(2.24) 101366 Ensure secure encryption standards are configured(oracle19:1:1621:POHK1RCT.hk.standardchartered.com) **Passed** **MEDIUM**

Instance	oracle19:1:1621:POHK1RCT.hk.standardchartered.com
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:09:56 PM (GMT+0530)

Ensure secure encryption standards are configured

Ensure secure encryption standards are configured

Scan Parameters:

DBQUERY: select network_service_banner from v$session_connect_info where sid=(select sid from v$mystat where rownum = 1) and network_service_banner like '%AES256%'

Expected **contains regular expression list**

DB Column Name: NETWORK_SERVICE_BANNER

AES256

OR, any of the selected values below:

Set status to PASS if no data found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

NETWORK_SERVICE_BANNER
AES256 Encryption service adapter for Linux: Version 19.0.1.0.0 - Production

Extended Evidence:

Statistics:

Query returned 1 rows

10.21.199.150 (hklpdss2b002.hk.standardchartered.com) - cpe:/o:redhat:enterprise_linux:7.9::server:

Controls:	98
Passed:	87 (88.78%)
Failed:	11 (11.22%)
Error:	0
Approved Exceptions:	0
Pending Exceptions:	0
Last Scan Date:	08/04/2024 at 06:01:09 PM (GMT+0530)
Tracking Method:	IP
Qualys Host ID:	-

Asset Tags:
ALL ASSET GROUPS, Vulnerability Management, Engineering Build, Internal Asset, CLOUD POC, SUBNET-HONG KONG, Oracle PC - AG, Policy Compliance - OS SAT/CCM, ICV-Scan-OS- HK1, Production Support, AG_SelfService, SVLM, Metrics Internal Facing IPs, ESC ATM, Test CCM Scan Key update - UNIX, ZINT-SERVER-INVENTORY-ALL, ALL_STATUS_HONG_KONG_PROD, 2021 Q1 Validation Internal, ICV-OS-Red Hat Enterprise Linux, RBI DB Cindy 2021, SGF total IP scanned of the month, MAP_HK 2/3, temp-all-server2, 2021 Q4 Validation Internal, Dec_2021_CDC_GDC_NC_Scanned, Jan_2022_CDC_GDC_NC_Scanned, Feb_2022_CDC_GDC_NC_Scanned, 2022 Q1 Validation Internal, Total IP scanned for the month of Feb 2022, Mar_2022_CDC_GDC_NC_Scanned, SGF IP not scanned of the month, Apr_2022_CDC_GDC_NC_Scanned, May_2022_GDC_CDC_NC_scanned, 2022 Q2 Validation Internal, Jun_2022_GDC_CDC_NC_scanned, Jul_2022_GDC_CDC_NC_scanned, 2022 Q3 Validation Internal, Aug_2022_GDC_CDC_NC_scanned, Sep_2022_GDC_CDC_NC_scanned, OpenSSL-Asia-Prod, Nov_2022_GDC_CDC_NC_scanned, 2022 Q4 Validation Internal, Purge Activity, Jan_2023_CDC_GDC_NC_Scanned, Feb_2023_CDC_GDC_NC_Scanned, Self_Service_AG_UM, 2023 Q1 Validation Internal, Mar_2023_CDC_GDC_NC_Scanned, Apr_2023_CDC_GDC_NC_Scanned, AG-ICV Scans-OS_Web [HK - Begins with 10.21.1], Database_Group, May_2023_CDC_GDC_NC_Scanned, 2023 Q2 Validation Internal, Jun_2023_CDC_GDC_NC_Scanned, Sep_2023_CDC_GDC_NC_Scanned, Oct_2023_CDC_GDC_NC_Scanned, 2023 Q4 Validation Internal, Nov_2023_CDC_GDC_NC_Scanned, JAN_2024_GDC_EAST, Jan_2024_CDC_GDC_NC_Scanned, FEB_2024_GDC_EAST, Feb_2024_CDC_GDC_NC_Scanned, MAR_2024_GDC_EAST, 2024 Q1 Validation Internal, Mar_2024_CDC_GDC_NC_Scanned, APR_2024_GDC_EAST, April_2024_CDC_GDC_NC_Scanned, MAY_2024_GDC_EAST, May_2024_CDC_GDC_NC_Scanned, 2024 Q2 Validation Internal, JUN_2024_GDC_EAST, Jun_2024_CDC_GDC_NC_Scanned, JUL_2024_GDC_EAST, July_2024_CDC_GDC_NC_Scanned

Oracle 19c

1. Database Controls

(1.1) 1049 Status of the 'remote_os_authent(remote OS authentication without password)' setting via SQL query(oracle19:1:1621:POHK1API_DG2) **Passed** **HIGH**

Instance oracle19:1:1621:POHK1API_DG2

Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

The 'REMOTE_OS_AUTHENT=TRUE' setting in the 'init.ora' file allows a connection to be made to the database instance as a specific user via OS-based, rather than database-local authentication. Oracle allows this connection, assuming the user was authenticated by the remote OS. This capability could allow a malicious user to impersonate another when OS credentials have been compromised. When this is set to FALSE (as recommended by the manufacturer), remote user connections will not be allowed without database-local credentials.

The String value X indicates the current state of the remote_os_authent setting in init.ora (remote OS authentication without password). Prohibiting such connections require the value to be FALSE.

Expected	**regular expression match**
	FALSE
	OR, any of the selected values below:
	Parameter: REMOTE_OS_AUTHENT not found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	FALSE

Extended Evidence:

NAME	VALUE
remote_os_authent	FALSE
remote_os_authent	FALSE
remote_os_authent	FALSE

(1.2) 1050 Status of the 'remote_os_roles' setting via SQL query(oracle19:1:1621:POHK1API_DG2) Passed HIGH

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

The 'remote_os_roles= *' setting is used to grant or revoke the right to have OS-based roles or privileges given to the user, based upon grants made to that user within the database. The manufacturer recommends that this be set to FALSE (the default) to prevent possible network-connection spoofing or user impersonation, which could lead to data compromise or damage to the database.

The String value X indicates the current status of the operating system role and whether connections are permitted for remote clients. To show that such connections are not permitted, the value should be FALSE.

Expected	**regular expression match**
	FALSE
	OR, any of the selected values below:
	Parameter: REMOTE_OS_ROLES not found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	FALSE

Extended Evidence:

NAME	VALUE
remote_os_roles	FALSE
remote_os_roles	FALSE
remote_os_roles	FALSE

(1.3) 1057 Status of the 'sql92_security=' (table-level SELECT privileges) in init.ora (oracle19:1:1621:POHK1API_DG2) Passed HIGH

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

The 'SQL92_SECURITY' parameter specifies that users can be required to have the 'SELECT' privilege on a table when performing UPDATE/DELETE operations on that table, if any column value(s) involve a 'SET' or 'WHERE' clause invocation. Having 'SQL92_SECURITY=TRUE' indicates that users must have been granted the 'SELECT object' privilege (for successfully completing a query) in order to execute any UPDATE or DELETE statements on that column value, reducing the potential

risk of unauthorized data alteration. NOTE: Implementing this is not without risk, for large jobs with complex settings can fail due to lack of a SELECT object capability by one user.

This String value X indicates whether or not the SELECT privilege must be granted in order to execute UPDATE or DELETE operations. The value should be TRUE if this has been set.

Expected	**regular expression match**
	TRUE
	OR, any of the selected values below:
	Parameter: SQL92_SECURITY not found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	TRUE

Extended Evidence:

NAME	VALUE
sql92_security	TRUE
sql92_security	TRUE
sql92_security	TRUE

(1.4) 1067 Status of the 'REMOTE_LOGIN_PASSWORD' setting via SQL query(oracle19:1:1621: POHK1API_DG2) Passed HIGH

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

The 'remote_login_password file=' parameter permits the creation of a password file that can be set to allow a remote user to connect to the database as 'sysdba' via this type of authentication. If compromised, this will allow unauthorized access to the system as one of the most powerful user levels, 'sysdba,' from a remote location and should be used with extreme caution. Setting this parameter value to NONE will disable the functionality.

This String value X indicates whether or not permission for remote login through the password file is active. The value should be NONE if this setting is disabled.

Expected	**regular expression match**
	EXCLUSIVE|NONE
	OR, any of the selected values below:
	Parameter: REMOTE_LOGIN_PASSWORD not found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	EXCLUSIVE

Extended Evidence:

NAME	VALUE
remote_login_passwordfile	EXCLUSIVE
remote_login_passwordfile	EXCLUSIVE
remote_login_passwordfile	EXCLUSIVE

(1.5) 3462 Permissions set for the 'ORACLE_HOME/bin' directory(oracle19:1:1621: POHK1API_DG2) Passed HIGH

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

The 'ORACLE_HOME\bin' directory contains the binary files related to the Oracle database instance. The binary files contained in the 'ORACLE_HOME/bin' folder are critical, system wide files required for the proper operation of the database. As these binary files are critical to the integrity and availability of the database, the permissions set for the 'ORACLE_HOME/bin' directory should be restricted as appropriate to the needs of the business.

The following List String value(s) X provides an inventory of the files and the permissions set for them in the ORACLE_HOME/bin directory. Output is returned in the form owner:group:directory permissions.

Expected	**matches regular expression list**
	.*(\-\-\-|\-\-x|\-w\-|\-wx|r\-\-|r\-x|rw\-|rwx)(\-\-\-|\-\-x|r\-\-|r\-x)(\-\-\-|\-\-x|r\-\-|r\-x).*

	OR, any of the selected values below:
	File not found
Actual	**Last Updated:04/21/2024 at 06:00:55 PM (GMT+0530)**
	root:root:r-xr-xr-x.:/bin

(1.6) 3463 Permissions set for the 'ORACLE_HOME' directory(oracle19:1:1621:POHK1API_DG2) **Failed** **HIGH**

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Failed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

Oracle database application software is installed in the operating system directory designated by the 'ORACLE_HOME' environment variable. As the 'ORACLE_HOME' directory contains critical database application files, permissions set for the directory should be restricted as appropriate to the needs of the business.

