 'DROP ROLE' Action Audit Is Enabled (Scored)

An Oracle database role is a collection or set of privileges that can be granted to users or other roles. Roles may include system privileges, object privileges or other roles. Enabling this unified audit action enables logging of all DROP ROLE statements, successful or unsuccessful, issued by the users regardless of the privileges held by the users to issue such statements.

Remediation

Execute the following SQL statement to remediate this setting.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD
ACTIONS
DROP ROLE;
```

> **Note:**
>
> If you do not have CIS_UNIFIED_AUDIT_POLICY, please create one using the CREATE AUDIT POLICY statement.

Ensure the 'GRANT' Action Audit Is Enabled (Scored)

GRANT statements are used to grant privileges to Oracle database users and roles, including the most powerful privileges and roles typically available to the database administrators. Enabling this unified action audit enables logging of all GRANT statements, whether successful or unsuccessful, issued by the users regardless of the privileges held by the users to issue such statements.

Remediation

Execute the following SQL statement to remediate this setting.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD
ACTIONS
GRANT;
```

> **Note:**
>
> If you do not have CIS_UNIFIED_AUDIT_POLICY, please create one using the CREATE AUDIT POLICY statement.

Ensure the 'REVOKE' Action Audit Is Enabled (Scored)

REVOKE statements are used to revoke privileges from Oracle database users and roles. Enabling this unified action audit enables logging of all REVOKE statements, successful or unsuccessful, issued by the users regardless of the privileges held by the users to issue such statements.

Remediation

Execute the following SQL statement to remediate this setting.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD
ACTIONS
REVOKE;
```

> **Note:**
>
> If you do not have CIS_UNIFIED_AUDIT_POLICY, please create one using the CREATE AUDIT POLICY statement.

Ensure the 'CREATE PROFILE' Action Audit Is Enabled (Scored)

Oracle database profiles are used to enforce resource usage limits and implement password policies such as password complexity rules and reuse restrictions. Enabling this unified action audit enables logging of all CREATE PROFILE statements, whether successful or unsuccessful, issued by the users regardless of the privileges held by the users to issue such statements.

Remediation

Execute the following SQL statement to remediate this setting.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD
ACTIONS
CREATE PROFILE;
```

> **Note:**
>
> If you do not have CIS_UNIFIED_AUDIT_POLICY, please create one using the CREATE AUDIT POLICY statement.

Ensure the 'ALTER PROFILE' Action Audit Is Enabled (Scored)

Oracle database profiles are used to enforce resource usage limits and implement password policies such as password complexity rules and reuse restrictions. Enabling this unified action

audit enables logging of all ALTER PROFILE statements, whether successful or unsuccessful, issued by the users regardless of the privileges held by the users to issue such statements.

Remediation

Execute the following SQL statement to remediate this setting.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD
ACTIONS
ALTER PROFILE;
```

> **Note:**
>
> If you do not have CIS_UNIFIED_AUDIT_POLICY, please create one using the CREATE AUDIT POLICY statement.

Ensure the 'DROP PROFILE' Action Audit Is Enabled (Scored)

Oracle database profiles are used to enforce resource usage limits and implement password policies such as password complexity rules and reuse restrictions. Enabling this unified action audit enables logging of all DROP PROFILE statements, whether successful or unsuccessful, issued by the users regardless of the privileges held by the users to issue such statements.

Remediation

Execute the following SQL statement to remediate this setting.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD
ACTIONS
DROP PROFILE;
```

> **Note:**
>
> If you do not have CIS_UNIFIED_AUDIT_POLICY, please create one using the CREATE AUDIT POLICY statement.

Ensure the 'CREATE DATABASE LINK' Action Audit Is Enabled (Scored)

Oracle database links are used to establish database-to-database connections to other databases. These connections are available without further authentication once the link is established. Enabling this unified action audit causes logging of all CREATE DATABASE and CREATE PUBLIC DATABASE statements, whether successful or unsuccessful, issued by the users regardless of the privileges held by the users to issue such statements.

Remediation

Execute the following SQL statement to remediate this setting.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD
ACTIONS
CREATE DATABASE LINK;
```

> **Note:**
>
> If you do not have CIS_UNIFIED_AUDIT_POLICY, please create one using the CREATE AUDIT POLICY statement.

Ensure the 'ALTER DATABASE LINK' Action Audit Is Enabled (Scored)

Oracle database links are used to establish database-to-database connections to other databases. These connections are always available without further authentication once the link is established. Enabling this unified action audit causes logging of all ALTER DATABASE and ALTER PUBLIC DATABASE statements, whether successful or unsuccessful, issued by the users regardless of the privileges held by the users to issue such statements.

Remediation

Execute the following SQL statement to remediate this setting.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD
ACTIONS
ALTER DATABASE LINK;
```

> **Note:**
>
> If you do not have CIS_UNIFIED_AUDIT_POLICY, please create one using the CREATE AUDIT POLICY statement.

Ensure the 'DROP DATABASE LINK' Action Audit Is Enabled (Scored)

Oracle database links are used to establish database-to-database connections to other databases. These connections are always available without further authentication once the link is established. Enabling this unified action audit causes logging of all DROP DATABASE and DROP PUBLIC DATABASE, whether successful or unsuccessful, statements issued by the users regardless of the privileges held by the users to issue such statements.

Remediation

Execute the following SQL statement to remediate this setting.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD
ACTIONS
DROP DATABASE LINK;
```

> **Note:**
>
> If you do not have CIS_UNIFIED_AUDIT_POLICY, please create one using the CREATE AUDIT POLICY statement.

Ensure the 'CREATE SYNONYM' Action Audit Is Enabled (Scored)

An Oracle database synonym is used to create an alternative name for a database object such as table, view, procedure, java object or even another synonym, etc. Enabling this unified action audit causes logging of all CREATE SYNONYM and CREATE PUBLIC SYNONYM statements, whether successful or unsuccessful, issued by the users regardless of the privileges held by the users to issue such statements.

Remediation

Execute the following SQL statement to remediate this setting.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD
ACTIONS
CREATE SYNONYM;
```

> **Note:**
>
> If you do not have CIS_UNIFIED_AUDIT_POLICY, please create one using the CREATE AUDIT POLICY statement.

Ensure the 'ALTER SYNONYM' Action Audit Is Enabled (Scored)

An Oracle database synonym is used to create an alternative name for a database object such as table, view, procedure, or java object, or even another synonym. Enabling this unified action audit causes logging of all ALTER SYNONYM and ALTER PUBLIC SYNONYM statements, whether successful or unsuccessful, issued by the users regardless of the privileges held by the users to issue such statements.

Remediation

Execute the following SQL statement to remediate this setting.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD
ACTIONS
ALTER SYNONYM;
```

> **Note:**
>
> If you do not have CIS_UNIFIED_AUDIT_POLICY, please create one using the CREATE AUDIT POLICY statement.

Ensure the 'DROP SYNONYM' Action Audit Is Enabled (Scored)

An Oracle database synonym is used to create an alternative name for a database object such as table, view, procedure, or java object, or even another synonym. Enabling his unified action audit causes logging of all DROP SYNONYM and DROP PUBLIC SYNONYM statements,

whether successful or unsuccessful, issued by the users regardless of the privileges held by the users to issue such statements.

Remediation

Execute the following SQL statement to remediate this setting.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD
ACTIONS
DROP SYNONYM;
```

> **Note:**
>
> If you do not have CIS_UNIFIED_AUDIT_POLICY, please create one using the CREATE AUDIT POLICY statement.

Ensure the 'SELECT ANY DICTIONARY' Privilege Audit Is Enabled (Scored)

The SELECT ANY DICTIONARY system privilege allows the user to view the definition of all schema objects in the database. It grants SELECT privileges on the data dictionary objects to the grantees, including SELECT on DBA_ views, V$ views, X$ views and underlying SYS tables such as TAB$ and OBJ$. This privilege also allows grantees to create stored objects such as procedures, packages and views on the underlying data dictionary objects. Please note that this privilege does not grant SELECT on tables with password hashes such as USER$, DEFAULT_PWD$, LINK$, and USER_HISTORY$. Enabling this audit causes logging of activities that exercise this privilege.

