Oracle® Enterprise Manager

Cloud Control Oracle Database Compliance Standards

12*c* Release 2 (12.1.0.2)

E36074-01

August 2012

ORACLE®

Oracle Enterprise Manager Cloud Control Oracle Database Compliance Standards, 12*c* Release 2 (12.1.0.2)

E36074-01

Primary Author: Jacqueline Gosselin

Contributor: Jerry Russell, David Wolf

Contents

Preface

Enterprise Manager 12*c* provides a rich and powerful compliance management framework that automatically tracks and reports conformance of managed targets to industry, Oracle, or internal standards. Enterprise Manager 12*c* ships with compliance standards for Oracle hardware and software including Database, Exadata Database Machine, Fusion Middle Ware, VM Manager and more. These compliance standards validate conformance to Oracle configuration recommendations, best practices, and security recommendations.

Audience

This document is intended for database administrators.

This document provides you with an understanding of the provided Oracle Database 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 have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For more information, see the following document in the Oracle Enterprise Manager Release 12*c* documentation set:

- *Oracle® Enterprise Manager Lifecycle Management Administrator's Guide*

Conventions

The following text conventions are used in this document:

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

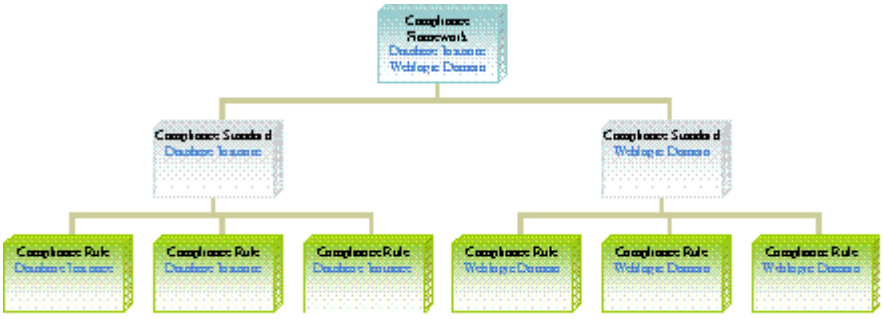
1 Introduction

Enterprise Manager 12*c* provides a rich and powerful compliance management framework that automatically tracks and reports conformance of managed targets to industry, Oracle, or internal standards. Enterprise Manager 12*c* ships with compliance standards for Oracle hardware and software including Database, Exadata Database Machine, Fusion Middleware, and more. These compliance standards validate conformance to Oracle configuration recommendations, best practices, and security recommendations.

1.1 Compliance Overview

The compliance framework in Enterprise Manager 12*c* is hierarchical in nature allowing for ease of management and reuse. Starting from the top level, the hierarchy contains Compliance Frameworks, Compliance Standards, and Compliance Rules. Compliance Frameworks aggregate the compliance scores of Compliance Standards which may be for different target types. Compliance Standards contain one or more Compliance Rules but are specific to a single target type. Compliance Rules are responsible for executing a single and specific validation of a target and reporting conformance.

Figure 1–1 Compliance Framework Hierarchy



Compliance Standards are the only item associated to a target. Once associated, all rules contained in the compliance standard are executed against the data in the Enterprise Manager repository. 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 Enterprise Manager 12*c* - Lifecycle Management Administrator's Guide.

As of this writing, there are 23 database compliance standards provided with Oracle Enterprise Manager 12*c*. The breakdown of these is as follows:

Table 1–1 Compliance Standards by Target Type

Target Type	Compliance Standards
Automatic Storage Management	2
Cluster	1
Cluster Database	7
Database Instance	9
Host	2
Listener	2
Total	23

1.2 Oracle Database Compliance Standards

For the Oracle Database and related targets, Enterprise Manager 12*c* ships with 16 ready-to-use compliance standards. Users can choose to implement some or all of these compliance standards which consist of more than 300 compliance rules. The following is a list of compliance standards by target type.

Oracle Single Instance Database Standards

- Basic Security Configuration for Oracle Database
- Configuration Best Practices for Oracle Database
- High Security Configuration for Oracle Database
- Patchable Configuration for Oracle Database
- Storage Best Practices for Oracle Database

Oracle Real Application Cluster Database Standards

- Basic Security Configuration for Oracle Cluster Database
- Configuration Best Practices for Oracle Real Application Cluster Database
- High Security Configuration for Oracle Cluster Database
- Patchable Configuration for Real Application Cluster Database
- Storage Best Practices for Oracle Real Application Cluster Database
- Basic Security Configuration for Oracle Cluster Database Instance
- High Security Configuration for Oracle Cluster Database Instance

Automatic Storage Management (ASM) Standards

- Storage Best Practices for ASM
- Patchable Configuration for ASM

Oracle Listener Standards

- Basic Security Configuration for Oracle Listener
- High Security Configuration for Oracle Listener

In order to leverage a security standard, you must apply the following templates first.

- To leverage any of the "Security" compliance standards, users must enable additional configuration collections for targets they wish 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 and Listener. Table 2 lists the Oracle Certified monitoring template that can be used to enable the required configuration collections necessary for use in the Security Standards. For complete information on how to use Monitoring templates see the *Enterprise Manager 12c - Administrator's Guide*.

Table 1–2 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
Listener	Oracle Certified-Enable Listener Security Configuration Metrics	Basic Security Configuration for Oracle Listener
		High Security Configuration for Oracle Listener

Note: Monitoring Template and Compliance Standard names as of Bundle Patch 1 (February 2012).