The following List String value(s) X indicate the current permissions set for the ORACLE_HOME directory. Output is returned in the form owner:group:directory permissions.

Expected	**matches regular expression list**
	.*(\-\-\-|\-\-x|\-w\-|\-wx|r\-\-|r\-x|rw\-|rwx)(\-\-\-|\-\-x|r\-\-|r\-x)(\-\-\-|\-\-x|r\-\-|r\-x).*
	OR, any of the selected values below:
	File not found
Actual	**Last Updated:04/21/2024 at 06:00:55 PM (GMT+0530)**
	File not found

Cause of Failure:

Unexpected values	**Additional values found in failed controls:**
	File not found
Missing values	**Expected values not found in failed controls:**
	.*(\-\-\-|\-\-x|\-w\-|\-wx|r\-\-|r\-x|rw\-|rwx)(\-\-\-|\-\-x|r\-\-|r\-x)(\-\-\-|\-\-x|r\-\-|r\-x).*
	OR, any of the selected values below:

(1.7) 3498 Status of the 'SEC_USER_AUDIT_ACTION_BANNER' parameter in sqlnet.ora (oracle19:1:1621:POHK1API_DG2) **Failed** **MEDIUM**

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Failed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

The sqlnet.ora file is used by the Oracle database application to configure profile parameters such as logging and tracing features, prioritizing naming methods, routing connections through specific processes, and Oracle Advanced Security options. By default, the sqlnet.ora file is located in the $ORACLE_HOME/network/admin directory. The 'SEC_USER_AUDIT_ACTION_BANNER' parameter in the sqlnet.ora file defines the file name and path for the text file that contains the user action audit banner. As the audit banner is used to notify users regarding possible user action auditing, the 'SEC_USER_AUDIT_ACTION_BANNER' parameter should be set to a content file appropriate to the needs of the business.

The following List String value(s) X indicate the file and path defined for the SEC_USER_AUDIT_ACTION_BANNER parameter in the sqlnet.ora file.

Expected	**does not contain regular expression list**
	NULL
	OR, any of the selected values below:
	Setting not found
	File not found
Actual	**Last Updated:04/21/2024 at 06:00:55 PM (GMT+0530)**
	File not found

Extended Evidence:

File name	Setting	Value
	SEC_USER_AUDIT_ACTION_BANNER	

Cause of Failure:

Unexpected values	**Additional values found in failed controls:**
	File not found

(1.8) 5601 Status of the RESOURCE_LIMIT parameter(oracle19:1:1621:POHK1API_DG2) — Passed — MEDIUM

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

The RESOURCE_LIMIT setting determines whether or not resource limits are enforced in database profiles. As not enforcing resourcing limits can lead to a Denial-of-Service condition, this value should be set according to the needs of the business.

The following List String value(s) X indicate the current status of the RESOURCE_LIMIT parameter.

Expected	**matches regular expression list**
	TRUE
	OR, any of the selected values below:
	☑ TRUE(0)
	☐ FALSE(1)
	☐ Parameter: RESOURCE_LIMIT not found
	☐ Table not found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	TRUE (0)

Extended Evidence:

VALUE
0

(1.9) 5676 Current installed Oracle version(oracle19:1:1621:POHK1API_DG2) — Passed — HIGH

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

This check inspects the current version of the Oracle installed on the host. The current Oracle version is important for determining that systems and applications are functioning at the levels expected. By periodically reviewing this version information, an administrator can ensure that all functions and security features required are currently in place and available. The setting should be configured according to the needs of the business.

The following List String value(s) X indicates the status of the of the database version to determine the type of ANSI compliant join syntax used.

Expected	**matches regular expression list**
	19.*
	OR, any of the selected values below:
	☐ Version not found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	19.2

Extended Evidence:

VERSION
19.2

(1.10) 8033 Setting for the 'sec_case_sensitive_logon' parameter(oracle19:1:1621:POHK1API_DG2) Passed MEDIUM

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

The SEC_CASE_SENSITIVE_LOGON information determines whether or not case-sensitivity is required for passwords during login. As using mixed-case passwords can strengthen the database against brute-force login attacks, this value should be set according to the needs of the business. WARNING: Due to the security bug CVE-2012-3137 it is recommended to set this parameter to TRUE if the October 2012 CPU/PSU or later was applied. If the patch was not applied it is recommended to set this parameter to FALSE to avoid this vulnerability.

The following List String value X indicates the status of the sec_case_sensitive_logon parameter. A value of TRUE shows that case-sensitive login has been implemented.

Expected	**matches regular expression list**
	TRUE
	OR, any of the selected values below:
	Parameter not found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	TRUE

Extended Evidence:

VALUE
TRUE
TRUE
TRUE

(1.11) 8034 Status of the 'sec_max_failed_login_attempts' parameter setting(oracle19:1:1621: POHK1API_DG2) Passed HIGH

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

The SEC_MAX_FAILED_LOGIN_ATTEMPTS parameter determines the number of failed logins that can occur before Oracle closes the login connection. As not limiting the number of failed login attempts for a user connection can facilitate both brute-force login attacks and the occurrence of Denial-of-Service conditions, this value should be set according to the needs of the organization.

The following List String value X indicates the status of the sec_max_failed_login_attempts parameter. A value of 1 - UNLIMITED shows that the requirement has been implemented.

Expected	**matches regular expression list**
	3
	OR, any of the selected values below:
	Parameter not found
	Table not found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	3

Extended Evidence:

VALUE
3
3
3

(1.12) 8035 Status of the 'sec_protocol_error_further_action' parameter setting(oracle19:1:1621: POHK1API_DG2) Failed MEDIUM

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Failed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

The SEC_PROTOCOL_ERROR_FURTHER_ACTION setting determines the Oracle's server's response to bad/malformed packets received from the client. As bad packets received from the client can potentially indicate packet-based attacks on the system, such as "TCP SYN Flood" or "Smurf" attacks, which may result in a Denial-of-Service condition, this value should be set according to the needs of the business.

The following List String value X indicates the status of the sec_protocol_error_further_action parameter. A value of TRUE shows that the requirement has been implemented.

Expected	**matches regular expression list**
	^\(DROP\,3\)$
	OR, any of the selected values below:
	Parameter not found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	CONTINUE

Extended Evidence:

VALUE
CONTINUE
CONTINUE
CONTINUE

Cause of Failure:

Unexpected values	**Additional values found in failed controls:**
	CONTINUE
Missing values	**Expected values not found in failed controls:**
	^\(DROP\,3\)$
	OR, any of the selected values below:

(1.13) 8036 Status of the 'sec_protocol_error_trace_action' parameter setting(oracle19:1:1621:POHK1API_DG2) **Failed** **MEDIUM**

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Failed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

The SEC_PROTOCOL_ERROR_TRACE_ACTION setting determines the Oracle's server's logging response level to bad/malformed packets received from the client, by generating ALERT, LOG, or TRACE levels of detail in the log files. As incoming bad packets can potentially indicate packet-based attacks, such as "TCP SYN Flood" or "Smurf" attacks that may result in a Denial-of-Service condition, this diagnostic/logging value for ALERT, LOG, or TRACE conditions should be set according to the needs of the business.

The following List String value(s) X indicate the status of the sec_protocol_error_trace_action parameter. A value of TRACE shows that the requirement to create a trace file has been implemented.

Expected	**matches regular expression list**
	^LOG$
	OR, any of the selected values below:
	Parameter not found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	TRACE

Extended Evidence:

VALUE
TRACE
TRACE
TRACE

Cause of Failure:

Unexpected values	**Additional values found in failed controls:**
	TRACE
Missing values	**Expected values not found in failed controls:**
	^LOG$
	OR, any of the selected values below:

(1.14) 8037 Status of the 'sec_return_server_release_banner' parameter setting using SQL query (oracle19:1:1621:POHK1API_DG2) **Passed** **MEDIUM**

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

The 'sec_return_server_release_banner' parameter setting can return information about patch/update release number, providing the exact patch/update version that is currently running. As allowing the return of information about the patch/update release could facilitate unauthorized attempts to gain access based upon known patch weaknesses, this value should be set according to the needs of the business.

The following List String value X indicates the status of the sec_return_server_release_banner parameter. A value of TRUE shows that the requirement has been implemented.

Expected	**matches regular expression list**
	FALSE
	OR, any of the selected values below:
	☑ Parameter not found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	FALSE

Extended Evidence:

VALUE
FALSE
FALSE
FALSE

(1.15) 9597 Ownership and permissions set on $ORACLE_HOME/network/admin directory and files (oracle19:1:1621:POHK1API_DG2) **Failed** **HIGH**

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Failed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

The 'ORACLE_HOME/network/admin' is a directory where oracle Network Configuration files are stored such as Listener.ora,Tnsnames.ora and Sqlnet.ora. Access to ORACLE_HOME/network/admin directory and files should be restricted in order to prevent it from unauthorized users. If unprivileged users can read or alter the network configuration files the security of the oracle server can be compromised. This should be configured according to the needs of the business.

This List String value X indicates the permissions of the files within the $ORACLE_HOME/network/admin directory. With UNIX these files will NOT have the required permission level of 0750.

Expected	**matches regular expression list**
	^oracle\ oinstall\ (0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).*|^grid\ oinstall\ (0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).*
	OR, any of the selected values below:
	☐ File(s) not found
Actual	**Last Updated:04/21/2024 at 06:00:55 PM (GMT+0530)**
	File(s) not found

Extended Evidence:

File name
/network/admin

Cause of Failure:

Unexpected values	**Additional values found in failed controls:**
	File(s) not found
Missing values	**Expected values not found in failed controls:**
	^oracle\ oinstall\ (0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).*|^grid\ oinstall\ (0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).*
	OR, any of the selected values below:

(1.16) 9598 Ownership and permissions set on $ORACLE_HOME/dbs and $ORACLE_HOME/dbs/*(oracle19:1:1621:POHK1API_DG2) **Failed** **HIGH**

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Failed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

The '$ORACLE_HOME/dbs/' is a directory where all Common message files are stored such as init.ora, spfile.ora and password files, logs files. Access to ORACLE_HOME/dbs directory and files should be restricted in order to prevent it from unauthorized users. If unprivileged users can read or alter the dbs files the security of the oracle server can be compromised. This should be configured according to the needs of the business.