Remediation

Execute the following SQL statement to remediate this setting.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD
PRIVILEGES
SELECT ANY DICTIONARY;
```

> **Note:**
>
> If you do not have CIS_UNIFIED_AUDIT_POLICY, please create one using the CREATE AUDIT POLICY statement.

Ensure the 'UNIFIED_AUDIT_TRAIL' Access Audit Is Enabled (Scored)

The UNIFIED_AUDIT_TRAIL view holds audit trail records generated by the database. Enabling this audit action causes logging of all access attempts to the UNIFIED_AUDIT_TRAIL view, whether successful or unsuccessful, regardless of the privileges held by the users to issue such statements.

Remediation

Execute the following SQL statement to remediate this setting.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD
```

```
ACTIONS
ALL on SYS.UNIFIED_AUDIT_TRAIL;
```

> **Note:**
>
> If you do not have CIS_UNIFIED_AUDIT_POLICY, please create one using the CREATE AUDIT POLICY statement.

Ensure the 'CREATE PROCEDURE/FUNCTION/PACKAGE/PACKAGE BODY' Action Audit Is Enabled (Scored)

Oracle database procedures, function, packages, and package bodies, which are stored within the database, are created to perform business functions and access database as defined by PL/SQL code and SQL statements contained within these objects. Enabling this unified action audit causes logging of all CREATE PROCEDURE, CREATE FUNCTION, CREATE PACKAGE and CREATE PACKAGE BODY statements, successful or unsuccessful, statements issued by the users regardless of the privileges held by the users to issue such statements.

Remediation

Execute the following SQL statement to remediate this setting.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD
ACTIONS
CREATE PROCEDURE,
CREATE FUNCTION,
CREATE PACKAGE,
CREATE PACKAGE BODY;
```

> **Note:**
>
> If you do not have CIS_UNIFIED_AUDIT_POLICY, please create one using the CREATE AUDIT POLICY statement.

Ensure the 'ALTER PROCEDURE/FUNCTION/PACKAGE/PACKAGE BODY' Action Audit Is Enabled (Scored)

Oracle database procedures, functions, packages, and package bodies, which are stored within the database, are created to carry out business functions and access database as defined by PL/SQL code and SQL statements contained within these objects. Enabling this unified action audit causes logging of all ALTER PROCEDURE, ALTER FUNCTION, ALTER PACKAGE and ALTER PACKAGE BODY statements, successful or unsuccessful, issued by the users regardless of the privileges held by the users to issue such statements.

Remediation

Execute the following SQL statement to remediate this setting.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD
ACTIONS
ALTER PROCEDURE,
ALTER FUNCTION,
```

```
ALTER PACKAGE,
ALTER PACKAGE BODY;
```

> **Note:**
>
> If you do not have CIS_UNIFIED_AUDIT_POLICY, please create one using the CREATE AUDIT POLICY statement.

Ensure the 'DROP PROCEDURE/FUNCTION/PACKAGE/PACKAGE BODY' Action Audit Is Enabled (Scored)

Oracle database procedures, functions, packages, and package bodies, which are stored within the database, are created to carry out business functions and access database as defined by PL/SQL code and SQL statements contained within these objects. Enabling this unified action audit causes logging of all DROP PROCEDURE, DROP FUNCTION, DROP PACKAGE or DROP PACKAGE BODY statements, successful or unsuccessful, issued by the users regardless of the privileges held by the users to issue such statements.

Remediation

Execute the following SQL statement to remediate this setting.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD
ACTIONS
DROP PROCEDURE,
DROP FUNCTION,
DROP PACKAGE,
DROP PACKAGE BODY;
```

> **Note:**
>
> If you do not have CIS_UNIFIED_AUDIT_POLICY, please create one using the CREATE AUDIT POLICY statement.

Ensure the 'ALTER SYSTEM' Privilege Audit Is Enabled (Scored)

The ALTER SYSTEM privilege allows the user to change instance settings which could impact security posture, performance or normal operation of the database. Additionally, the ALTER SYSTEM privilege may be used to run operating system commands using undocumented Oracle functionality. Enabling this unified audit causes logging of activities that involve exercise of this privilege, whether successful or unsuccessful, issued by the users regardless of the privileges held by the users to issue such statements.

Remediation

Execute the following SQL statement to remediate this setting.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD
ACTIONS
ALTER SYSTEM;
```

> **Note:**
>
> If you do not have CIS_UNIFIED_AUDIT_POLICY, please create one using the CREATE AUDIT POLICY statement.

Ensure the 'CREATE TRIGGER' Action Audit Is Enabled (Scored)

Oracle database triggers are executed automatically when specified conditions on the underlying objects occur. Trigger bodies contain the code, quite often to perform data validation, ensure data integrity/security or enforce critical constraints on allowable actions on data. Enabling this unified audit causes logging of all CREATE TRIGGER statements, whether successful or unsuccessful, issued by the users regardless of the privileges held by the users to issue such statements.

Remediation

Execute the following SQL statement to remediate this setting.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD
ACTIONS
CREATE TRIGGER;
```

> **Note:**
>
> If you do not have CIS_UNIFIED_AUDIT_POLICY, please create one using the CREATE AUDIT POLICY statement.

Ensure the 'ALTER TRIGGER' Action Audit IS Enabled (Scored)

Oracle database triggers are executed automatically when specified conditions on the underlying objects occur. Trigger bodies contain the code, quite often to perform data validation, ensure data integrity/security or enforce critical constraints on allowable actions on data. Enabling this unified audit causes logging of all ALTER TRIGGER statements, whether successful or unsuccessful, issued by the users regardless of the privileges held by the users to issue such statements.

Remediation

Execute the following SQL statement to remediate this setting.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD
ACTIONS
ALTER TRIGGER;
```

> **Note:**
>
> If you do not have CIS_UNIFIED_AUDIT_POLICY, please create one using the CREATE AUDIT POLICY statement.

Ensure the 'DROP TRIGGER' Action Audit Is Enabled (Scored)

Oracle database triggers are executed automatically when specified conditions on the underlying objects occur. Trigger bodies contain the code, quite often to perform data validation, ensure data integrity/security or enforce critical constraints on allowable actions on data. Enabling this unified audit causes logging of all DROP TRIGGER statements, whether successful or unsuccessful, issued by the users regardless of the privileges held by the users to issue such statements.

Remediation

Execute the following SQL statement to remediate this setting.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD
ACTIONS
DROP TRIGGER;
```

> **Note:**
>
> If you do not have CIS_UNIFIED_AUDIT_POLICY, please create one using the CREATE AUDIT POLICY statement.

Ensure the 'LOGON' AND 'LOGOFF' Actions Audit Is Enabled (Scored)

Oracle database users log on to the database to perform their work. Enabling this unified audit causes logging of all LOGON actions, whether successful or unsuccessful, issued by the users regardless of the privileges held by the users to log into the database. In addition, LOGOFF action audit captures logoff activities. This audit action also captures logon/logoff to the open database by SYSDBA and SYSOPER.

Remediation

Execute the following SQL statement to remediate this setting.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD
ACTIONS
LOGON,
LOGOFF;
```

> **Note:**
>
> If you do not have CIS_UNIFIED_AUDIT_POLICY, please create one using the CREATE AUDIT POLICY statement.

PDB Specific Remediation

The recommendations in this section should be followed if a PDB with unified auditing is used.