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

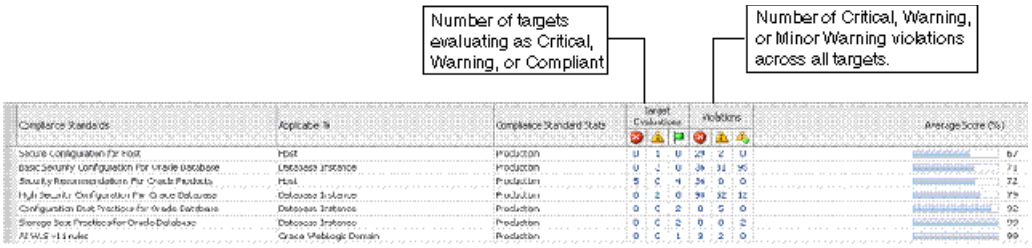
1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Select the Compliance Standard and click the **Associate** button.
3. Choose the target to add and click **OK**.

1.3 Viewing and Understanding Compliance Results

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

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



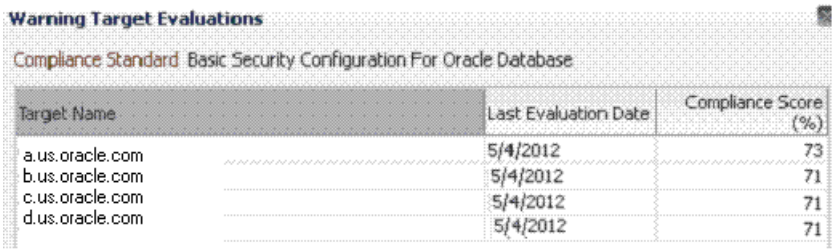
Column descriptions follow.

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. Figure 1–3.

Figure 1–3 Warning Target Evaluations Details



Violations

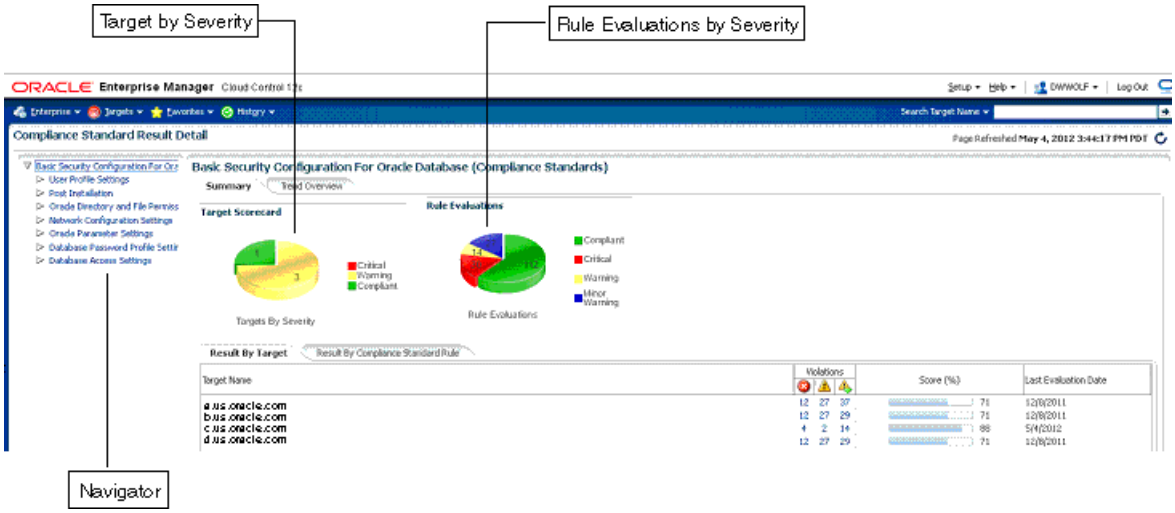
The Violations columns show the number of unique violations by compliance rule severity (Critical, Warning, or Minor Warning) across all evaluated targets. It is important to remember that the number of violations is not related to the number of compliance rules in the compliance standard. Each compliance 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. Figure 1–4.

Figure 1–4 Critical Compliance Violations

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

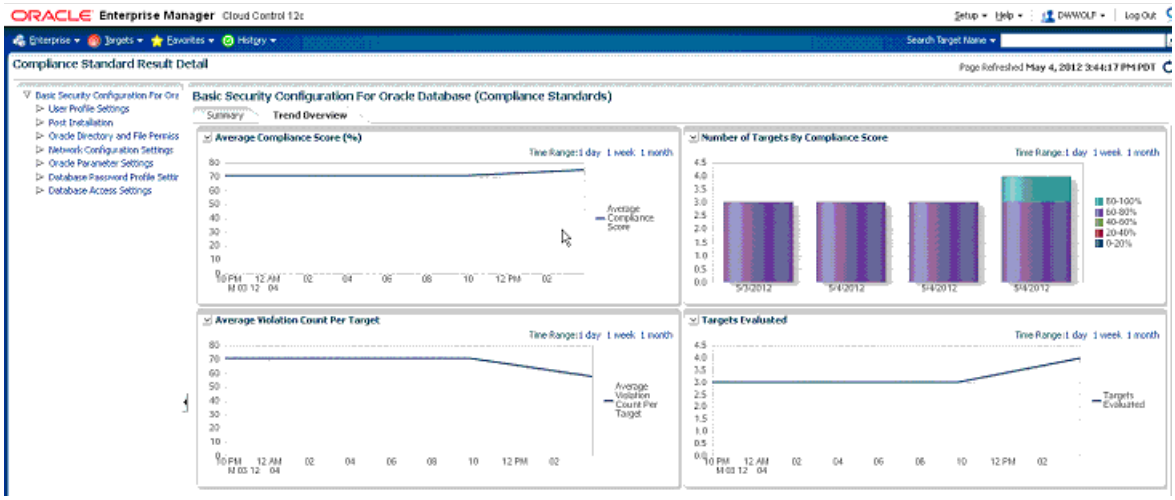
Figure 1–5 Compliance Standard Result Details - Summary



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 Target by Severity and Rule Evaluation results by severity.