This List String value X indicates the permissions of the files within the $ORACLE_HOME/dbs directory. With UNIX these files will NOT have the required permission level of 0750.

Expected	**matches regular expression list**
	^oracle\ oinstall\ (0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).*|^oracle\ asmadmin\ (0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).*
	OR, any of the selected values below:
	File(s) not found
Actual	**Last Updated:04/21/2024 at 06:00:55 PM (GMT+0530)**
	File(s) not found

Extended Evidence:

File name
/dbs

Cause of Failure:

Unexpected values	**Additional values found in failed controls:**
	File(s) not found
Missing values	**Expected values not found in failed controls:**
	^oracle\ oinstall\ (0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).*|^oracle\ asmadmin\ (0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).*
	OR, any of the selected values below:

(1.17) 12623 Status of Unified Auditing mode(oracle19:1:1621:POHK1API_DG2) **Passed** **MEDIUM**

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

This setting specifies the mode of unified auditing, the possible values are Mixed mode: Has both traditional and unified auditing, Pure unified auditing: Has only unified auditing. If database is not configured to audit then it is more difficult to detect and track system compromises and damages incurred during a system compromise. This should be configured as appropriate to the needs of the business.

The following String value of X indicate the status of unified auditing set for the database. Note: FALSE means mix mode of unified auditing is enabled, True means pure mode of unified auditing is enabled.

Expected	**regular expression match**

	TRUE
	OR, any of the selected values below:
	☐ Setting not found
	☐ Table not found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	TRUE

Extended Evidence:

PARAMETER	VALUE
Unified Auditing	TRUE

(1.18) 12624 Status of policies enabled for Unified Auditing(oracle19:1:1621:POHK1API_DG2) — Passed — MEDIUM

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

This setting specifies the list of enabled policies for unified auditing. If database is not configured to audit then it is more difficult to detect and track system compromises and damages incurred during a system compromise. This should be configured as appropriate to the needs of the business.

The following List String value(s) of X provides the list of POLICY enabled for unified auditing in the database. The output contains colon separated values of entity_name, policy_name, enabled_option, success, and failure option set for the unified auditing policies.

Expected	**contains regular expression list**
	.*:SCB_AUDIT_DDL_POLICY:.*:.*:.*
	.*:SCB_AUDIT_DROP_POLICY:.*:.*:.*
	.*:SCB_LOGON_ALL_FAILURES:.*:.*:.*
	.*:SCB_LOGON_LOGOFF_PRIVUSER:.*:.*:.*
	OR, any of the selected values below:
	☐ Setting not found
	☐ Table not found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	ALL USERS:SCB_AUDIT_DDL_POLICY:BY USER:YES:YES
	ALL USERS:SCB_AUDIT_DROP_POLICY:BY USER:YES:YES
	ALL USERS:SCB_LOGON_ALL_FAILURES:BY USER:NO:YES
	ALL USERS:SCB_LOGON_LOGOFF_PRIVUSER:BY USER:YES:YES

Extended Evidence:

ENTITY_NAME	POLICY_NAME	ENABLED_OPTION	SUCCESS	FAILURE
ALL USERS	SCB_LOGON_LOGOFF_PRIVUSER	BY USER	YES	YES
ALL USERS	SCB_LOGON_ALL_FAILURES	BY USER	NO	YES
ALL USERS	SCB_AUDIT_DDL_POLICY	BY USER	YES	YES
ALL USERS	SCB_AUDIT_DROP_POLICY	BY USER	YES	YES

(1.19) 12707 Status of 'extproc' in listener.ora(oracle19:1:1621:POHK1API_DG2) — Failed — HIGH

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Failed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

The listener.ora configuration file is used by the Oracle database application to set profile parameters such as listener name, protocol addresses accepting listener connection requests, database parameters, and control parameters. The 'EXTPROC' parameter allows the database to run procedures from operating system libraries. These library calls can, in turn, run any operating system command. The 'extproc' parameter should be removed from the listener.ora to mitigate the risk that OS libraries can be invoked by the Oracle instance, this should be configured as appropriate to the needs of the business.

The following List String value(s) of X indicate the status of EXTPROC parameter defined in the listener.ora file.

Expected	**does not contain regular expression list**
	EXTPROC

	OR, any of the selected values below:
	☑ String not found
	☐ File not found
Actual	**Last Updated:04/21/2024 at 06:00:55 PM (GMT+0530)**
	File not found

Extended Evidence:

File name	Pattern
	EXTPROC

Cause of Failure:

Unexpected values	**Additional values found in failed controls:**
	File not found

(1.20) 14340 Status of auditing for 'CREATE USER' privilege (Unified Auditing)(oracle19:1:1621: POHK1API_DG2) — Passed — MEDIUM

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

The 'CREATE USER' statement is used to create Oracle database accounts and assign database properties to them. Logging and monitoring of all attempts to create user accounts, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the CREATE USER audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected	**matches regular expression list**
	.*:CREATE USER:.*:YES:YES:.*:.*
	OR, any of the selected values below:
	☐ Setting not found
	☐ Table not found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	SCB_AUDIT_DDL_POLICY:CREATE USER:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_P–OLICY	CREATE USER	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.21) 14341 Status of auditing for 'ALTER USER' privilege (Unified Auditing)(oracle19:1:1621: POHK1API_DG2) — Passed — MEDIUM

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

The ALTER USER statement is used to change database users' password, lock accounts, and expire passwords. Logging and mo nitoring of all attempts to alter user accounts, whether successful or unsuccessful, may provide clues and forensic evid ences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the n eeds of the business.

The following List String value(s) of X indicates the status of the ALTER USER audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected	**matches regular expression list**
	.*:ALTER USER:.*:YES:YES:.*:.*
	OR, any of the selected values below:
	☐ Setting not found

Table not found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

SCB_AUDIT_DDL_POLICY:ALTER USER:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_POLICY	ALTER USER	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.22) 14342 Status of auditing for 'DROP USER' privilege (Unified Auditing)(oracle19:1:1621: POHK1API_DG2) Passed MEDIUM

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

The 'DROP USER' statement is used to drop Oracle database accounts and schemas associated with them. Logging and monitoring of all attempts to drop user accounts, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the DROP USER audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected **matches regular expression list**

.*:DROP USER:.*:YES:YES:.*:.*

OR, any of the selected values below:

Setting not found
Table not found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

SCB_AUDIT_DDL_POLICY:DROP USER:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_POLICY	DROP USER	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.23) 14343 Status of auditing for 'CREATE ROLE' privilege (Unified Auditing)(oracle19:1:1621: POHK1API_DG2) Passed MEDIUM

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

The 'CREATE ROLE' command is a powerful database tool, allowing the creation of a 'role' that can be assigned to a large numbers of users who need the same object/system privileges. Logging and monitoring of all attempts to create roles, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the CREATE ROLE audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected **matches regular expression list**

.*:CREATE ROLE:.*:YES:YES:.*:.*

OR, any of the selected values below:

Setting not found
Table not found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

SCB_AUDIT_DDL_POLICY:CREATE ROLE:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_POLICY	CREATE ROLE	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.24) 14344 Status of auditing for 'ALTER ROLE' privilege (Unified Auditing)(oracle19:1:1621: POHK1API_DG2) Passed MEDIUM

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

The 'ALTER ROLE' command is a powerful database tool, allowing the alteration of a 'role' that can be assigned to a large numbers of users who need the same object/system privileges. Logging and monitoring of all attempts to alter roles, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the ALTER ROLE audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected **matches regular expression list**

.*:ALTER ROLE:.*:YES:YES:.*:.*

OR, any of the selected values below:

- Setting not found
- Table not found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

SCB_AUDIT_DDL_POLICY:ALTER ROLE:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_P–OLICY	ALTER ROLE	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.25) 14345 Status of auditing for 'DROP ROLE' privilege (Unified Auditing)(oracle19:1:1621: POHK1API_DG2) Passed MEDIUM

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

The 'DROP ROLE' command is a powerful database tool, allowing the drop of a 'role' that can be assigned to a large numbers of users who need the same object/system privileges. Logging and monitoring of all attempts to drop roles, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the DROP ROLE audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected **matches regular expression list**

.*:DROP ROLE:.*:YES:YES:.*:.*

OR, any of the selected values below:

- Setting not found
- Table not found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

SCB_AUDIT_DDL_POLICY:DROP ROLE:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_P–OLICY	DROP ROLE	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.26) 14346 Status of auditing for 'GRANT' privilege (Unified Auditing)(oracle19:1:1621: POHK1API_DG2) Passed MEDIUM

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

The 'GRANT' statements are used to grant privileges to Oracle database users and roles, including the most powerful

privileges and roles typically available to the database administrators. With unauthorized grants and permissions, a malicious user may be able to change the security of the database, access/update confidential data, or compromise the integrity of the database. Logging and monitoring of all attempts to grant system privileges, object privileges or roles, whether successful or unsuccessful, may provide forensic evidence about potential suspicious/unauthorized activities as well as privilege escalation activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the GRANT audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected **matches regular expression list**

.*:GRANT:.*:YES:YES:.*:.*

OR, any of the selected values below:

- Setting not found
- Table not found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

SCB_AUDIT_DDL_POLICY:GRANT:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_POLICY	GRANT	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.27) 14347 Status of auditing for 'REVOKE' privilege (Unified Auditing)(oracle19:1:1621:POHK1API_DG2) Passed MEDIUM

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

The 'REVOKE' statements are used to revoke privileges from Oracle database users and roles. Logging and monitoring of all attempts to revoke system privileges, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the REVOKE audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected **matches regular expression list**

.*:REVOKE:.*:YES:YES:.*:.*

OR, any of the selected values below:

- Setting not found
- Table not found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