Rules to Remediate from a CDB

The following rules cannot be remediated from inside the PDB. The user must remediate them by connecting to CDB and performing the remediation action specified in CIS documentation:

- Rule 2.2.1 Ensure 'AUDIT_SYS_OPERATIONS' Is Set to 'TRUE' (Compliance Standard Rule)
- Rule 2.2.2 Ensure 'AUDIT_TRAIL' Is Set to 'DB', 'XML', 'OS', 'DB,EXTENDED', or 'XML,EXTENDED' (Compliance Standard Rule)
- Rule 2.2.5 Ensure 'OS_ROLES' Is Set to 'FALSE' (Compliance Standard Rule)
- Rule 2.2.6 Ensure 'REMOTE_LISTENER' Is Empty (Compliance Standard Rule)
- Rule 2.2.8 Ensure 'REMOTE_OS_AUTHENT' Is Set to 'FALSE' (Compliance Standard Rule)
- Rule 2.2.9 Ensure 'REMOTE_OS_ROLES' Is Set to 'FALSE' (Compliance Standard Rule)
- Rule 2.2.10 Ensure 'UTL_FILE_DIR' Is Empty (Compliance Standard Rule)
- Rule 2.2.11 Ensure 'SEC_CASE_SENSITIVE_LOGON' Is Set to 'TRUE' (Compliance Standard Rule)
- Rule 2.2.12 Ensure 'SEC_MAX_FAILED_LOGIN_ATTEMPTS' Is '3' or Less (Compliance Standard Rule)
- Rule 2.2.15 Ensure 'SEC_RETURN_SERVER_RELEASE_BANNER' Is Set to 'FALSE' (Compliance Standard Rule)
- Rule 2.2.17 Ensure '_trace_files_public' Is Set to 'FALSE' (Compliance Standard Rule)
- Rule 2.2.13 Ensure 'SEC_PROTOCOL_ERROR_FURTHER_ACTION' Is Set to 'DROP,3' (Compliance Standard Rule)
- Rule 2.2.14 Ensure 'SEC_PROTOCOL_ERROR_TRACE_ACTION' Is Set to 'LOG' (Compliance Standard Rule)
- Rule 2.2.16 Ensure 'SQL92_SECURITY' Is Set to 'TRUE' (Compliance Standard Rule)

21

SCAP Supported Standards

Enterprise Manager supports Security Content Automation Protocol (SCAP) enabled compliance standards. SCAP is a multi-purpose framework of specifications that supports automated configuration, vulnerability and patch checking, technical control compliance activities, and security measurement.

> **Note:**
>
> OSCAP is not part of Enterprise Manager or an Oracle product. It's part of the OpenScap initiative.

OSCAP consumes a compliance standard Extensible Configuration Checklist Description Format (XCCDF) payload is delivered via Oracle Linux. It can then be imported into Enterprise Manager using EM CLI verb `upload_compliance_standard`, and manage the compliance of managed targets against your policies. For more information see: Import XCCDF based standards using EMCLI. By using Enterprise Manager, this allows a way to mass-deploy the payload (XCCDF and OVAL files) to be consumed by OSCAP already installed on the hosts.

> **Note:**
>
> Enterprise Manager cannot resolve compatibility issues if the payload is incompatible with the OSCAP installed on the hosts. It can only report these errors.

SCAP Prerequisites

In order to upload and use SCAP supported standards, OSCAP (Open SCAP) needs to be installed in the agent targets using the install method of your choice (RPM, YUM, DNF). To download OSCAP see: https://www.open-scap.org/download/.

> **Note:**
>
> If you are using Oracle Linux make sure that the `LibXML` PERL module is installed. To install use the following code:
>
> ```
> yum install "perl(XML::LibXML)"
> ```

Before using SCAP supported standards, the Database Lifecycle Management Pack for Oracle Database is required. For more information see: Database Lifecycle Management Pack for Oracle Database.

For information on how to install binaries in Oracle Linux using YUM see: Installing Software from Oracle Linux Yum Server.

SCAP Best Practices

- Ensure the OSCAP command runs with the desired XCCDF STIG profile on a few reference hosts. (Outside of Enterprise Manager)
- Ensure the other hosts where you intend to run OSCAP are identical to the reference hosts.
- Ensure the latest OSCAP version is installed on all hosts. (YUM or RPM install)

Once all these best practice pre-requisites are met, you can now:

- Associate all the Enterprise Manager host targets to the newly created SCAP compliance standard.
- Upload SCAP standards by uploading the XCCDF file containing the desired SCAP standards, this will create a new standard in the Compliance library.

.

SCAP Standards Available for Oracle Linux 7

The following is a list of SCAP Standards included in Oracle Enterprise Manager 24.1:

Health Insurance Portability and Accountability Act (HIPAA): The HIPAA Security Rule establishes US national standards to protect individuals' electronic personal health information that is created, received, used or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. This profile configure Oracle Linux 7 to the HIPAA Security Rule for securing electronic protected health information. (V0.1.72).

For more information on securing Linux configuration for HIPAA compliance see: https://complianceascode.github.io/content-pages/guides/ssg-ol7-guide-hipaa.html.

DISA STIG For Oracle Linux 7: This profile contains configuration checks that align to DISA STIG for Oracle Linux V1R1. (V0.1.72).

For more information see: https://complianceascode.github.io/content-pages/guides/ssg-ol7-guide-stig.html

PCI-DSS v3.2.1 Control Baseline for Oracle Linux 7: Ensures PCI-DSS v3.2.1 related security configuration settings are applied. (V0.1.72).

For more information see: https://complianceascode.github.io/content-pages/guides/ssg-ol7-guide-pci-dss.html

Standard System Security Profile for Oracle Linux 7: This profile contains rule to ensure standard security baseline of an Oracle Linux 7 system. (V0.1.72).

For more information see: https://complianceascode.github.io/content-pages/guides/ssg-ol7-guide-standard.html

SCAP Standards Available for Oracle Linux 8

The following is a list of SCAP Standards included in Oracle Enterprise Manager 24.1:

Health Insurance Portability and Accountability Act (HIPAA): The HIPAA Security Rule establishes US national standards to protect individuals' electronic personal health information that is created, received, used or maintained by a covered entity. The Security Rule requires

appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. This profile configure Oracle Linux 8 to the HIPAA Security Rule for securing electronic protected health information. (V0.1.72). For more information on securing Linux configuration for HIPAA compliance see: https://complianceascode.github.io/content-pages/guides/ssg-ol8-guide-hipaa.html.

DISA STIG for Oracle Linux 8: This profile contains configuration checks that align to DISA STIG for Oracle Linux 8. (V0.1.72).

For more information see: https://complianceascode.github.io/content-pages/guides/ssg-ol8-guide-stig.html.

PCI-DSS v3.2.1 Control Baseline Draft for Oracle Linux 8: Ensures PCI-DSS v3.2.1 related security configuration settings are applied. (V0.1.72).

For more information see: https://complianceascode.github.io/content-pages/guides/ssg-ol8-guide-pci-dss.html.

Standard System Security Profile for Oracle Linux 8: his profile contains rule to ensure standard security baseline of an Oracle Linux 8 system. (V0.1.72).

For more information see: https://complianceascode.github.io/content-pages/guides/ssg-ol8-guide-standard.html.

SCAP Standards Available for Oracle Linux 9

The following is a list of SCAP Standards included in Oracle Enterprise Manager 24.1:

Health Insurance Portability and Accountability Act (HIPAA): The HIPAA Security Rule establishes US national standards to protect individuals' electronic personal health information that is created, received, used or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. This profile configure Oracle Linux 9 to the HIPAA Security Rule for securing electronic protected health information. (V0.1.69). For more information on securing Linux configuration for HIPAA compliance see: https://complianceascode.github.io/content-pages/guides/ssg-ol9-guide-hipaa.html.

DISA STIG for Oracle Linux 9: This profile contains configuration checks that align to DISA STIG for Oracle Linux 9. (V0.1.69).

For more information see: https://complianceascode.github.io/content-pages/guides/ssg-ol9-guide-stig.html.

PCI-DSS v3.2.1 Control Baseline Draft for Oracle Linux 9: Ensures PCI-DSS v4.0 related security configuration settings are applied. (V0.1.69).

For more information see: https://complianceascode.github.io/content-pages/guides/ssg-ol9-guide-pci-dss.html.