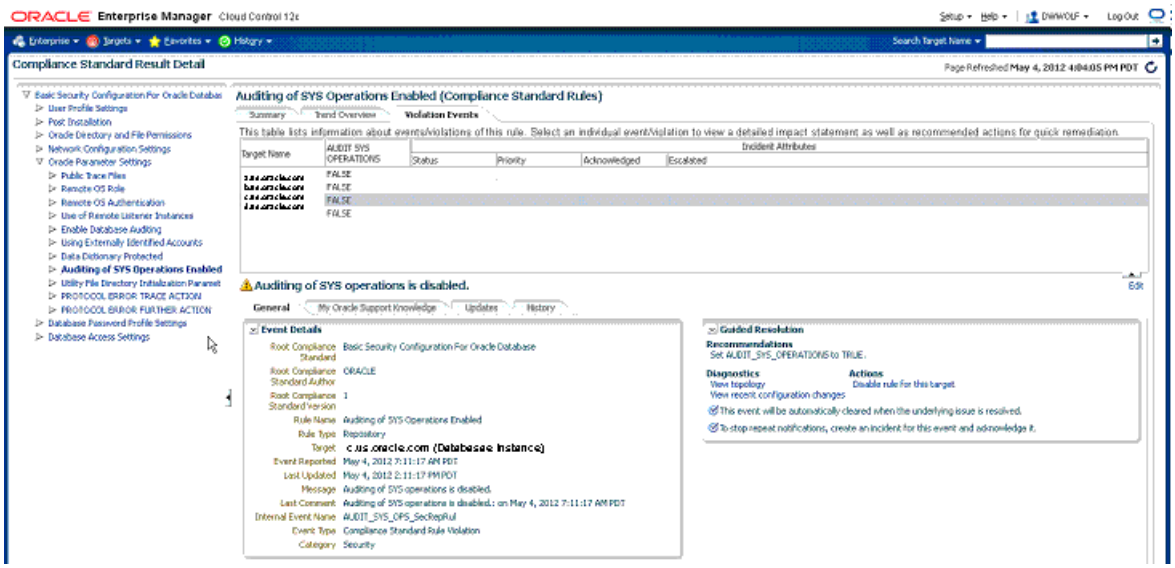
Clicking the **Trend Overview** tab shows the historical compliance metrics which can each be changed to show date ranges of 1 day, 1 week, or 1 month.

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 users 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.

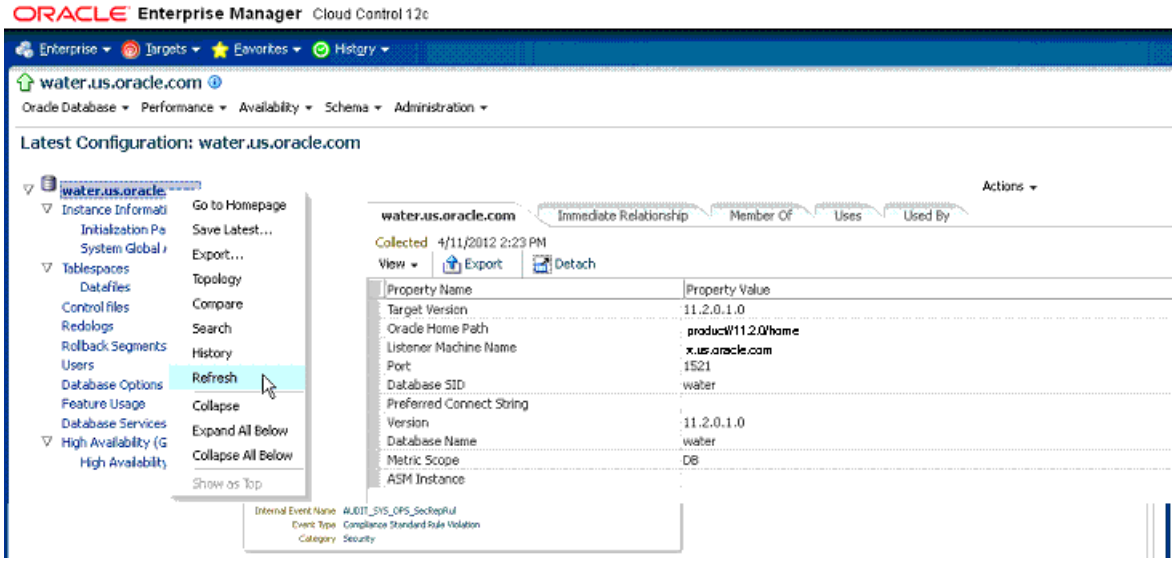
From this point the user has many options to investigate the violation further or resolve the issue including:

- 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 users want to force a collection sooner, they can select refresh from the targets Last Collected configuration page as shown in Figure 1–8.