SCB_AUDIT_DDL_POLICY:REVOKE:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_POLICY	REVOKE	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.28) 14348 Status of auditing for 'CREATE PROFILE' privilege (Unified Auditing)(oracle19:1:1621:POHK1API_DG2) Passed MEDIUM

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Oracle database profiles are used to enforce resource usage limits and implement password policies such as password complexity rules and reuse restrictions. Logging and monitoring of all attempts to create profiles, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the CREATE PROFILE audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected	**matches regular expression list**
	.*:CREATE PROFILE:.*:YES:YES:.*:.*
	OR, any of the selected values below:
	Setting not found
	Table not found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	SCB_AUDIT_DDL_POLICY:CREATE PROFILE:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_P–OLICY	CREATE PROFILE	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.29) 14349 Status of auditing for 'ALTER PROFILE' privilege (Unified Auditing)(oracle19:1:1621: POHK1API_DG2) Passed MEDIUM

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

Oracle database profiles are used to enforce resource usage limits and implement password policies such as password complexity rules and reuse restrictions. Logging and monitoring of all attempts to alter profiles, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the ALTER PROFILE audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected	**matches regular expression list**
	.*:ALTER PROFILE:.*:YES:YES:.*:.*
	OR, any of the selected values below:
	Setting not found
	Table not found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	SCB_AUDIT_DDL_POLICY:ALTER PROFILE:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_P–OLICY	ALTER PROFILE	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.30) 14350 Status of auditing for 'DROP PROFILE' privilege (Unified Auditing)(oracle19:1:1621: POHK1API_DG2) Passed MEDIUM

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

Oracle database profiles are used to enforce resource usage limits and implement password policies such as password complexity rules and reuse restrictions. Logging and monitoring of all attempts to drop profiles, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the DROP PROFILE audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected	**matches regular expression list**
	.*:DROP PROFILE:.*:YES:YES:.*:.*
	OR, any of the selected values below:
	Setting not found
	Table not found

Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	SCB_AUDIT_DDL_POLICY:DROP PROFILE:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_POLICY	DROP PROFILE	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.31) 14351 Status of auditing for 'CREATE DATABASE LINK' privilege (Unified Auditing) (oracle19:1:1621:POHK1API_DG2) — Passed — MEDIUM

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Oracle database links are used to establish database-to-database connections to other databases. These connections are available without further authentication once the link is established. Logging and monitoring of all attempts to create database links, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the CREATE DATABASE LINK audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected	**matches regular expression list**
	.*:CREATE DATABASE LINK:.*:YES:YES:.*:.*
	OR, any of the selected values below:
	☐ Setting not found
	☐ Table not found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	SCB_AUDIT_DDL_POLICY:CREATE DATABASE LINK:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_POLICY	CREATE DATABASE LINK	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.32) 14352 Status of auditing for 'ALTER DATABASE LINK' privilege (Unified Auditing) (oracle19:1:1621:POHK1API_DG2) — Passed — MEDIUM

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Oracle database links are used to establish database-to-database connections to other databases. These connections are available without further authentication once the link is established. Logging and monitoring of all attempts to alter database links, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the ALTER DATABASE LINK audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected	**matches regular expression list**
	.*:ALTER DATABASE LINK:.*:YES:YES:.*:.*
	OR, any of the selected values below:
	☐ Setting not found
	☐ Table not found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	SCB_AUDIT_DDL_POLICY:ALTER DATABASE LINK:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_POLICY	ALTER DATABASE LINK	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.33) 14353 Status of auditing for 'DROP DATABASE LINK' privilege (Unified Auditing) (oracle19:1:1621:POHK1API_DG2) — Passed — MEDIUM

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

Oracle database links are used to establish database-to-database connections to other databases. These connections are available without further authentication once the link is established. Logging and monitoring of all attempts to drop database links, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the DROP DATABASE LINK audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected — **matches regular expression list**

.*:DROP DATABASE LINK:.*:YES:YES:.*:.*

OR, any of the selected values below:

- Setting not found
- Table not found

Actual — **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

SCB_AUDIT_DDL_POLICY:DROP DATABASE LINK:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_POLICY	DROP DATABASE LINK	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.34) 14354 Status of auditing for 'CREATE SYNONYM' privilege (Unified Auditing)(oracle19:1:1621:POHK1API_DG2) — Passed — MEDIUM

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

An Oracle database synonym is used to create an alternative name for a database object such as table, view, procedure, java object or even another synonym, etc. Logging and monitoring of all attempts to create synonyms, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the CREATE SYNONYM audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected — **matches regular expression list**

.*:CREATE SYNONYM:.*:YES:YES:.*:.*

OR, any of the selected values below:

- Setting not found
- Table not found

Actual — **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

SCB_AUDIT_DDL_POLICY:CREATE SYNONYM:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_POLICY	CREATE SYNONYM	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.35) 14355 Status of auditing for 'ALTER SYNONYM' privilege (Unified Auditing)(oracle19:1:1621:POHK1API_DG2) — Passed — MEDIUM

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

An Oracle database synonym is used to create an alternative name for a database object such as table, view, procedure,

java object or even another synonym, etc. Logging and monitoring of all attempts to alter synonyms, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the ALTER SYNONYM audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected **matches regular expression list**

.*:ALTER SYNONYM:.*:YES:YES:.*:.*

OR, any of the selected values below:

- Setting not found
- Table not found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

SCB_AUDIT_DDL_POLICY:ALTER SYNONYM:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_POLICY	ALTER SYNONYM	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.36) 14356 Status of auditing for 'DROP SYNONYM' privilege (Unified Auditing)(oracle19:1:1621:POHK1API_DG2) Passed MEDIUM

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

An Oracle database synonym is used to create an alternative name for a database object such as table, view, procedure, java object or even another synonym, etc. Logging and monitoring of all attempts to drop synonyms, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the DROP SYNONYM audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected **matches regular expression list**

.*:DROP SYNONYM:.*:YES:YES:.*:.*

OR, any of the selected values below:

- Setting not found
- Table not found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

SCB_AUDIT_DDL_POLICY:DROP SYNONYM:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_POLICY	DROP SYNONYM	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.37) 14359 Status of auditing for 'ALTER SYSTEM' privilege (Unified Auditing)(oracle19:1:1621:POHK1API_DG2) Passed MEDIUM

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

The 'ALTER SYSTEM' privilege allows the user to change instance settings which could impact security posture, performance or normal operation of the database. Additionally, the ALTER SYSTEM privilege may be used to run operating system commands using undocumented Oracle functionality. Logging and monitoring of all attempts to execute ALTER SYSTEM statements, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the ALTER SYSTEM audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected **matches regular expression list**

	.*:ALTER SYSTEM:.*:YES:YES:.*:.*
	OR, any of the selected values below:
	☐ Setting not found
	☐ Table not found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	SCB_AUDIT_DDL_POLICY:ALTER SYSTEM:SYSTEM PRIVILEGE:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_P–OLICY	ALTER SYSTEM	SYSTEM PRIVILEGE	YES	YES	BY USER	ALL USERS

(1.38) 14360 Status of auditing for 'CREATE TRIGGER' privilege (Unified Auditing)(oracle19:1:1621: POHK1API_DG2) Passed MEDIUM

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Oracle database triggers are executed automatically when specified conditions on the underlying objects occur. Trigger bodies contain the code, quite often to perform data validation, ensure data integrity/security or enforce critical constraints on allowable actions on data. Logging and monitoring of all attempts to create triggers, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the CREATE TRIGGER audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected	**matches regular expression list**
	.*:CREATE TRIGGER:.*:YES:YES:.*:.*
	OR, any of the selected values below:
	☐ Setting not found
	☐ Table not found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	SCB_AUDIT_DDL_POLICY:CREATE TRIGGER:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_P–OLICY	CREATE TRIGGER	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.39) 14361 Status of auditing for 'ALTER TRIGGER' privilege (Unified Auditing)(oracle19:1:1621: POHK1API_DG2) Passed MEDIUM

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Oracle database triggers are executed automatically when specified conditions on the underlying objects occur. Trigger bodies contain the code, quite often to perform data validation, ensure data integrity/security or enforce critical constraints on allowable actions on data. Logging and monitoring of all attempts to alter triggers, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the ALTER TRIGGER audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected	**matches regular expression list**
	.*:ALTER TRIGGER:.*:YES:YES:.*:.*
	OR, any of the selected values below:
	☐ Setting not found
	☐ Table not found

Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	SCB_AUDIT_DDL_POLICY:ALTER TRIGGER:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_P–OLICY	ALTER TRIGGER	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.40) 14362 Status of auditing for 'DROP TRIGGER' privilege (Unified Auditing)(oracle19:1:1621:POHK1API_DG2) Passed MEDIUM

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Oracle database triggers are executed automatically when specified conditions on the underlying objects occur. Trigger bodies contain the code, quite often to perform data validation, ensure data integrity/security or enforce critical constraints on allowable actions on data. Logging and monitoring of all attempts to drop triggers, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the DROP TRIGGER audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected	**matches regular expression list**
	.*:DROP TRIGGER:.*:YES:YES:.*:.*
	OR, any of the selected values below:
	☐ Setting not found
	☐ Table not found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	SCB_AUDIT_DDL_POLICY:DROP TRIGGER:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_P–OLICY	DROP TRIGGER	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.41) 14364 Status of auditing for 'CREATE PROCEDURE' statement (Unified Auditing) (oracle19:1:1621:POHK1API_DG2) Passed MEDIUM

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Oracle database procedures, which are stored within the database, are created to perform business functions and access database as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring of all attempts to create procedure, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the CREATE PROCEDURE audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected	**matches regular expression list**
	.*:CREATE PROCEDURE:.*:YES:YES:.*:.*
	OR, any of the selected values below:
	☐ Setting not found
	☐ Table not found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	SCB_AUDIT_DDL_POLICY:CREATE PROCEDURE:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_P–OLICY	CREATE PROCEDURE	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.42) 14365 Status of auditing for 'CREATE FUNCTION' statement (Unified Auditing)(oracle19:1:1621: POHK1API_DG2) Passed MEDIUM