Standard System Security Profile for Oracle Linux 9: his profile contains rule to ensure standard security baseline of an Oracle Linux 8 system. (V0.1.69).

For more information see: https://complianceascode.github.io/content-pages/guides/ssg-ol9-guide-standard.html.

Import XCCDF based standards using EMCLI

SCAP XCCDF standards that are not included by default can be imported into enterprise manager with the EM CLI verb `upload_compliance_standard` and a `-file` parameter with the XML data stream file containing one or more standards.

Example:

```
$ emcli upload_compliance_standard -file="ssg-ol8-ds.xml"
```

22

AHF EXAchk Compliance Standards

This chapter explains AHF EXAchk Compliance Standards for Exadata Engineered Systems managed by Enterprise Manager utilizing Autonomous Health Framework (AHF).

About AHF EXAchk Compliance Standards

Oracle AHF EXAchk is a lightweight and non-intrusive health check framework for stack of software and hardware components in Exadata. Enterprise Manager provides a set of compliance standards and associated controls for overall health monitoring, automated risk identifications and proactive notification of issues for each Exadata System component and database instances.

- Oracle Enterprise Manager 13 Release 5 Update 3 (13.5.0.3) integrates Oracle Autonomous Health Framework (AHF) EXAchk for Exadata Engineered Systems.
- Oracle Enterprise Manager 13 Release 5 Update 6 (13.5.0.6) integrates Oracle Autonomous Health Framework (AHF) EXAchk for Virtual Exadata Engineered Systems.
- Oracle Enterprise Manager 13 Release 5 Update 12 (13.5.0.12) integrates Oracle Autonomous Health Framework (AHF) EXAchk for Exadata Cloud@Customer (ExaCC) targets.

AHF EXAchk standards are available out-of-box. When you update AHF, the associated EXAchk compliance standards are automatically updated to the corresponding version.

For more information on AHF EXAchk see: Autonomous Health Framework

Prerequisites for AHF EXAchk Compliance Standards

In order to utilize AHF EXAchk Compliance Standards, the following prerequisites must be met:

1. The latest version of Autonomous Health Framework (AHF) needs to be installed in the target to be monitored. For more information on installing AHF EXAchk see: Installing and Upgrading Oracle Autonomous Health Framework in *Oracle Autonomous Health Framework Checks and Diagnostics User's Guide*.
2. Ensure the latest version of the Enterprise Manager agent is installed on the compute nodes.
    a. For on-premises Exadata, Enterprise Manager agent must be version 13.5.0.3 or later.
    b. For virtual Exadata, Enterprise Manager agent must be version 13.5.0.6 or later.
    c. For Exadata Cloud@Customer (ExaCC), Enterprise Manager agent must be version 13.5.0.12 or later.
3. Ensure the latest version of Enterprise Manager is installed.
    a. For on-premises Exadata, Enterprise Manager must be version 13.5.0.3 or later.
    b. For virtual Exadata, Enterprise Manager must be version 13.5.0.6 or later.

c. For Exadata Cloud @Customer (ExaCC), Enterprise Manager must be version 13.5.0.12 or later.

> **Note:**
>
> AHF EXAchk Compliance Standards will not work on Enterprise Manager deployments with the ORAchk Healthchecks Plug-in installed. Ensure the following for AHF EXAchk Compliance Standards to properly work:
>
> 1. Disassociate any Exadata systems and/or components using the ORAchk Healthchecks plug-in.
> 2. Remove the ORAchk Healthchecks plug-in entirely. For more information on removing the plug-in see: Undeploying Plug-Ins in *Oracle Enterprise Manager Administrator's Guide*

Oracle Exadata infrastructure for Oracle Engineered systems

Oracle Exadata Database Machine

To associate, follow the instructions in: Associate Exadata Components to AHF EXAchk Standards and filter your targets by **Oracle Exadata Database Machine** select the standard **AHF EXAchk System Best Practices for Oracle Engineered System** and click **Associate**. Once associated the rest of the standards will be associated automatically to all linked targets.

AHF EXAchk (Exadata Health Check) standard provides a comprehensive diagnostic scan, identifying potential issues within the Oracle Exadata Database Machine and its components, thus ensuring peak performance and reliability. By leveraging deep insights into system configurations, performance metrics, and best practice recommendations, AHF EXAchk enables administrators to proactively manage and optimize their Exadata environments.

With its ability to automatically detect and report critical vulnerabilities, AHF EXAchk significantly enhances the security posture of Oracle Exadata Database Machines. Administrators are empowered with actionable intelligence to swiftly address security concerns, safeguarding sensitive data and maintaining compliance with stringent regulatory standards.

Oracle Exadata Database Infrastructure

It is highly recommended to associate your ExaCC and ExaCS Exadata infrastructure systems targets with **AHF EXAchk Exadata Infrastructure Best Practices for Oracle Engineered System** compliance standards. This standard encompasses all Oracle Exadata infrastructure components with their compliance standards, ensuring that every component within Exadata Infrastructure is properly managed per compliance management.

It is also highly recommended to associate your on-premises physical and virtual Oracle Exadata Database Machine systems targets with the **AHF EXAchk system best practices for Oracle Engineered System** compliance standards. This standard encompasses all Oracle Exadata physical, and virtual systems within the engineered system and is properly managed per compliance management.

AHF EXAchk standard provides deep diagnostics and proactive health checks across your Oracle Exadata Cloud at Customer (EXACC) and Exadata Cloud Service (EXaCS), preemptively identifying and mitigating potential system vulnerabilities and performance bottlenecks. It ensures seamless integration and optimal performance of Oracle Exadata database infrastructure, including EXACC and EXaCS, by leveraging comprehensive checks

and best practices, thereby enhancing reliability, scalability, and security in cloud and on-premises environments.

AHF EXAchk Component Standards

The following are the list of Exadata component standards:

Exachk HTML reports contains rule severity values that differ from Enterprise Manager Compliance rules report violations. Given these changes the Engineered Systems tab works differently that other Compliance tabs. With Engineered Systems, even if there is one Critical violation it reports the target as non compliant. This differs from other compliance standards that use a graded system to generate the compliance report.

The grading system for EXAchk Component standards is as follows:

1. A score of 80 to 100 is labeled as **Compliant**
2. A score of 60 to 80 is labeled as **Warning**
3. A score below 60 is labeled as **Critical/Non compliant**

If a target has at least one Critical/Non compliant standard the target is reported as non compliant.

Component/Target Name	Exadata Component Standard Name	Description
Oracle Exadata Database Machine	AHF EXAchk System Best Practices for Oracle Engineered System	System Best Practices for configuration check, overall health monitoring, automatic risk identification and proactive notification of issues in an Oracle Engineered System. This compliance standard checks version uniformity among all Exadata components. • All database nodes (hosts) must have the same software version • All storage cells must have the same software version • All network switches must have the same software version
Oracle Exadata Infrastructure	AHF EXAchk Exadata Infrastructure Best Practices for Oracle Engineered System	Exadata Infrastructure (ExaCC and ExaCS) Best Practices for configuration check, overall health monitoring, automated risk identification and proactive notification of issues in an Oracle Engineered System.
Database Instance	AHF EXAchk Database Instance Best Practices for Oracle Engineered System	Single Instance Database Best Practices for configuration check, overall health monitoring, automated risk identification and proactive notification of issues in an Oracle Engineered System.