Figure 1–8 Manual Configuration Refresh



1.4 Summary

Enterprise Manager 12*c* makes it easy for users to validate their databases against Oracle recommendations, best practices and security standards by providing ready to use Compliance Standards. DBAs and IT managers can easily track, manage, and report on the adherence of their managed databases to these standards in an automated and consistent manor.

2

Oracle Single Instance Database Compliance Standards

These are the compliance rules for the Oracle Single Instance Database compliance standards. The compliance standards are:

- Basic Security Configuration for Oracle Database
- Configuration Best Practices for Oracle Database
- High Security Configuration for Oracle Database
- Patchable Configuration for Oracle Database
- Storage Best Practices for Oracle Database

2.1 Basic Security Configuration for Oracle Database

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

2.1.1 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.

2.1.2 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.

2.1.3 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.

2.1.4 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.

2.1.5 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.

2.1.6 Remote OS Authentication

Description: Ensures 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.

2.1.7 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.

2.1.8 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.

2.1.9 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.

2.1.10 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.

2.1.11 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.

2.1.12 Enable Database Auditing

Description: Ensures database auditing is enabled.

Severity: Minor Warning

Rationale: The AUDIT_TRAIL parameter enables or disables database auditing. 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.

2.1.13 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.

2.1.14 Default Passwords

Description: Ensures there are no default passwords for known accounts.

Severity: Warning

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

2.1.15 Server Parameter File Permission

Description: Ensures that access to the server parameter 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.

2.1.16 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.

2.1.17 Initialization Parameter File Permission (Windows)

Description: Ensures that access to the initialization parameter 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.

2.1.18 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.

2.1.19 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.

2.1.20 Oracle Net Server Trace Directory Permission (Windows)

Description: Ensures that the serv.er 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.

2.1.21 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.

2.1.22 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.

2.1.23 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.

2.1.24 Password Life Time

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.

2.1.25 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.

2.1.26 Restricted Privilege to Execute UTL_TCP

Description: Ensures 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.

2.1.27 IDLE TIME

Description: Ensures that users profile settings IDLE_TIME have appropriate value set for the particular database and application.

Severity: Critical

Rationale: Idle 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. Limit the maximum number of minutes a session can idle.

2.1.28 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.

2.1.29 Server Parameter File Permission (Windows)

Description: Ensures that access to the server parameter 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.

2.1.30 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.

2.1.31 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.

2.1.32 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 user name with user names 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.

2.1.33 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 by a malicious user.

2.1.34 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.

2.1.35 Restricted Privilege to Execute UTL_SMTP

Description: Ensures 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.

2.1.36 Initialization Parameter File Permission

Description: Ensures that access to the initialization parameter 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.

2.1.37 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.

2.1.38 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.

2.1.39 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.

2.1.40 Access to SYS.USER_HISTORY$ Table

Description: Ensures restricted access to SYS.USER_HISTORY$ table.

Severity: Minor Warning

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

2.1.41 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.

2.1.42 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.

2.1.43 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.

2.1.44 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.

2.1.45 Access to SYS.USER$ Table

Description: Ensures restricted access to SYS.USER$ table.

Severity: Minor Warning

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

2.1.46 Use of Appropriate Umask on UNIX systems

Description: On UNIX systems, ensures 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.

2.1.47 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.

2.1.48 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.

2.1.49 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.

2.1.50 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.

2.1.51 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.

2.1.52 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.

2.1.53 Access to SYS.AUD$Table

Description: Ensures restricted access to SYS.AUD$ table.

Severity: Minor Warning

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

2.1.54 Restricted Privilege to Execute UTL_HTTP

Description: Ensures 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.

2.1.55 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.

2.1.56 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.

2.1.57 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.

2.1.58 Remote OS Role

Description: Ensures 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.

2.1.59 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.

2.1.60 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.

2.1.61 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.

2.1.62 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.

2.1.63 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.

2.2 Configuration Best Practices for Oracle Database

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

2.2.1 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.

2.2.2 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).

2.2.3 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.

2.2.4 Fast Recovery Area Not Set

Description: Checks whether recovery area is set.

Severity: Warning

Rationale: NO_RECOVERY_AREA_IMPACT

2.2.5 Statistics Level 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.

2.2.6 Not Using SP File

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 across database 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 a shutdown and restart.

2.2.7 Statistics Level Set to BASIC

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.

2.2.8 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.

2.2.9 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 you lose the only copy of the control file due to a media error, there will be unnecessary down time and other risks.

2.2.10 Use of Non-Standard Initialization Params

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.

2.3 High Security Configuration for Oracle Database

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

2.3.1 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.

2.3.2 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.

2.3.3 Execute Privileges on UTL_FILE To PUBLIC

Description: Ensures 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.

2.3.4 Access to %_CATALOG% Roles

Description: Ensures 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 the database system.

2.3.5 $ORACLE_HOME/network/admin Directory 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.

2.3.6 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.

2.3.7 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 user name and password that can be used access sensitive data or to launch further attacks.

2.3.8 Log Archive Duplex Destination

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.

2.3.9 Oracle Agent SNMP Real-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 services it 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, and so on.

2.3.10 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.

2.3.11 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.

2.3.12 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.

2.3.13 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.

2.3.14 Audit EXECUTE 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.

2.3.15 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.

2.3.16 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.