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

Oracle database function, which are stored within the database, are created to perform business functions and access database as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring of all attempts to create function, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the CREATE FUNCTION audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected **matches regular expression list**

.*:CREATE FUNCTION:.*:YES:YES:.*:.*

OR, any of the selected values below:

- Setting not found
- Table not found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

SCB_AUDIT_DDL_POLICY:CREATE FUNCTION:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_POLICY	CREATE FUNCTION	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.43) 14366 Status of auditing for 'CREATE PACKAGE' statement (Unified Auditing) (oracle19:1:1621:POHK1API_DG2) Passed MEDIUM

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

Oracle database packages, which are stored within the database, are created to perform business functions and access database as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring of all attempts to create package, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the CREATE PACKAGE audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected **matches regular expression list**

.*:CREATE PACKAGE:.*:YES:YES:.*:.*

OR, any of the selected values below:

- Setting not found
- Table not found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

SCB_AUDIT_DDL_POLICY:CREATE PACKAGE:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_POLICY	CREATE PACKAGE	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.44) 14367 Status of auditing for 'CREATE PACKAGE BODY' statement (Unified Auditing) (oracle19:1:1621:POHK1API_DG2) Passed MEDIUM

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

Oracle database packages body, which are stored within the database, are created to perform business functions and

access database as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring of all attempts to create package body, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the CREATE PACKAGE BODY audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected **matches regular expression list**

.*:CREATE PACKAGE BODY:.*:YES:YES:.*:.*

OR, any of the selected values below:

- Setting not found
- Table not found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

SCB_AUDIT_DDL_POLICY:CREATE PACKAGE BODY:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_POLICY	CREATE PACKAGE BODY	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.45) 14368 Status of auditing for 'ALTER PROCEDURE' statement (Unified Auditing) (oracle19:1:1621:POHK1API_DG2) — Passed — MEDIUM

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Oracle database procedures, which are stored within the database, are created to perform business functions and access database as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring of all attempts to alter procedure, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the ALTER PROCEDURE audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected **matches regular expression list**

.*:ALTER PROCEDURE:.*:YES:YES:.*:.*

OR, any of the selected values below:

- Setting not found
- Table not found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

SCB_AUDIT_DDL_POLICY:ALTER PROCEDURE:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_POLICY	ALTER PROCEDURE	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.46) 14369 Status of auditing for 'ALTER FUNCTION' statement (Unified Auditing)(oracle19:1:1621: POHK1API_DG2) — Passed — MEDIUM

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Oracle database function, which are stored within the database, are created to perform business functions and access database as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring of all attempts to alter function, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the ALTER FUNCTION audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected	**matches regular expression list**
	.*:ALTER FUNCTION:.*:YES:YES:.*:.*
	OR, any of the selected values below:
	☐ Setting not found
	☐ Table not found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	SCB_AUDIT_DDL_POLICY:ALTER FUNCTION:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_P–OLICY	ALTER FUNCTION	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.47) 14370 Status of auditing for 'ALTER PACKAGE' statement (Unified Auditing)(oracle19:1:1621: POHK1API_DG2) Passed MEDIUM

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Oracle database packages, which are stored within the database, are created to perform business functions and access database as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring of all attempts to alter package, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the ALTER PACKAGE audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected	**matches regular expression list**
	.*:ALTER PACKAGE:.*:YES:YES:.*:.*
	OR, any of the selected values below:
	☐ Setting not found
	☐ Table not found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	SCB_AUDIT_DDL_POLICY:ALTER PACKAGE:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_P–OLICY	ALTER PACKAGE	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.48) 14371 Status of auditing for 'ALTER PACKAGE BODY' statement (Unified Auditing) (oracle19:1:1621:POHK1API_DG2) Passed MEDIUM

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Oracle database package bodies, which are stored within the database, are created to perform business functions and access database as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring of all attempts to alter package body, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the ALTER PACKAGE BODY audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected	**matches regular expression list**
	.*:ALTER PACKAGE BODY:.*:YES:YES:.*:.*
	OR, any of the selected values below:
	☐ Setting not found
	☐ Table not found

Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	SCB_AUDIT_DDL_POLICY:ALTER PACKAGE BODY:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_POLICY	ALTER PACKAGE BODY	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.49) 14372 Status of auditing for 'DROP PROCEDURE' statement (Unified Auditing) (oracle19:1:1621:POHK1API_DG2) — Passed — MEDIUM

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Oracle database procedures, which are stored within the database, are created to perform business functions and access database as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring of all attempts to drop procedure, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the DROP PROCEDURE audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected	**matches regular expression list**
	.*:DROP PROCEDURE:.*:YES:YES:.*:.*
	OR, any of the selected values below:
	☐ Setting not found
	☐ Table not found

Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	SCB_AUDIT_DDL_POLICY:DROP PROCEDURE:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_POLICY	DROP PROCEDURE	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.50) 14373 Status of auditing for 'DROP FUNCTION' statement (Unified Auditing)(oracle19:1:1621:POHK1API_DG2) — Passed — MEDIUM

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Oracle database function, which are stored within the database, are created to perform business functions and access database as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring of all attempts to drop function, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the DROP FUNCTION audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected	**matches regular expression list**
	.*:DROP FUNCTION:.*:YES:YES:.*:.*
	OR, any of the selected values below:
	☐ Setting not found
	☐ Table not found

Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	SCB_AUDIT_DDL_POLICY:DROP FUNCTION:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_POLICY	DROP FUNCTION	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.51) 14374 Status of auditing for 'DROP PACKAGE' statement (Unified Auditing)(oracle19:1:1621:POHK1API_DG2) Passed MEDIUM

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Oracle database packages, which are stored within the database, are created to perform business functions and access database as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring of all attempts to drop package, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the DROP PACKAGE audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected **matches regular expression list**

.*:DROP PACKAGE:.*:YES:YES:.*:.*

OR, any of the selected values below:

- Setting not found
- Table not found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

SCB_AUDIT_DDL_POLICY:DROP PACKAGE:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_POLICY	DROP PACKAGE	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.52) 14375 Status of auditing for 'DROP PACKAGE BODY' statement (Unified Auditing) (oracle19:1:1621:POHK1API_DG2) Passed MEDIUM

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Oracle database package bodies, which are stored within the database, are created to perform business functions and access database as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring of all attempts to drop package body, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the DROP PACKAGE BODY audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected **matches regular expression list**

.*DROP PACKAGE BODY:.*:YES:YES:.*:.*

OR, any of the selected values below:

- Setting not found
- Table not found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

SCB_AUDIT_DDL_POLICY:DROP PACKAGE BODY:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_POLICY	DROP PACKAGE BODY	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.53) 14376 Status of auditing for 'LOGON' action (Unified Auditing)(oracle19:1:1621:POHK1API_DG2) Passed MEDIUM

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Oracle database users log on to the database to perform their work. Logon action audit captures logon activities. Logging and monitoring of all attempts to logon to the database, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the LOGON audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected **matches regular expression list**

.*:LOGON:.*:.*:YES:.*:.*

OR, any of the selected values below:

Setting not found

Table not found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

SCB_LOGON_ALL_FAILURES:LOGON:STANDARD ACTION:NO:YES:BY USER:ALL USERS

SCB_LOGON_LOGOFF_PRIVUSER:LOGON:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_LOGON_LOGO–FF_PRIVUSER	LOGON	STANDARD ACTION	YES	YES	BY USER	ALL USERS
SCB_LOGON_ALL_–FAILURES	LOGON	STANDARD ACTION	NO	YES	BY USER	ALL USERS

(1.54) 14377 Status of auditing for 'LOGOFF' action (Unified Auditing)(oracle19:1:1621: POHK1API_DG2) — Passed — MEDIUM

Instance oracle19:1:1621:POHK1API_DG2

Previous Status Passed

Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

The 'Logoff' action audit captures logoff activities of the database users. Logging and monitoring of all attempts to logon to the database, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the LOGOFF audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

Expected **matches regular expression list**

.*:LOGOFF:.*:YES:YES:.*:.*

OR, any of the selected values below:

Setting not found

Table not found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

SCB_LOGON_LOGOFF_PRIVUSER:LOGOFF:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_LOGON_LOGO–FF_PRIVUSER	LOGOFF	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.55) 24264 Status of ENCRYPTION_SERVER and AUTHENTICATION_SERVICES(oracle19:1:1621: POHK1API_DG2) — Failed — MEDIUM

Instance oracle19:1:1621:POHK1API_DG2

Previous Status Failed

Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

The sqlnet.ora file is used by the Oracle database application to configure profile parameters such as logging and tracing features, prioritizing naming methods, routing connections through specific processes, and Oracle Advanced Security options. The 'ENCRYPTION_SERVER' parameter in the sqlnet.ora file determines whether or not encryption is enabled on the database server. 'AUTHENTICATION_SERVICES' enables one or more authentication services. If authentication has been installed, then the valid authentication method can be none, all, beq, Kerberos, nts, radius, and tips. This setting should be configured according to the needs of the business.

This String value X indicates the current value set for the SQLNET.ENCRYPTION_SERVER parameter in the sqlnet.ora file.

Expected **regular expression match**

REQUESTED

OR, any of the selected values below:

- ☐ Setting not found
- ☐ File not found

Actual **Last Updated:04/21/2024 at 06:00:55 PM (GMT+0530)**

File not found

Extended Evidence:

File name	Setting	Value
	sqlnet.encryption_server	

OR

The following List String value(s) of X indicates the status of the SQLNET.authentication_services setting defined within the sqlnet.ora file.