Component/Target Name	Exadata Component Standard Name	Description
Cluster Database	AHF EXAchk Cluster Database Best Practices for Oracle Engineered System	Cluster Database Best Practices for configuration check, overall health monitoring, automated risk identification and proactive notification of issues in an Oracle Engineered System.
Oracle Home	AHF EXAchk Oracle Home Best Practices for Oracle Engineered System	Oracle Home Best Practices for configuration check, overall health monitoring, automated risk identification and proactive notification of issues in an Oracle Engineered System.
Host	AHF EXAchk Host Best Practices for Oracle Engineered System	Host Best Practices for configuration check, overall health monitoring, automated risk identification and proactive notification of issues in an Oracle Engineered System.
Cluster	AHF EXAchk Cluster Best Practices for Oracle Engineered System	Cluster Best Practices for configuration check, overall health monitoring, automated risk identification and proactive notification of issues in an Oracle Engineered System.
Cluster ASM	AHF EXAchk ASM Cluster Best Practices for Oracle Engineered System	Cluster ASM Best Practices for configuration check, overall health monitoring, automated risk identification and proactive notification of issues in an Oracle Engineered System.
Oracle Exadata Storage Server	AHF EXAchk Storage Server Best Practices for Oracle Engineered System	Storage Server Best Practices for configuration check, overall health monitoring, automated risk identification and proactive notification of issues in an Oracle Engineered System.
Oracle Infiniband Switch	AHF EXAchk Infiniband Switch Best Practices for Oracle Engineered System	Infiniband Switch Best Practices for configuration check, overall health monitoring, automated risk identification and proactive notification of issues in an Oracle Engineered System.
Automatic Storage Management	AHF EXAchk Automatic Storage Management Best Practices for Oracle Engineered System	Automatic Storage Management Best Practices for configuration check, overall health monitoring, automated risk identification and proactive notification of issues in an Oracle Engineered System.
Oracle High Availability Service	AHF EXAchk High Availability Service Best Practices for Oracle Engineered System	High Availability Service Best Practices for configuration check, overall health monitoring, automated risk identification and proactive notification of issues in an Oracle Engineered System.

Component/Target Name	Exadata Component Standard Name	Description
System Infrastructure Switch / RoCE	AHF EXAchk Systems Infrastructure Switch Best Practices for Oracle Engineered System	Systems Infrastructure Switch Best Practices for configuration check, overall health monitoring, automated risk identification and proactive notification of issues in an Oracle Engineered System.
Oracle VM Instance	AHF EXAchk Virtual Server Best Practices for Oracle Engineered System	Virtual Server Best Practices for configuration check, overall health monitoring, automated risk identification and proactive notification of issues in an Oracle Engineered System.
Oracle Virtual Platform	AHF EXAchk Virtual Platform Best Practices for Oracle Engineered System	Virtual Platform Best Practices for configuration check, overall health monitoring, automated risk identification and proactive notification of issues in an Oracle Engineered System.

Associate Exadata Components to AHF EXAchk Standards

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Select the **Compliance Standards** tab and select the EXAchk standard.
3. Select the Exadata component target to be monitored and click **Associate Targets**.
4. Click **Add** and select the targets you want to monitor. The targets will appear in the table after you close the selector dialog.
5. Click **OK** to confirm that you want to save the EXAchk association.
6. After deployment and subsequent configuration collection occurs, you can view the results from the EXAchk Standards in one of three ways:
   - Navigate from the **Enterprise** menu, select **Compliance**, then select **Dashboard**. The compliance dashboard has a dedicated Engineered Systems tab. For more information on the Compliance Dashboard see: About the Compliance Dashboard in *Oracle Enterprise Manager Database Lifecycle Management Administrator's Guide*.
   - Navigate from the **Enterprise** menu, select **Compliance**, then select **Results**. In the Compliance Results page select the Compliance standard you wish to review and click **Show Details**.
   - Within each Exadata target home page the compliance results are available. To view navigate to **Targets** then select **Systems** and click on the target you wish to view. The results will be under the **Compliance Summary** section.

   In the Compliance Dashboard scroll down to the Compliance Summary and select either the **Standards** or **Targets** tab. Click on either the number below **Compliant Targets** or **Non-Compliant Targets**, and in the pop up select **Report** for the Compliance Standard HTML report or select **AHF EXAchk Report** for the raw HTML AHF EXAchk report.

AHF EXAchk Compliance Standards Known Issues

First Time or Initial Compliance Score States 100% For All Targets

There are several ways to verify that your AHF EXAchk Compliance Standards are configured correctly:

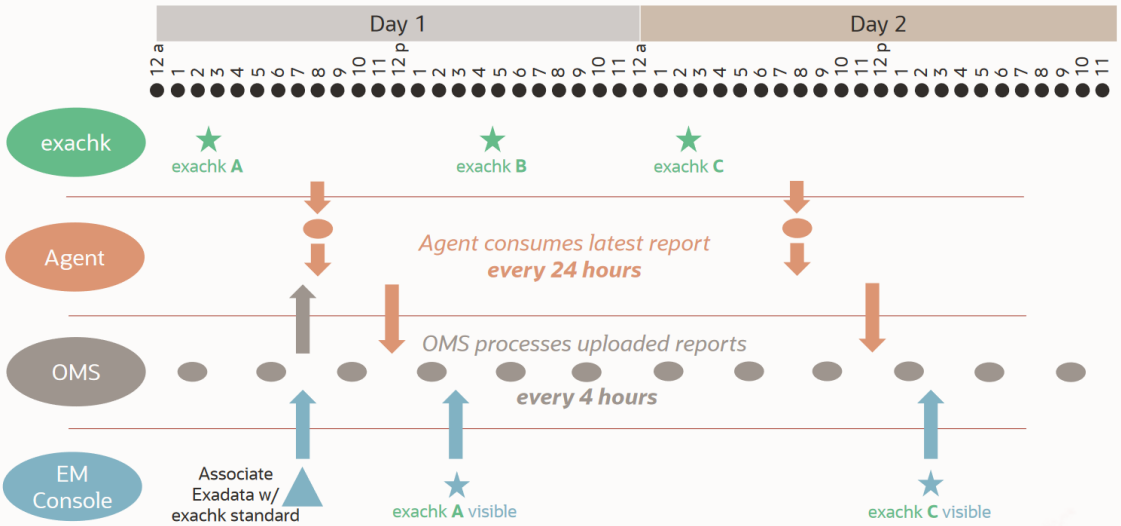
1. Go to the **Targets** drop down menu, then select **Exadata**. In the list of available targets locate the primary **DB Machine** to trouble shoot and click **More**. Locate your primary compute node **Host** target and select it. Go to **Host**, then **Configuration** and select **Latest**. Click **AHF EXAchk Metadata Config-Metadata**, this shows the AHF version installed in the host target, this version should be same or lower than that of the one in the Compliance Library.
2. Go to the **Targets** drop down menu, then select **Exadata**. In the list of available targets locate the primary **DB Machine** to trouble shoot and click **More**. Locate your primary compute node **Host** target and select it. Go to **Host**, then **Configuration** and select **Latest**. Click on **AHF EXAchk Result Configuration**, click **Location**.
   - If you see an error for no credentials, configure the Monitoring Credentials.
   - Errors are shown and described in this window allowing for easy troubleshooting.
   - If results are blank, AHF EXAchk data is sent by each Exadata target every 24 hours. This data is collected in a central store by the management server as and when it arrives from each target. The Compliance Evaluation is performed every 4 hours by referring to the latest AHF EXAchk data available in the central store at that time.
3. AHF EXAchk Compliance Evaluation is performed every 4 hours, to verify that the jobs are running properly go to **Enterprise**, then **Job** and click on **Activity**. Search for and click on **COMPLIANCE_RE_EVAL_EXACHK**. A new window will open showing what targets are associated to what standards. If there are none or missing, re-associate targets to standards.

EXAchk Compliance Is Not Being Displaying After Onboarding

EXAchk has several underlying jobs that run at different refresh intervals throughout the day, this may cause a lag in an Exadata apearing under EXAchk Compliance. The following jobs need to happen for data collection:

- The EXAchk Compliance tool has its own job run schedule separate from the rest at a determined time.
- The EM Config Extension job runs once every 24 hour refresh interval, during which it consumes the EXAchk results.
- The EM Agent Compliance Collection job runs once every 24 hours. This service sends the results processed by the Config Extension to the repository.
- OMS jobs run every 4 hours looking for new results, once found they are converted into EXAchk rule results.