2.3.17 Access to V$ Synonyms Roles

Description: Ensures SELECT privilege is not granted to 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 when possible.

2.3.18 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.

2.3.19 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.

2.3.20 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.

2.3.21 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 user name and password that can be used access sensitive data or to launch further attacks.

2.3.22 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.

2.3.23 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.

2.3.24 Oracle HTTP Server mod_plsql 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 services.

2.3.25 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.

2.3.26 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 sessions for each individual user.

2.3.27 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.

2.3.28 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.

2.3.29 "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.

2.3.30 Restrict Permissions of the tkprof Executable to the Owner of the Oracle Software Set and the DBA Group

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.

2.3.31 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.

2.3.32 Execute Privilege on SYS.DBMS_RANDOM PUBLIC

Description: Ensures 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 user will be able to take advantage.

2.3.33 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, and so on.

2.3.34 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, and so on.

2.3.35 Use of SQL 92 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.

2.3.36 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.

2.3.37 DB SECUREFILE

Description: Ensures 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.

2.3.38 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.

2.3.39 PRIVATE SGA

Description: Ensures 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.

2.3.40 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.

2.3.41 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.

2.3.42 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.

2.3.43 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.

2.3.44 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.

2.3.45 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 security issues.

2.3.46 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.

2.3.47 Access to SYS.LINK$ Table

Description: Ensures restricted access to SYS.LINK$ table.

Severity: Minor Warning

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

2.3.48 Access to X_$Views

Description: Ensures access on X$ views is restricted.

Severity: Critical

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

2.3.49 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, and so on.

2.3.50 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_ARCHIEVE_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.

2.3.51 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.

2.3.52 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.

2.3.53 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.

2.3.54 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.

2.3.55 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.

2.3.56 Execute Privilege on SYS.DBMS_EXPORT_EXTENSION to PUBLIC

Description: Ensures 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 user will be able to take advantage.

2.3.57 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.

2.3.58 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.

2.3.59 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 services it 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, and so on.

2.3.60 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.

2.3.61 $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.

2.3.62 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.

2.3.63 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.

2.3.64 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.

2.3.65 System Privileges to Public

Description: Ensures 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.

2.3.66 Utility File Directory Initialization Parameter Setting in Oracle 9i Release 1 and Later

Description: Ensures that the UTL_FILE_DIR initialization parameter is not used in Oracle9*i* 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.

2.3.67 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.

2.3.68 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.

2.3.69 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 user name and password that can be used access sensitive data or to launch further attacks.

2.3.70 OS ROLES

Description: Ensures 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, can cause serious security issues.

2.3.71 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.

2.3.72 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.

2.3.73 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.

2.3.74 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.

2.3.75 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.

2.3.76 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.

2.3.77 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.

2.3.78 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.

2.3.79 $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.

2.3.80 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, and so on.

2.3.81 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.

2.3.82 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.

2.3.83 LOGICAL READS PER SESSION

Description: Ensures 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.

2.3.84 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.

2.3.85 Audit CREATE SYSSION 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.

2.3.86 Limit OS Authentication

Description: Ensures database accounts do not rely on OS authentication.

Severity: Critical

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

2.3.87 Otrace Data File

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.

2.3.88 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.

2.3.89 SQL*Plus Executable Owner

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

Severity: Warning

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

2.3.90 Oracle HTTP Server Distributed Configuration File 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.

2.3.91 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.

2.3.92 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.

2.3.93 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.

2.3.94 CONNECT TIME

Description: Ensures 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.

2.3.95 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.

2.3.96 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.

2.4 Patchable Configuration for Oracle Database

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

2.4.1 Patchability

Description: Ensures the Oracle Database target has a patchable configuration

Severity: Warning

Rationale: Unpatchable Oracle Database target could not be patched by using the provided Enterprise Manager Patching feature.

2.5 Storage Best Practices for Oracle Database

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

2.5.1 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.

2.5.2 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.

2.5.3 Non-Uniform Defaults 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 in size leading to fragmentation, inefficient space usage and performance degradation.

2.5.4 Segment with Extent Growth Policy Violation

Description: Checks for segments in dictionary managed or migrated locally managed tablespaces having irregular extent sizes and/or non-zero Percent Increase settings.

Severity: Minor Warning

Rationale: These segments have extents with sizes that are not multiples of the initial extent or have a non-zero Percent Increase setting. This can result in inefficient reuse of space and fragmentation problems.

2.5.5 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 be consumed, thus causing the database to stop working.

2.5.6 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.

2.5.7 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.

2.5.8 Tablespace 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.

2.5.9 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.

2.5.10 Non-System Data Segments in System Tablespaces

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

Severity: Minor Warning

Rationale: These segments belonging to non-system users are stored in system tablespaces SYSTEM or SYSAUX. 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.

2.5.11 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.

2.5.12 Database Rollback Segment 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.

2.5.13 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.

3

Oracle Real Application Cluster Database Compliance Standards

These are the compliance rules for the Oracle Application Cluster Database compliance standards. The compliance standards are:

- Basic Security Configuration for Oracle Cluster Database
- Configuration Best Practices for Oracle Real Application Cluster Database
- High Security Configuration for Oracle Cluster Database
- Patchable Configuration for Real Application Cluster Database
- Storage Best Practices for Oracle Real Application Database
- Basic Security Configuration for Oracle Cluster Database Instance
- High Security Configuration for Oracle Cluster Database Instance

3.1 Basic Security Configuration for Oracle Cluster Database

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

3.1.1 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.