Expected **contains regular expression list**

tcps

OR, any of the selected values below:

- ☐ Setting not found
- ☐ File not found

Actual **Last Updated:04/21/2024 at 06:00:55 PM (GMT+0530)**

File not found

Extended Evidence:

File name	Setting	Value
	sqlnet.authentication_services	

(1.56) 100628 Disallow Factory or Vendor Default accounts in Production(oracle19:1:1621:POHK1API_DG2) — Passed — HIGH

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

Disallow Factory or Vendor Default accounts in Production

Disallow Factory or Vendor Default accounts in Production

Scan Parameters:

DBQUERY: select username from dba_users

Expected **does not contain regular expression list**

DB Column Name: USERNAME

^SH$

^SCOTT$

^PM$

^OE$

^IX$

^HR$

^BI$

OR, any of the selected values below:

- ☑ Set status to PASS if no data found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

USERNAME
SYS
SYSTEM
XS$NULL
OJVMSYS
LBACSYS

OUTLN
SYS$UMF
APPQOSSYS
DBSFWUSER
GGSYS
ANONYMOUS
CTXSYS
DVSYS
DVF
GSMADMIN_INTERNAL
MDSYS
OLAPSYS
XDB
WMSYS
DBSNMP
GSMCATUSER
MDDATA
SYSBACKUP
REMOTE_SCHEDULER_AGENT
GSMUSER
SYSRAC
GSMROOTUSER
SI_INFORMTN_SCHEMA
AUDSYS
DIP
ORDPLUGINS
SYSKM
ORDDATA
ORACLE_OCM
SYSDG
ORDSYS
ORARO
SECADMIN
CCS_SCAN
SCB_LINK
DBARO
DBADDM
OEMUSER
ORAMED1
CC_ITRS
AOGEMS
SCB_ADMIN

Extended Evidence:

Statistics:

Query returned 47 rows

(1.57) 101067 Status of auditing on the unified audit table(CIS-100)(oracle19:1:1621:POHK1API_DG2) Passed HIGH

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

Status of auditing on the unified audit table(CIS-100)

Status of auditing on the unified audit table(CIS-100)

Scan Parameters:

DBQUERY: SELECT OBJECT_NAME FROM AUDIT_UNIFIED_POLICIES WHERE AUDIT_OPTION='ALL' AND OBJECT_NAME='AUD$UNIFIED' AND POLICY_NAME IN (SELECT POLICY_NAME FROM AUDIT_UNIFIED_ENABLED_POLICIES)

Expected	**matches regular expression list**
	DB Column Name: OBJECT_NAME
	AUD\$UNIFIED
	OR, any of the selected values below:
	☐ Set status to PASS if no data found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

OBJECT_NAME
AUD$UNIFIED

Extended Evidence:

Statistics:

Query returned 1 rows

(1.58) 101068 Status of Vendor Default accounts in Production(IAM-120)(oracle19:1:1621:POHK1API_DG2) — Passed — HIGH

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Status of Vendor Default accounts in Production(IAM-120)

Status of Vendor Default accounts in Production(IAM-120)

Scan Parameters:

DBQUERY: SELECT DISTINCT A.USERNAME FROM DBA_USERS_WITH_DEFPWD A, DBA_USERS B WHERE A.USERNAME = B.USERNAME AND B.ACCOUNT_STATUS = 'OPEN'

Expected	**any of the selected values below:**
	☑ Set status to PASS if no data found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.59) 101070 Status of Database user password complexity('PASSWORD_VERIFY_FUNCTION')(IAM-400,CIS-26,CIS-9)(oracle19:1:1621:POHK1API_DG2) — Passed — HIGH

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Status of Database user password complexity('PASSWORD_VERIFY_FUNCTION')(IAM-400,CIS-26,CIS-9)

Status of Database user password complexity('PASSWORD_VERIFY_FUNCTION')(IAM-400,CIS-26,CIS-9)

Scan Parameters:

DBQUERY: select distinct con_id,profile,limit,common from cdb_profiles where resource_name='PASSWORD_VERIFY_FUNCTION' and con_id<>2 and limit<>'FROM ROOT'

Expected	**matches regular expression list**
	DB Column Name: LIMIT
	SCB_19C_PWD_VERIFY_FUNCTION*
	OR, any of the selected values below:
	☐ Set status to PASS if no data found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

CON_ID	PROFILE	LIMIT	COMMON
1	SCB_INFRA_APP	SCB_19C_PWD_VERIFY_FUNCTION	YES
3	SCB_STATIC_APP_ATX	SCB_19C_PWD_VERIFY_FUNCTION	NO
1	DEFAULT	SCB_19C_PWD_VERIFY_FUNCTION	NO

1	ORA_STIG_PROFILE	SCB_19C_PWD_VERIFY_FUNCTION	NO
1	SCB_STATIC_APP	SCB_19C_PWD_VERIFY_FUNCTION	YES
3	SCB_SUPP	SCB_19C_PWD_VERIFY_FUNCTION	NO
3	SCB_STATIC_APP_PSS	SCB_19C_PWD_VERIFY_FUNCTION	NO
3	DEFAULT	SCB_19C_PWD_VERIFY_FUNCTION	NO
1	SCB_INFRA_SUPP	SCB_19C_PWD_VERIFY_FUNCTION	YES
3	ORA_STIG_PROFILE	SCB_19C_PWD_VERIFY_FUNCTION	NO

Extended Evidence:

Statistics:

Query returned 10 rows

(1.60) 101075 Status of the IDLE-TIME resource parameter set for Oracle profiles (IAM-450) (oracle19:1:1621:POHK1API_DG2) — Passed — MEDIUM

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Status of the IDLE-TIME resource parameter set for Oracle profiles (IAM-450)

Status of the IDLE-TIME resource parameter set for Oracle profiles (IAM-450)

Scan Parameters:

DBQUERY: select distinct profile,limit from cdb_profiles where (profile like 'SCB_SUPP%' or profile like 'SCB_INFRA_SUPP%') and resource_name= 'IDLE_TIME'

Expected **match all equal to**

DB Column Name: LIMIT

15

OR, any of the selected values below:

☐ Set status to PASS if no data found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

PROFILE	LIMIT
SCB_SUPP	15
SCB_INFRA_SUPP	15

Extended Evidence:

Statistics:

Query returned 2 rows

(1.61) 101101 Ensure 'EXECUTE_CATALOG_ROLE' Is Revoked from Unauthorized 'GRANTEE' (CIS-62)(oracle19:1:1621:POHK1API_DG2) — Passed — HIGH

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Ensure 'EXECUTE_CATALOG_ROLE' Is Revoked from Unauthorized 'GRANTEE'(CIS-62)

Ensure 'EXECUTE_CATALOG_ROLE' Is Revoked from Unauthorized 'GRANTEE'(CIS-62)

Scan Parameters:

DBQUERY:
```
SELECT GRANTEE, GRANTED_ROLE,CON_ID
FROM CDB_ROLE_PRIVS A WHERE GRANTED_ROLE='EXECUTE_CATALOG_ROLE'
AND GRANTEE NOT IN (SELECT USERNAME FROM CDB_USERS WHERE ORACLE_MAINTAINED='Y')
AND GRANTEE NOT IN (SELECT ROLE FROM CDB_ROLES WHERE ORACLE_MAINTAINED='Y')
AND GRANTEE NOT IN ('SQLTXPLAIN')
```

Expected **any of the selected values below:**

☑ Set status to PASS if no data found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.62) 101103 Ensure 'SELECT_CATALOG_ROLE' Is Revoked from Unauthorized 'GRANTEE'(CIS-61) (oracle19:1:1621:POHK1API_DG2) Passed MEDIUM

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

Ensure 'SELECT_CATALOG_ROLE' Is Revoked from Unauthorized 'GRANTEE'(CIS-61)

Ensure 'SELECT_CATALOG_ROLE' Is Revoked from Unauthorized 'GRANTEE'(CIS-61)

Scan Parameters:

DBQUERY: SELECT GRANTEE, GRANTED_ROLE FROM DBA_ROLE_PRIVS
WHERE GRANTED_ROLE='SELECT_CATALOG_ROLE' AND GRANTEE NOT IN (SELECT USERNAME FROM DBA_USERS WHERE ORACLE_MAINTAINED='Y') AND GRANTEE NOT IN (SELECT ROLE FROM DBA_ROLES WHERE ORACLE_MAINTAINED='Y')
AND GRANTEE NOT IN ('CCS_SCAN','SECADMIN','ORAMED1','ORAMED2','GGADMIN','SCB_ADMIN','AOGEMS','DBAID','DBADDM', 'DBARO','ORARO','DBARO2', 'SCB_LINK', 'ORACLE', 'PATROL','PUPPETAM') and GRANTEE not like '%CDC%' and GRANTEE not like 'SQLT%' and GRANTEE not like 'GGADM%' and GRANTEE not like 'PATROL%'

Expected **any of the selected values below:**

☑ Set status to PASS if no data found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.63) 101107 Ensure 'CREATE LIBRARY' Is Revoked from Unauthorized 'GRANTEE'(CIS-57) (oracle19:1:1621:POHK1API_DG2) Passed HIGH

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

Ensure 'CREATE LIBRARY' Is Revoked from Unauthorized 'GRANTEE'(CIS-57)

Ensure 'CREATE LIBRARY' Is Revoked from Unauthorized 'GRANTEE'(CIS-57)

Scan Parameters:

DBQUERY: SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS
WHERE PRIVILEGE='CREATE LIBRARY' AND GRANTEE NOT IN (SELECT USERNAME FROM DBA_USERS WHERE ORACLE_MAINTAINED='Y') AND GRANTEE NOT IN (SELECT ROLE FROM DBA_ROLES WHERE ORACLE_MAINTAINED='Y')
And GRANTEE not in ('SPATIAL_WFS_ADMIN_USR','SPATIAL_CSW_ADMIN_USR')

Expected **any of the selected values below:**

☑ Set status to PASS if no data found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.64) 101108 Ensure 'CREATE ANY LIBRARY' Is Revoked from Unauthorized 'GRANTEE'(CIS-56) (oracle19:1:1621:POHK1API_DG2) Passed HIGH

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

Ensure 'CREATE ANY LIBRARY' Is Revoked from Unauthorized 'GRANTEE'(CIS-56)

Ensure 'CREATE ANY LIBRARY' Is Revoked from Unauthorized 'GRANTEE'(CIS-56)