Figure 22-1 EXAchk Process Calendar



23

Oracle Database Security Assessment Tool Compliance Standard

Is a popular command-line tool that identifies areas where your database configuration, operation, or implementation introduce risk. DBSAT recommends changes and controls to mitigate risks. DBSAT helps assess how secure the database is configured, determines who the users and their entitlements are, and identifies where sensitive data resides within the database.

With Oracle Enterprise Manager 24.1ai Release 1 (24.1) DBSAT 3.1 is integrated as a Compliance Standard. This will allow you to associate your database targets, run the security assessment through the existing Compliance functionality and view it's results directly in Enterprise Manager through the Security Assessment Report.

The Sensitive Data Assessment report is also available for EM 24.1ai further enhancing DBSAT offerings in Enterprise Manager. There are no additional DBSAT association actions to be performed to generate this second report.

With EM 24.1ai, DBSAT can also be used with Pluggable databases (PDB) and Real Application Cluster (RAC) databases.

For more information on DBSAT see: Oracle Database Security Assessment Tool.

Oracle DBSAT Compliance Standard Prerequisites

The following are a list of prerequisites required for Oracle DBSAT to be deployed as a Compliance Standard.

- Currently Oracle DBSAT Compliance Standard is available only for Oracle Red Hat Linux 7 and above.
- The DBSAT Standard must be associated to the database target which is being monitored by EM agent running on the same host OS.
- Oracle DBSAT Compliance Standard requires a minimum version of Oracle Enterprise Manager 13 Release 5 Update 5 (13.5.0.5) for single instance and CDBs. Oracle Enterprise Manager 13 Release 5 update 22 (13.5.0.22) is required for PDBs and RAC databases.
- Oracle Enterprise Manager 13 Release 5 Update 11 (13.5.0.11) is required to use the Sensitive Data Assessment Report.
- Oracle DBSAT Compliance Standard requires PERL installed on the database target being monitored by the EM agent.

  1. Verify PERL is installed:

     ```
     perl -v
     ```

> **Note:**
>
> If PERL is already installed in the database target being monitored by EM, there is no further action to be taken.

2. To install the PERL modules use the following commands:

```
sudo yum -y install perl-DBI
sudo yum install -y perl-XML-XPath
```

If the installation is correct, the following messages will be displayed:

```
Loaded plugins: langpacks, ulninfo Package perl-DBI-1.627-4.el7.x86_64 already
installed and latest version
Loaded plugins: langpacks, ulninfo Package perl-XML-XPath-1.13-22.el7.noarch
```

- In order for the integrated reported to with the Enterprise Manager integrated DBSAT, Python needs to installed.

1. Unzip Python onto the server:

```
yum install -y zip unzip python
```

2. Check the Python version installed, it must be 2.7.5 or higher:

```
python -V
```

It will return the installed version:

```
Python 2.7.5
```

- If you are planning on using Discoverer with DBSAT, a Java 8 JDK environment is required. The `JAVA_HOME` environment variable needs to be set with the following command:

```
JAVA_HOME=/u01/jdk1.8.0_181
```

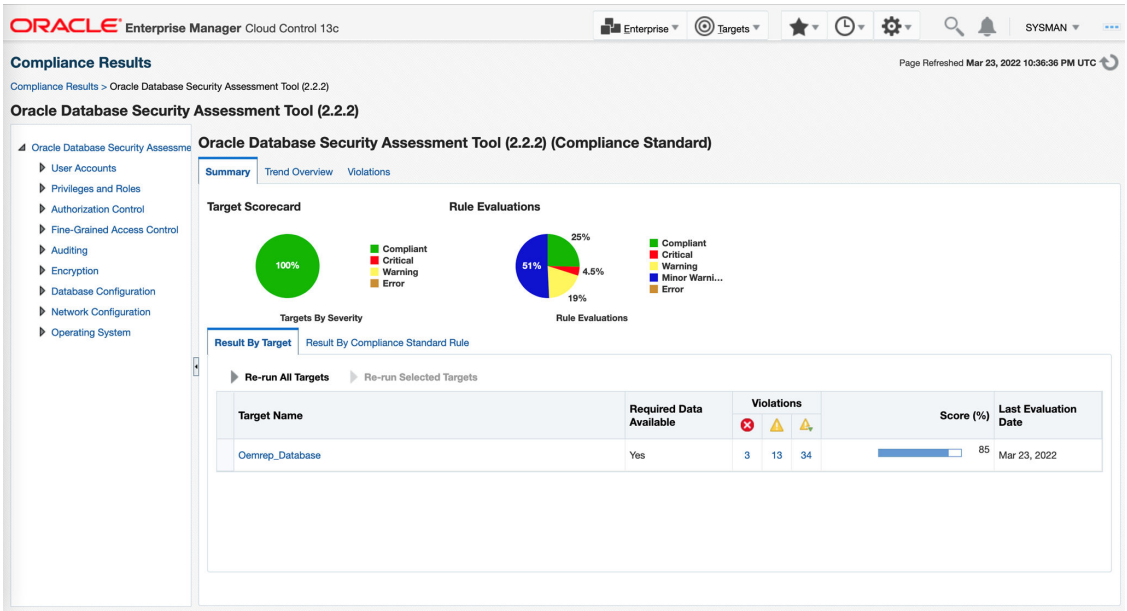
For further information on prerequisites for the DBSAT tool see: Oracle Database Security Assessment Tool Prerequisites.

Oracle DBSAT Compliance Standard Results

DBSAT Compliance Standard Overview

You can review the compliance information collected by Oracle DBSAT under Compliance Results, by navigating to **Database Security Assessment Tool**. Here the information collected is presented in an easy to read template within Enterprise Manager. Showing Scorecard, Rule Evaluation, Target Violations, Targets and Evaluation Date.

Figure 23-1 DBSAT Compliance Standard Overview



DBSAT Compliance Standard Reports

In addition to the standard HTML Compliance report, you can also open the raw HTML reports generated by the DBSAT tool. To verify both of these reports (Security Assessment Report and Sensitive Data Assessment Report) follow these steps:

1. Navigate to **Enterprise**, highlight **Compliance** and click on **Dashboard**.
2. In the Compliance Dashboard scroll down to the Compliance Summary and select either the **Standards** or **Targets** tab.
3. Click on the number below **Compliant Targets** or **Non-Compliant Targets**.
4. In the pop up select **DBSAT Report** for the raw HTML DBSAT report.
5. In the DBSAT Report pop up there are two report options **Security Assessment Report** and **Sensitive Data Assessment Report**, click on the report of your choosing.

Figure 23-2 HTML Report Options

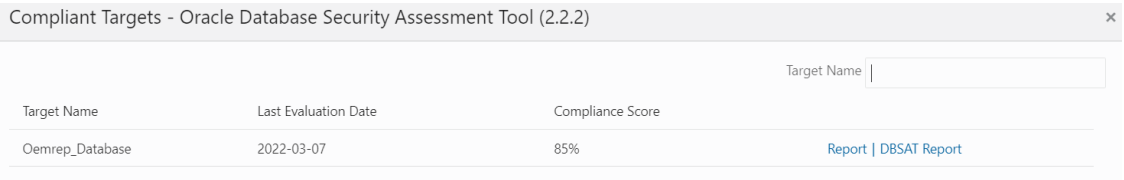
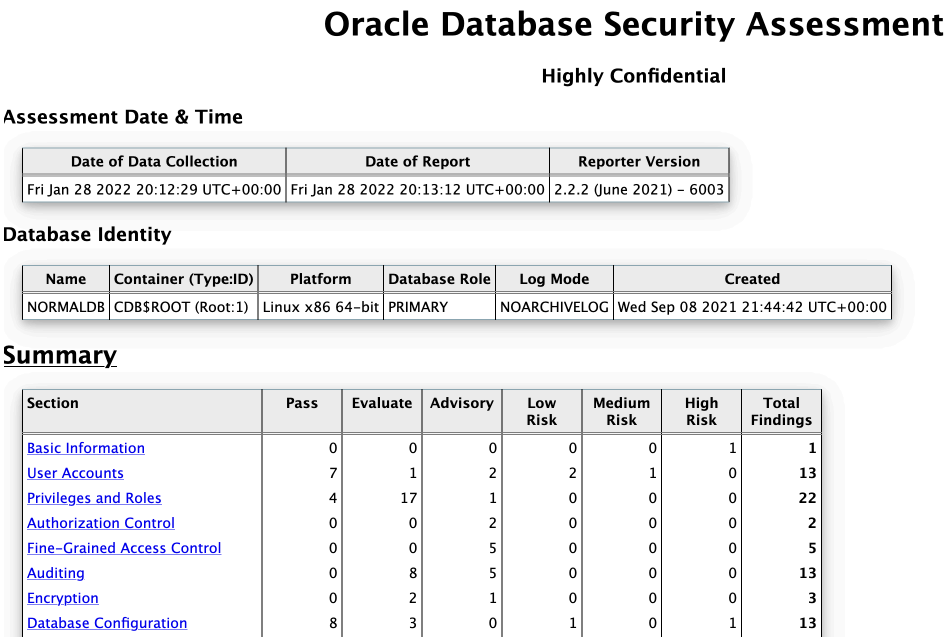