3.1.2 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.

3.1.3 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.

3.1.4 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.

3.1.5 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.

3.1.6 Remote OS Authentication

Description: Ensures 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.

3.1.7 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.

3.1.8 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.

3.1.9 Access to SYS.USER_HISTORY$ Table

Description: Ensures restricted access to SYS.USER_HISTORY$ table.

Severity: Minor Warning

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

3.1.10 Access to SYS.USER$ Table

Description: Ensures restricted access to SYS.USER$ table.

Severity: Minor Warning

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

3.1.11 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.

3.1.12 Restricted Privilege to Execute UTL_HTTP

Description: Ensures 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.

3.1.13 IDLE TIME

Description: Ensures that users profile settings IDLE_TIME have appropriate value set for the particular database and application.

Severity: Critical

Rationale: Idle 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. Limit the maximum number of minutes a session can idle.

3.1.14 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.

3.1.15 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.

3.1.16 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.

3.1.17 Enable Database Auditing

Description: Ensures database auditing is enabled.

Severity: Minor Warning

Rationale: The AUDIT_TRAIL parameter enables or disables database auditing. 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.

3.1.18 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.

3.1.19 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.

3.1.20 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.

3.1.21 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.

3.1.22 Server Parameter File Permission

Description: Ensures that access to the server parameter 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.

3.1.23 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.

3.1.24 Initialization Parameter File Permission (Windows)

Description: Ensures that access to the initialization parameter 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.

3.1.25 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.

3.1.26 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.

3.1.27 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.

3.1.28 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.

3.1.29 Password Life Time

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.

3.1.30 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.

3.1.31 Server Parameter File Permission (Windows)

Description: Ensures that access to the server parameter 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.

3.1.32 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.

3.1.33 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 user name with user names 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.

3.1.34 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.

3.1.35 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.

3.1.36 Initialization Parameter File Permission

Description: Ensures that access to the initialization parameter 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.

3.1.37 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.

3.1.38 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.

3.1.39 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.

3.1.40 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.

3.1.41 Access to STATS$SQL_SUMMARY Table

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.

3.1.42 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.

3.1.43 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.

3.1.44 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.

3.1.45 Access to SYS.AUD$ Table

Description: Ensures restricted access to SYS.AUD$ table.

Severity: Minor Warning

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

3.1.46 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.

3.1.47 Use of Appropriate Umask on UNIX systems

Description: On UNIX systems, ensures 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.

3.1.48 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.

3.1.49 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.

3.1.50 Default Passwords

Description: Ensures there are no default passwords for known accounts.

Severity: Warning

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

3.1.51 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.

3.1.52 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 by a malicious user.

3.1.53 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.

3.1.54 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.

3.1.55 Restricted Privilege to Execute UTL_TCP

Description: Ensures 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.

3.1.56 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.

3.1.57 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.

3.1.58 Remote OS Role

Description: Ensures 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.

3.1.59 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.

3.1.60 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 Real Application Cluster environment where this setting provides a load balancing mechanism for the listener.

3.1.61 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.

3.1.62 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.

3.1.63 Restricted Privilege to Execute UTL_SMTP

Description: Ensures 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.

3.2 Configuration Best Practices for Oracle Real Application Cluster Database

The compliance standard rules for the Configuration Best Practices for Oracle Real Application Cluster Database compliance standard follow.

3.2.1 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 you lose the only copy of the control file due to a media error, there will be unnecessary down time and other risks.

3.2.2 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.

3.2.3 Fast Recovery Area Not Set

Description: Checks whether recovery area is set.

Severity: Warning

Rationale: NO_RECOVERY_AREA_IMPACT

Using a fast recovery area minimizes the need to manually manage disk space for your backup-related files and balance the use of space among the different types of files. Oracle recommends that you enable a fast recovery area to simplify your backup management.

3.3 High Security Configuration for Oracle Cluster Database

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

3.3.1 $ORACLE_HOME/network/admin Directory 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.

3.3.2 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.

3.3.3 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 user name and password that can be used access sensitive data or to launch further attacks.

3.3.4 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.

3.3.5 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 services it 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, and so on.

3.3.6 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.

3.3.7 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.

3.3.8 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.

3.3.9 Execute Privileges on UTL_FILE To PUBLIC

Description: Ensures 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.

3.3.10 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.

3.3.11 Audit EXECUTE 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.

3.3.12 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.

3.3.13 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.

3.3.14 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.

3.3.15 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.

3.3.16 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 user name and password that can be used to access sensitive data or to launch further attacks.

3.3.17 Webcache Initialization File Permissions

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.

3.3.18 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.

3.3.19 Oracle HTTP Server mod_plsql 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 services it 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, and so on.

3.3.20 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.

3.3.21 Restrict Permissions of the tkprof Executable to the Owner of the Oracle Software Set and the DBA Group

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 leaks.

3.3.22 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 sessions for each individual user.

3.3.23 Audit DROP ANY ROLE Privilege

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

Severity: Critical

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

3.3.24 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.

3.3.25 "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.

3.3.26 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, and so on.

3.3.27 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, and so on.

3.3.28 Use of SQL92 Security Features

Description: Ensures use of SQL92 security.

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.

3.3.29 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.

3.3.30 DB SECUREFILE

Description: Ensures 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.

3.3.31 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.

3.3.32 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.

3.3.33 Execute Privilege on SYS.DBMS_EXPORT_EXTENSION to PUBLIC

Description: Ensures 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 user will be able to take advantage.