Scan Parameters:

DBQUERY: SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS
WHERE PRIVILEGE='CREATE ANY LIBRARY' AND GRANTEE NOT IN (SELECT USERNAME FROM DBA_USERS WHERE ORACLE_MAINTAINED='Y') AND GRANTEE NOT IN (SELECT ROLE FROM DBA_ROLES WHERE ORACLE_MAINTAINED='Y');

Expected **any of the selected values below:**

☑ Set status to PASS if no data found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.65) 101109 Ensure 'ALTER SYSTEM' Is Revoked from Unauthorized 'GRANTEE'(CIS-55) (oracle19:1:1621:POHK1API_DG2) — Passed — HIGH

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Ensure 'ALTER SYSTEM' Is Revoked from Unauthorized 'GRANTEE'(CIS-55)

Ensure 'ALTER SYSTEM' Is Revoked from Unauthorized 'GRANTEE'(CIS-55)

Scan Parameters:

DBQUERY: SELECT GRANTEE, PRIVILEGE,CON_ID
FROM CDB_SYS_PRIVS A WHERE PRIVILEGE='ALTER SYSTEM' AND GRANTEE NOT IN (SELECT USERNAME FROM CDB_USERS WHERE
ORACLE_MAINTAINED='Y') AND GRANTEE NOT IN (SELECT ROLE FROM CDB_ROLES WHERE ORACLE_MAINTAINED='Y')
and grantee not in ('GGADMIN')

Expected **any of the selected values below:**

☑ Set status to PASS if no data found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.66) 101110 Ensure 'BECOME USER' Is Revoked from Unauthorized 'GRANTEE'(CIS-53) (oracle19:1:1621:POHK1API_DG2) — Passed — HIGH

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Ensure 'BECOME USER' Is Revoked from Unauthorized 'GRANTEE'(CIS-53)

Ensure 'BECOME USER' Is Revoked from Unauthorized 'GRANTEE'(CIS-53)

Scan Parameters:

DBQUERY: SELECT GRANTEE, PRIVILEGE,CON_ID
FROM CDB_SYS_PRIVS A WHERE PRIVILEGE='BECOME USER'
AND GRANTEE NOT IN (SELECT USERNAME FROM CDB_USERS WHERE ORACLE_MAINTAINED='Y')
AND GRANTEE NOT IN (SELECT ROLE FROM CDB_ROLES WHERE ORACLE_MAINTAINED='Y') and grantee not in ('GGADMIN')

Expected **any of the selected values below:**

☑ Set status to PASS if no data found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.67) 101112 Ensure 'AUDIT SYSTEM' Is Revoked from Unauthorized 'GRANTEE'(CIS-51) (oracle19:1:1621:POHK1API_DG2) — Passed — HIGH

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Ensure 'AUDIT SYSTEM' Is Revoked from Unauthorized 'GRANTEE'(CIS-51)

Ensure 'AUDIT SYSTEM' Is Revoked from Unauthorized 'GRANTEE'(CIS-51)

Scan Parameters:

DBQUERY:
```
SELECT GRANTEE, PRIVILEGE,CON_ID
FROM CDB_SYS_PRIVS A WHERE PRIVILEGE='AUDIT SYSTEM'
AND GRANTEE NOT IN (SELECT USERNAME FROM CDB_USERS WHERE ORACLE_MAINTAINED='Y')
AND GRANTEE NOT IN (SELECT ROLE FROM CDB_ROLES WHERE ORACLE_MAINTAINED='Y');
```

Expected **any of the selected values below:**

☑ Set status to PASS if no data found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.68) 101113 Ensure 'SELECT ANY DICTIONARY' Is Revoked from Unauthorized 'GRANTEE'(cis-49) (oracle19:1:1621:POHK1API_DG2) — Failed — MEDIUM

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Failed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Ensure 'SELECT ANY DICTIONARY' Is Revoked from Unauthorized 'GRANTEE'(cis-49)

Ensure 'SELECT ANY DICTIONARY' Is Revoked from Unauthorized 'GRANTEE'(cis-49)

Scan Parameters:

DBQUERY:
```
SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS
WHERE PRIVILEGE='SELECT ANY DICTIONARY' AND GRANTEE NOT IN (SELECT USERNAME FROM DBA_USERS WHERE
ORACLE_MAINTAINED='Y') AND GRANTEE NOT IN (SELECT ROLE FROM DBA_ROLES WHERE ORACLE_MAINTAINED='Y')
AND GRANTEE NOT IN  ('CCS_SCAN','SECADMIN','DBARO','ORARO','DBARO2','ORAMED1','GGADMIN','SCB_ADMIN', 'SCB_LINK',
'ORACLE', 'ORAMED2',  'PATROL', 'SYSADM', 'SELECT_SYSADM_ROLE','PUPPETAM') and GRANTEE not like '%CDC%' and GRANTEE not
like 'GGADM%' and GRANTEE not like 'PATROL%' and GRANTEE not like 'APEX%' and GRANTEE not like 'GGMON%' and GRANTEE not
like
'PERF_MON%' and GRANTEE not like 'SCB_PERFSTAT%' and GRANTEE not like 'SPLEX%' and GRANTEE  not like  'SQLT%'
```

Expected **any of the selected values below:**

☑ Set status to PASS if no data found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

GRANTEE	PRIVILEGE
CC_ITRS	SELECT ANY DICTIONARY

Extended Evidence:

Statistics:

Query returned 1 rows

(1.69) 101115 Ensure 'ALL' Is Revoked from Unauthorized 'GRANTEE' on 'AUD$'(CIS-42) (oracle19:1:1621:POHK1API_DG2) — Passed — HIGH

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed

Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Ensure 'ALL' Is Revoked from Unauthorized 'GRANTEE' on 'AUD$'(CIS-42)

Ensure 'ALL' Is Revoked from Unauthorized 'GRANTEE' on 'AUD$'(CIS-42)

Scan Parameters:

DBQUERY: SELECT GRANTEE, PRIVILEGE, CON_ID
FROM CDB_TAB_PRIVS A WHERE TABLE_NAME='AUD$' AND OWNER = 'SYS' and grantee not in('DELETE_CATALOG_ROLE', 'SECURITY_ADMIN');

Expected **any of the selected values below:**

☑ Set status to PASS if no data found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.70) 101140 Status of the 'REMOTE_LISTENER' setting via SQL query (CIS-8)(oracle19:1:1621: POHK1API_DG2) Passed HIGH

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Status of the 'REMOTE_LISTENER' setting via SQL query (CIS-8)

Status of the 'REMOTE_LISTENER' setting via SQL query (CIS-8)

Scan Parameters:

DBQUERY: select 'N' from v$system_parameter sp , v$system_parameter cd where upper(sp.name)= 'REMOTE_LISTENER' and lower(cd.name)= 'cluster_database' and cd.value='TRUE' and sp.value is null
union
select 'N' from v$system_parameter sp , v$system_parameter cd where upper(sp.name)= 'REMOTE_LISTENER' and lower(cd.name)= 'cluster_database' and cd.value='FALSE' and sp.value is not null

Expected **any of the selected values below:**

☑ Set status to PASS if no data found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.71) 101149 Status of the existence of the sys.user$mig table(CIS-33)(oracle19:1:1621: POHK1API_DG2) Passed HIGH

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Status of the existence of the sys.user$mig table(CIS-33)

Status of the existence of the sys.user$mig table(CIS-33)

Scan Parameters:

DBQUERY: SELECT OWNER, TABLE_NAME, CON_ID FROM CDB_TABLES A WHERE TABLE_NAME='USER$MIG' AND OWNER='SYS'

Expected **any of the selected values below:**

☑ Set status to PASS if no data found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.72) 101150 List of public database links present in the database(CIS-34)(oracle19:1:1621:POHK1API_DG2) — Passed — MEDIUM

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

List of public database links present in the database(CIS-34)

List of public database links present in the database(CIS-34)

Scan Parameters:

DBQUERY: SELECT DB_LINK, HOST,CON_ID FROM CDB_DB_LINKS A WHERE OWNER = 'PUBLIC'

Expected	**any of the selected values below:**
	☑ Set status to PASS if no data found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.73) 1051 Status of the 'os_roles=' setting in init.ora(oracle19:1:1621:POHK1API_DG2) — Passed — HIGH

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

The 'os_roles=*' setting determines if the database or the operating system will identify/manage the roles of each username. As OS roles are subject to control outside of the database, this can be a security risk, for the OS Admin (instead of the DBA) will be granting privileges and should be set according to the needs of the business. NOTE: The manufacturer recommends that this be set to FALSE (the default) to ensure the Database Administrators and OS System Administrators maintain an appropriate degree of segregation/separation of duties.

This String value X indicates whether or not database roles have been separated from operating system roles within the init.ora file. A value of FALSE shows that database roles have been separated from OS roles. A value of TRUE shows that database roles have not been separated from OS roles.