Figure 23-3 Oracle Database Security Assessment Report



Oracle Database Security Assessment

Highly Confidential

Assessment Date & Time

Date of Data Collection	Date of Report	Reporter Version
Fri Jan 28 2022 20:12:29 UTC+00:00	Fri Jan 28 2022 20:13:12 UTC+00:00	2.2.2 (June 2021) - 6003

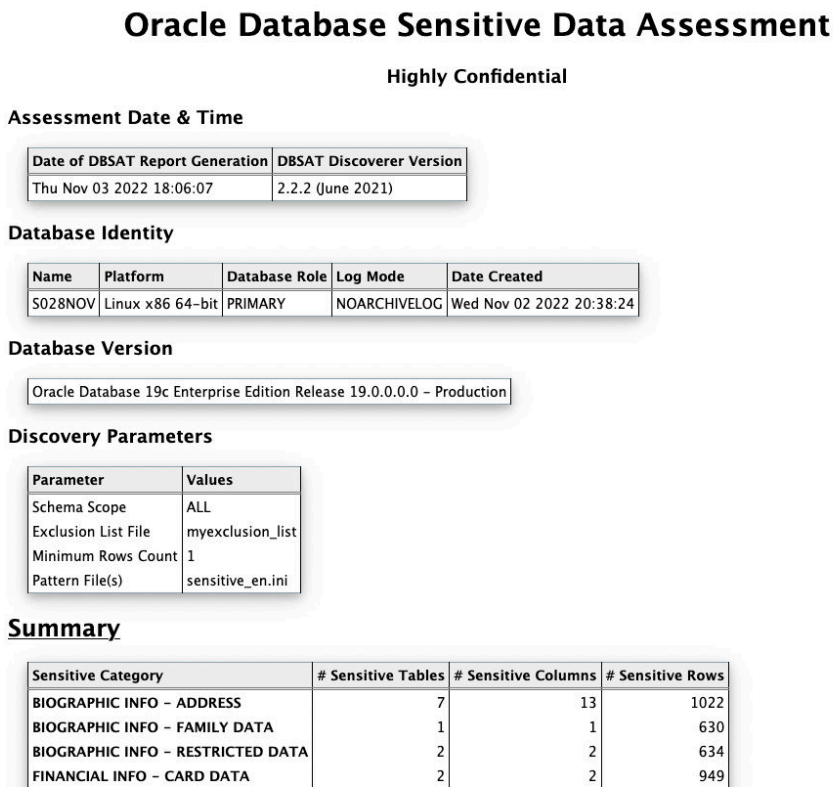
Database Identity

Name	Container (Type:ID)	Platform	Database Role	Log Mode	Created
NORMALDB	CDB$ROOT (Root:1)	Linux x86 64-bit	PRIMARY	NOARCHIVELOG	Wed Sep 08 2021 21:44:42 UTC+00:00

Summary

Section	Pass	Evaluate	Advisory	Low Risk	Medium Risk	High Risk	Total Findings
Basic Information	0	0	0	0	0	1	1
User Accounts	7	1	2	2	1	0	13
Privileges and Roles	4	17	1	0	0	0	22
Authorization Control	0	0	2	0	0	0	2
Fine-Grained Access Control	0	0	5	0	0	0	5
Auditing	0	8	5	0	0	0	13
Encryption	0	2	1	0	0	0	3
Database Configuration	8	3	0	1	0	1	13

Figure 23-4 Oracle Database Sensitive Data Assessment



Oracle Database Sensitive Data Assessment

Highly Confidential

Assessment Date & Time

Date of DBSAT Report Generation	DBSAT Discoverer Version
Thu Nov 03 2022 18:06:07	2.2.2 (June 2021)

Database Identity

Name	Platform	Database Role	Log Mode	Date Created
S028NOV	Linux x86 64-bit	PRIMARY	NOARCHIVELOG	Wed Nov 02 2022 20:38:24

Database Version

Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production

Discovery Parameters

Parameter	Values
Schema Scope	ALL
Exclusion List File	myexclusion_list
Minimum Rows Count	1
Pattern File(s)	sensitive_en.ini

Summary

Sensitive Category	# Sensitive Tables	# Sensitive Columns	# Sensitive Rows
BIOGRAPHIC INFO - ADDRESS	7	13	1022
BIOGRAPHIC INFO - FAMILY DATA	1	1	630
BIOGRAPHIC INFO - RESTRICTED DATA	2	2	634
FINANCIAL INFO - CARD DATA	2	2	949

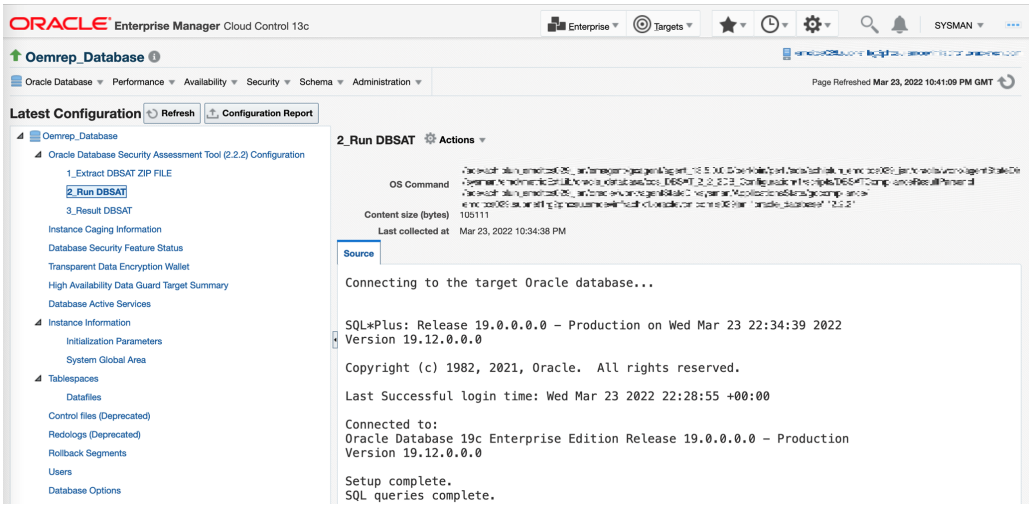
In order to setup Oracle DBSAT Compliance Standard see: About Compliance Standards in *Oracle Enterprise Manager Database Lifecycle Management Administrator's Guide*.

Oracle DBSAT Compliance Standard Known Issues

The following is a list of known issues and their most common solutions for Oracle DBSAT Compliance Standard.