3.3.34 Access to %_CATALOG% Roles

Description: Ensures 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 the database system.

3.3.35 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.

3.3.36 PRIVATE SGA

Description: Ensures 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.

3.3.37 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.

3.3.38 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.

3.3.39 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.

3.3.40 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.

3.3.41 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.

3.3.42 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 security issues.

3.3.43 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, and so on.

3.3.44 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_ARCHIEVE_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.

3.3.45 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.

3.3.46 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.

3.3.47 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.

3.3.48 System Privileges to Public

Description: Ensures 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.

3.3.49 Access to V$ Synonyms Roles

Description: Ensures SELECT privilege is not granted to 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 when possible.

3.3.50 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.

3.3.51 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.

3.3.52 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.

3.3.53 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.

3.3.54 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.

3.3.55 Oracle Agent SNMP Read-Only Configuration File Permission

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

Severity: Warning

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

3.3.56 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.

3.3.57 $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.

3.3.58 Access to X_$Views

Description: Ensures access on X$ views is restricted.

Severity: Critical

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

3.3.59 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.

3.3.60 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.

3.3.61 Execute Privilege on SYS.DBMS_RANDOM PUBLIC

Description: Ensures 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.

3.3.62 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.

3.3.63 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.

3.3.64 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.

3.3.65 Utility File Directory Initialization Parameter Setting in Oracle 9i Release 1 and Later

Description: Ensures that the UTL_FILE_DIR initialization parameter is not used in Oracle9*i* 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.

3.3.66 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.

3.3.67 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.

3.3.68 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 user name and password that can be used access sensitive data or to launch further attacks.

3.3.69 OS ROLES

Description: Ensures 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, can cause serious security issues.

3.3.70 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.

3.3.71 Access to SYS.LINK$ Table

Description: Ensures restricted access to SYS.LINK$ table.

Severity: Minor Warning

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

3.3.72 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.

3.3.73 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.

3.3.74 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.

3.3.75 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.

3.3.76 $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.

3.3.77 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, and so on.

3.3.78 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-only configuration file can be used to extract sensitive data like the tracing directory location, dbsnmp address, and so on.

3.3.79 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.

3.3.80 Otrace Data File

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.

3.3.81 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.

3.3.82 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.

3.3.83 LOGICAL READS PER SESSION

Description: Ensures 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.

3.3.84 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.

3.3.85 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.

3.3.86 Limit OS Authentication

Description: Ensures database accounts do not rely on OS authentication.

Severity: Critical

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

3.3.87 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.

3.3.88 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.

3.3.89 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.

3.3.90 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.

3.3.91 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.

3.3.92 Secure OS Audit Level

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

Severity: Warning

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

3.3.93 CONNECT TIME

Description: Ensures 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.

3.3.94 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.

3.3.95 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.

3.4 Patchable Configuration for Real Application Cluster Database

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

3.4.1 Patchability

Description: Ensures the Real Application Cluster Database target has a patchable configuration.

Severity: Warning

Rationale: Unpatchable Real Application Cluster Database target could not be patched by using the provided Enterprise Manager Patching feature.

3.5 Storage Best Practices for Oracle Real Application Database

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

3.5.1 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.

3.5.2 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 in size leading to fragmentation, inefficient space usage and performance degradation.

3.5.3 Database Rollback Segment 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.

3.5.4 Non-System Data Segments in System Tablespaces

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

Severity: Minor Warning

Rationale: These segments belonging to non-system users are stored in system tablespaces SYSTEM or SYSAUX. 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.

3.5.5 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.

3.5.6 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.

3.5.7 Tablespace 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.

3.5.8 Segment with Extent Growth Policy Violation

Description: Checks for segments in dictionary managed or migrated locally managed tablespaces having irregular extent sizes and/or non-zero Percent Increase settings.

Severity: Minor Warning

Rationale: These segments have extents with sizes that are not multiples of the initial extent or have a non-zero Percent Increase setting. This can result in inefficient reuse of space and fragmentation problems.

3.5.9 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 be consumed, thus causing the database to stop working.

3.5.10 Tablespace Not Using Automatic Segment-Space Management

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

Severity: Minor Warning

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

3.5.11 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.

3.5.12 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.

3.5.13 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.

3.6 Basic Security Configuration for Oracle Cluster Database Instance

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

3.6.1 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.

3.6.2 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.

3.6.3 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.

3.6.4 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.

3.6.5 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.

3.6.6 Remote OS Authentication

Description: Ensures 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.

3.6.7 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.

3.6.8 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.

3.6.9 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.

3.6.10 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.

3.6.11 Enable Database Auditing

Description: Ensures database auditing is enabled.

Severity: Minor Warning

Rationale: The AUDIT_TRAIL parameter enables or disables database auditing. 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.

3.6.12 Server Parameter File Permission

Description: Ensures that access to the server parameter 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.

3.6.13 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.

3.6.14 Initialization Parameter File Permission (Windows)

Description: Ensures that access to the initialization parameter 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.

3.6.15 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.

3.6.16 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.

3.6.17 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.

3.6.18 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.

3.6.19 Server Parameter File Permission (Windows)

Description: Ensures that access to the server parameter 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.

3.6.20 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.

3.6.21 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 user name with user names 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.

3.6.22 Initialization Parameter File Permission

Description: Ensures that access to the initialization parameter 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.

3.6.23 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.

3.6.24 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.