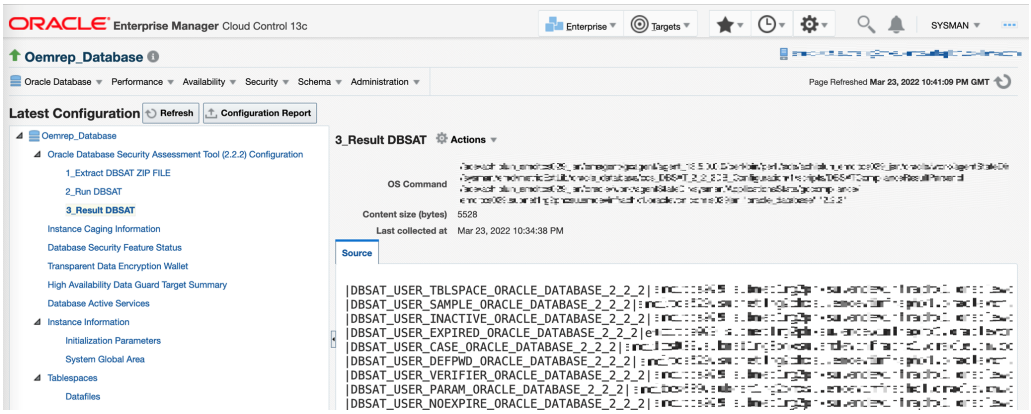
- In some instance Compliance score initially states 100% for all targets. There are several ways to verify that your Oracle DBSAT Compliance Standards are configured correctly:
  - Verify Run DBSAT settings:
    1. From the **Targets** menu, select **Databases**. On the Databases page, select **Database Name**.
    2. On the selected Database page, go to the Oracle Database drop down menu, select **Configuration**, then select **Latest**.
    3. On the Database page with Identity Latest Configuration, click on **Database**, select **Oracle Database Security Assessment Tool (2.2.2) Configuration** then select **2_Run_DBSAT**. This shows the current run execution of DBSAT any errors will be listed here.

Figure 23-5 Run DBSAT Settings



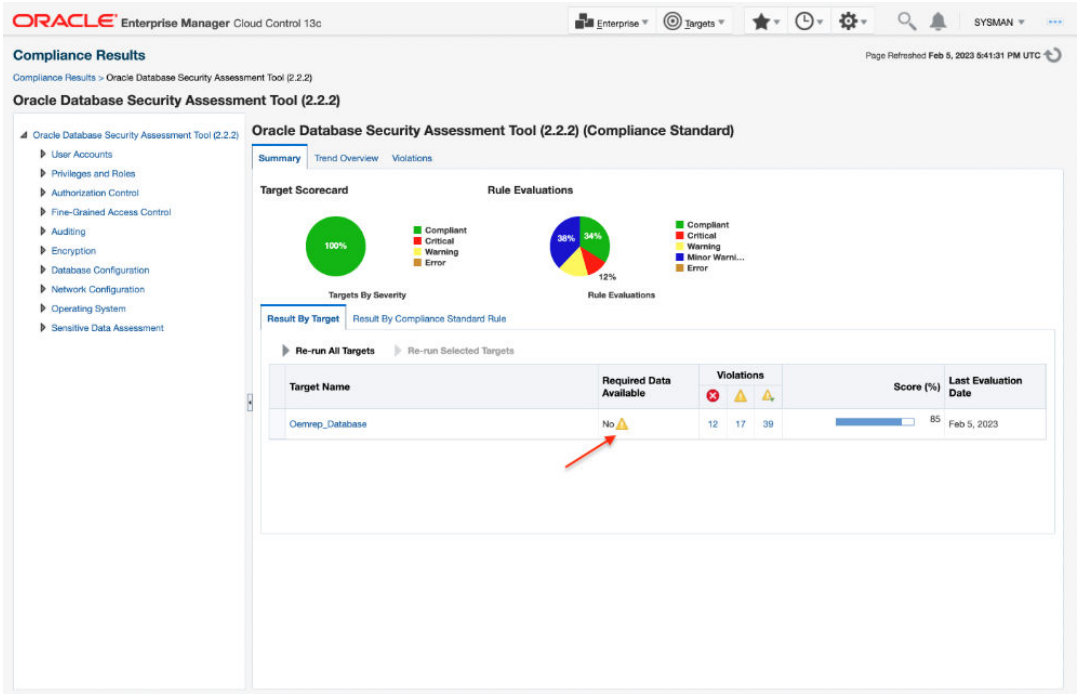
  - Verify DBSAT Result settings:
    1. From the **Targets** menu, select **Databases**. On the Databases page, select **Database Name**.
    2. On the selected database page, go to the Oracle Database drop down menu, select **Configuration**, then select **Latest**.
    3. On Database page with Identity Latest Configuration components, click on **Database**, select **Oracle Database Security Assessment Tool (2.2.2) Configuration** then select **3_Result_DBSAT**. If the **Source** field is blank, DBSAT execution failed to generate valid results. Check the errors displayed in **Run DBSAT** for possible remediation.

Figure 23-6 DBSAT Results Settings



- Required Data Available shows **No** even though a report was successfully generated. There are situations where the DBSAT script runs and creates the expected data and report, but the script also reports non-zero exist status which causes the Enterprise Manager agent to report an error. To verify go to **Enterprise** then select **Compliance** and click on **Results**. This opens the Compliance Results page, every row represents one standard associated to a number of targets. Clicking a standard opens the results for that combination, for DBSAT even when valid results data is obtained, the column shows *No*. This is because the DBSAT script reports a false error even though it managed to collect the required data.

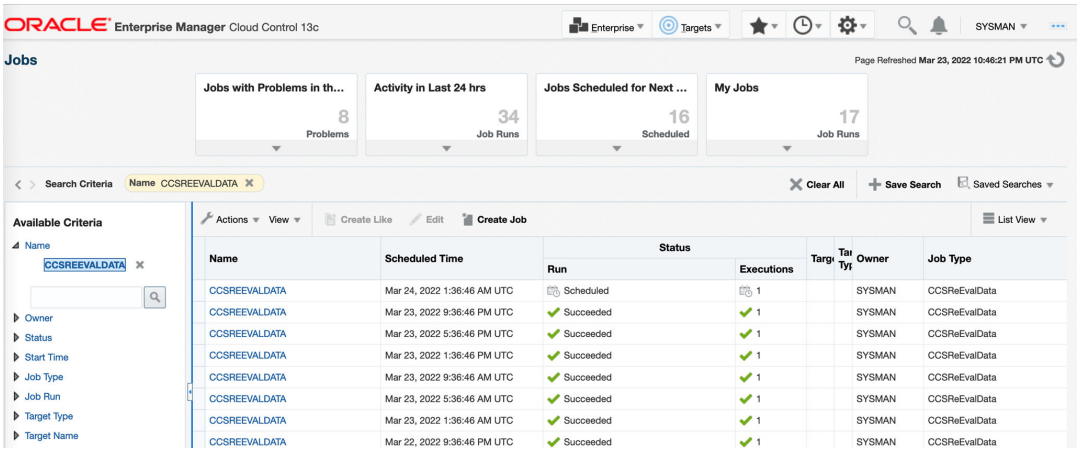
Figure 23-7 Required Data Available



There is no remedial action to take, do not trust the **Required Data Available** column only for DBSAT. Instead verify the status of the actual DBSAT command by following the steps previously outlined.

- DBSAT data is sent by the DBSAT target every 24 hours. This data is collected in a central store by the management server as it arrives from each target. The Compliance Evaluation is performed every 4 hours by referring to the latest DBSAT data available in the central store at that time. To verify that the jobs are running properly go to **Enterprise**, then **Job** and click on **Activity**. On Jobs Page, in the **Available Criteria** components panel, select **Name** and **Search** by entering value **CCSREEVALDATA**, information will show targets with their respective associated standards. If there are none or missing, reassociate targets to their respective standards.

Figure 23-8 DBSAT Job Overview



- DBSAT and the Enterprise Manager integration tool do not work if there is a space character in the database monitoring user's password. Common database password guidelines discourage usage of a space character in password. To remedy change the password of the Oracle Database monitoring user (typically DBSNMP).

Index