3.6.25 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

3.6.26 Access to STATS$SQL_SUMMARY Table

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.

3.6.27 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.

3.6.28 Use of Appropriate Umask on UNIX Systems

Description: On UNIX systems, ensures 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.

3.6.29 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.

3.6.30 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.

3.6.31 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.

3.6.32 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.

3.6.33 Remote OS Role

Description: Ensures 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.

3.6.34 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.

3.6.35 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 Real Application Cluster environment where this setting provides a load balancing mechanism for the listener.

3.7 High Security Configuration for Oracle Cluster Database Instance

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

3.7.1 $ORACLE_HOME/network/admin Directory 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.

3.7.2 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.

3.7.3 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 user name and password that can be used access sensitive data or to launch further attacks.

3.7.4 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.

3.7.5 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 services it 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, and so on.

3.7.6 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.

3.7.7 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.

3.7.8 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.

3.7.9 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.

3.7.10 Log Archive Destination Owner

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

Severity: Critical

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

3.7.11 Log Archive Destination Permission

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

Severity: Critical

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

3.7.12 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 user name and password that can be used to access sensitive data or to launch further attacks.

3.7.13 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.

3.7.14 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.

3.7.15 Oracle HTTP Server mod_plsql 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 services it 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, and so on.

3.7.16 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.

3.7.17 Restrict Permissions of the tkprof Executable to the Owner of the Oracle Software Set and the DBA Group

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 leaks.

3.7.18 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, and so on.

3.7.19 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, and so on.

3.7.20 Use of SQL 92 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.

3.7.21 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.

3.7.22 DB SECUREFILE

Description: Ensures 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.

3.7.23 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.

3.7.24 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, and so on.

3.7.25 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 the database is in archivelog mode.

Severity: Critical

Rationale: Setting the LOG_ARCHIEVE_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.

3.7.26 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.

3.7.27 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.

3.7.28 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.

3.7.29 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.

3.7.30 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 services it 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, and so on.

3.7.31 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.

3.7.32 $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.

3.7.33 Utility File Directory Initialization Parameter Setting in Oracle 9i Release 1 and Later

Description: Ensures that the UTL_FILE_DIR initialization parameter is not used in Oracle9*i* 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.

3.7.34 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.

3.7.35 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.

3.7.36 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 user name and password that can be used access sensitive data or to launch further attacks.

3.7.37 OS ROLES

Description: Ensures 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, can cause serious security issues.

3.7.38 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.

3.7.39 $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.

3.7.40 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, and so on.

3.7.41 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 users 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, and so on.

3.7.42 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.

3.7.43 Otrace Data File

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.

3.7.44 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.

3.7.45 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.

3.7.46 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.

3.7.47 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.

3.7.48 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.

3.7.49 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.

4

Automatic Storage Management Compliance Standards

These are the compliance rules for the Automatic Storage Management (ASM) compliance standards. The compliance standards are:

- Storage Best Practices for ASM
- Patchable Configuration for ASM

4.1 Storage Best Practices for ASM

The compliance rules for the Storage Best Practices for ASM compliance standard follow.

4.1.1 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.

4.1.2 Disk Group Depends on External Redundancy and Has Unprotected Disks

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

Severity: Warning

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

4.1.3 Disk Group Contains Disks with Different Redundancy Attributes

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

Severity: Warning

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

4.1.4 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.

4.2 Patchable Configuration for ASM

The compliance rule for the Patchable Configuration for ASM compliance standard follows.

4.2.1 Patchability

Description: Ensures the ASM target has a patchable configuration.

Severity: Warning

Rationale: Unpatchable ASM target could not be patched by using the provided Enterprise Manager Patching feature.

5

Oracle Listener Compliance Standards

These are the compliance rules for the Oracle Listener compliance standards. The compliance standards are:

- Basic Security Configuration for Oracle Listener
- High Security Configuration for Oracle Listener

5.1 Basic Security Configuration for Oracle Listener

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

5.1.1 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 it to public scrutiny with possible security implications

5.1.2 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.

5.1.3 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.

5.1.4 Listener Logfile Permission

Description: Ensures that the listener log file cannot be read by or written to by public.

Severity: Critical

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

5.1.5 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.

5.1.6 Listener Logfile Permission (Windows)

Description: Ensures that the listener log file cannot be read by or written to by public.

Severity: Critical

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

5.2 High Security Configuration for Oracle Listener

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

5.2.1 Oracle Net Tcp Valid Node 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 server, including a malicious user.

5.2.2 Listener Logging Status

Description: Ensures that listener logging is enabled.

Severity: Warning

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

5.2.3 Use of Host Name in Listener.ora

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

5.2.4 Secure Remote Listener Administration

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

Severity: Warning

Rationale: Limiting the transports for remote administration to TCPS and IPC reduces the risk of unauthorized access.

5.2.5 Listener Direct Administration

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

Severity: Critical

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

5.2.6 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.

5.2.7 Listener Logfile Owner

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

Severity: Critical

Rationale: The information in the log file 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.

5.2.8 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.

5.2.9 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.

5.2.10 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.

5.2.11 Listener Trace File Owner

Description: Ensures that the listener trace file owner is the 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.

5.2.12 tcp.excluded_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 server, including a malicious user.

5.2.13 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.

5.2.14 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.

5.2.15 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.

5.2.16 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.

5.2.17 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.

5.2.18 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 server, including a malicious user.

5.2.19 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.

5.2.20 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.