Expected	**regular expression match**
	FALSE
	OR, any of the selected values below:
	☑ Parameter: OS_ROLES not found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	FALSE

Extended Evidence:

NAME	VALUE
os_roles	FALSE
os_roles	FALSE
os_roles	FALSE

(1.74) 101064 Status of instance configuration (alter database / alter system) are captured in the security events(oracle19:1:1621:POHK1API_DG2) — Passed — HIGH

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

Status of instance configuration (alter database / alter system) are captured in the security events

Status of instance configuration (alter database / alter system) are captured in the security events

Scan Parameters:

DBQUERY: SELECT POLICY_NAME,AUDIT_OPTION ,AUDIT_OPTION_TYPE FROM AUDIT_UNIFIED_POLICIES WHERE AUDIT_OPTION IN ('ALTER DATABASE','ALTER SYSTEM') AND POLICY_NAME in(SELECT POLICY_NAME FROM AUDIT_UNIFIED_ENABLED_POLICIES)

Expected **matches regular expression list**

DB Column Name: AUDIT_OPTION

.*

OR, any of the selected values below:

Set status to PASS if no data found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE
SCB_AUDIT_DDL_POLICY	ALTER DATABASE	SYSTEM PRIVILEGE
SCB_AUDIT_DDL_POLICY	ALTER SYSTEM	SYSTEM PRIVILEGE

Extended Evidence:

Statistics:

Query returned 2 rows

2. TIP 3.0

(2.1) 101311 Ensure all Users are authenticated before access to an information System(IAM-340) (oracle19:1:1621:POHK1API_DG2) Passed MEDIUM

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

select distinct AUTHENTICATION_TYPE from cdb_users where AUTHENTICATION_TYPE not in ('NONE') and username not in('ORARO','PUPPETAM')

Ensure all Users are authenticated before access to an information System(IAM-340)

Scan Parameters:

DBQUERY: select distinct AUTHENTICATION_TYPE from cdb_users where AUTHENTICATION_TYPE not in ('NONE') and username not in('ORARO', 'PUPPETAM')

Expected **is contained in regular expression list**

DB Column Name: AUTHENTICATION_TYPE

^PASSWORD$

OR, any of the selected values below:

Set status to PASS if no data found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

AUTHENTICATION_TYPE
PASSWORD

Extended Evidence:

Statistics:

Query returned 1 rows

(2.2) 101319 Status of 'DBA_%' granted to grantees (direct and indirect grants)(CIS-43) (oracle19:1:1621:POHK1API_DG2) Passed HIGH

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Status of 'DBA_%' granted to grantees (direct and indirect grants)(CIS-43)

Status of 'DBA_%' granted to grantees (direct and indirect grants)(CIS-43)

Scan Parameters:

DBQUERY: SELECT GRANTEE,TABLE_NAME FROM DBA_TAB_PRIVS A WHERE TABLE_NAME LIKE 'DBA_%' AND OWNER = 'SYS' AND GRANTEE NOT IN (SELECT USERNAME FROM DBA_USERS WHERE ORACLE_MAINTAINED='Y') AND GRANTEE NOT IN (SELECT ROLE FROM DBA_ROLES WHERE ORACLE_MAINTAINED='Y') AND GRANTEE NOT IN ('CCS_SCAN','SECADMIN','SCB_ADMIN', 'GGADMIN','PUBLIC','DBADDM', 'INFA_META_01', 'INFA_META_02','PUPPETAM','ORDS_ADMIN','ORDS_METADATA') AND GRANTEE NOT like '%CDC%' and GRANTEE not like 'PATROL%' and GRANTEE not like 'APEX%'

Expected **any of the selected values below:**

☑ Set status to PASS if no data found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.3) 101322 Ensure 'DBA_SYS_PRIVS.%' Is Revoked from Unauthorized 'GRANTEE' with 'ADMIN_OPTION'(CIS-46)(oracle19:1:1621:POHK1API_DG2) — Passed — HIGH

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Ensure 'DBA_SYS_PRIVS.%' Is Revoked from Unauthorized 'GRANTEE' with 'ADMIN_OPTION'(CIS-46)

Ensure 'DBA_SYS_PRIVS.%' Is Revoked from Unauthorized 'GRANTEE' with 'ADMIN_OPTION'(CIS-46)

Scan Parameters:

DBQUERY: SELECT GRANTEE, PRIVILEGE,CON_ID
FROM CDB_SYS_PRIVS A WHERE ADMIN_OPTION='YES'
AND GRANTEE NOT IN (SELECT USERNAME FROM CDB_USERS WHERE ORACLE_MAINTAINED='Y')
AND GRANTEE NOT IN (SELECT ROLE FROM CDB_ROLES WHERE ORACLE_MAINTAINED='Y')
AND GRANTEE NOT IN ('CCS_SCAN','SECADMIN','ORAMED1','GGADMIN','SCB_ADMIN','AOGEMS','DBAID','DBADDM','OEMUSER', 'SCB_LINK', 'ORACLE', 'ORAMED2', 'PATROL','PUPPETAM','ORDS_ADMIN')

Expected **any of the selected values below:**

☑ Set status to PASS if no data found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.4) 101323 Ensure 'EXEMPT ACCESS POLICY' Is Revoked from Unauthorized 'GRANTEE'(CIS-52) (oracle19:1:1621:POHK1API_DG2) — Passed — HIGH

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Ensure 'EXEMPT ACCESS POLICY' Is Revoked from Unauthorized 'GRANTEE'(CIS-52)

Ensure 'EXEMPT ACCESS POLICY' Is Revoked from Unauthorized 'GRANTEE'(CIS-52)

Scan Parameters:

DBQUERY: SELECT GRANTEE, PRIVILEGE,CON_ID
FROM CDB_SYS_PRIVS A WHERE PRIVILEGE='EXEMPT ACCESS POLICY'
AND GRANTEE NOT IN (SELECT USERNAME FROM CDB_USERS WHERE ORACLE_MAINTAINED='Y')
AND GRANTEE NOT IN (SELECT ROLE FROM CDB_ROLES WHERE ORACLE_MAINTAINED='Y')
AND GRANTEE NOT IN('SCB_LINK','REPO_OWNER')

Expected **any of the selected values below:**

☑ Set status to PASS if no data found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.5) 101325 Status of '%ANY%' system privilege granted to grantees (direct and indirect grants) (CIS-45)(oracle19:1:1621:POHK1API_DG2) — Failed — HIGH

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Failed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

Status of '%ANY%' system privilege granted to grantees (direct and indirect grants)(CIS-45)

Status of '%ANY%' system privilege granted to grantees (direct and indirect grants)(CIS-45)

Scan Parameters:

DBQUERY:
```
SELECT GRANTEE, PRIVILEGE
 FROM DBA_SYS_PRIVS
 WHERE PRIVILEGE LIKE '%ANY%'
 AND GRANTEE NOT IN (SELECT USERNAME FROM DBA_USERS WHERE
 ORACLE_MAINTAINED='Y')
 AND GRANTEE NOT IN (SELECT ROLE FROM DBA_ROLES WHERE ORACLE_MAINTAINED='Y')
 AND GRANTEE NOT IN ('CCS_SCAN','SECADMIN','DBARO','ORARO','DBARO2','ORAMED1','GGADMIN','SCB_ADMIN',
 'SCB_LINK', 'ORACLE', 'ORAMED2', 'PATROL', 'SPATIAL_CSW_ADMIN_USR','SPATIAL_WFS_ADMIN_USR','PUPPETAM',
'HCVPWDMANID_ROOT', 'HCVPWDMANID','ORDS_ADMIN') and GRANTEE not like
 '%CDC%' and GRANTEE not like 'GGADM%' and GRANTEE not like 'PATROL%' and GRANTEE not like 'APEX%' and GRANTEE not
 like 'GGMON%' and GRANTEE not like 'PERF%' and GRANTEE not like 'SCB_PERFSTAT%' and GRANTEE not like 'SPLEX%' and GRANTEE
not like 'SQLT%' and GRANTEE not like '%SYSADM%'
```

Expected — **any of the selected values below:**

☑ Set status to PASS if no data found

Actual — **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

GRANTEE	PRIVILEGE
CC_ITRS	SELECT ANY DICTIONARY

Extended Evidence:

Statistics:

Query returned 1 rows

(2.6) 101326 Status of username and account status granted SELECT ANY TABLE privilege(CIS-50) (oracle19:1:1621:POHK1API_DG2) — Passed — HIGH

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

Status of username and account status granted SELECT ANY TABLE privilege(CIS-50)

Status of username and account status granted SELECT ANY TABLE privilege(CIS-50)

Scan Parameters:

DBQUERY:
```
SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS
WHERE PRIVILEGE='SELECT ANY TABLE' AND GRANTEE NOT IN (SELECT USERNAME FROM DBA_USERS WHERE
ORACLE_MAINTAINED='Y') AND GRANTEE NOT IN (SELECT ROLE FROM DBA_ROLES WHERE ORACLE_MAINTAINED='Y')
AND GRANTEE NOT IN  ('CCS_SCAN','SECADMIN','DBARO','ORARO','DBARO2','ORAMED1','GGADMIN','SCB_ADMIN', 'SCB_LINK',
'ORACLE', 'ORAMED2',  'PATROL','PUPPETAM','ORDS_ADMIN') and GRANTEE not like '%CDC%' and GRANTEE not like 'GGADM%' and
GRANTEE not like 'PATROL%' and GRANTEE not like 'APEX%' and GRANTEE not like 'GGMON%' and GRANTEE not like 'PERF_MON%'
and GRANTEE not like 'SCB_PERFSTAT%' and GRANTEE not like 'SPLEX%' and GRANTEE  not like  'SQLT%' and GRANTEE not like
'AOGEM%'
```

Expected — **any of the selected values below:**

☑ Set status to PASS if no data found

Actual — **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.7) 101334 Status of the 'execute any procedure' privilege for user DBSNMP(oracle19:1:1621:POHK1API_DG2) — Passed — HIGH

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

Status of the 'execute any procedure' privilege for user DBSNMP

Status of the 'execute any procedure' privilege for user DBSNMP

Scan Parameters:

DBQUERY: SELECT GRANTEE, PRIVILEGE, CON_ID
FROM CDB_SYS_PRIVS A WHERE PRIVILEGE='EXECUTE ANY PROCEDURE' AND GRANTEE='DBSNMP'

Expected **any of the selected values below:**

☑ Set status to PASS if no data found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.8) 101332 Status of the FAILED_LOGIN_ATTEMPTS resource parameter set in all Oracle profiles (oracle19:1:1621:POHK1API_DG2) — Passed — HIGH

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

Status of the FAILED_LOGIN_ATTEMPTS resource parameter set in all Oracle profiles_12210

Status of the FAILED_LOGIN_ATTEMPTS resource parameter set in all Oracle profiles_12210

Scan Parameters:

DBQUERY: select distinct profile||':'||limit from cdb_profiles where con_id<>2 and resource_name='FAILED_LOGIN_ATTEMPTS'

Expected **is contained in regular expression list**

DB Column Name: PROFILE||':'||LIMIT
DEFAULT:UNLIMITED$
ORA_STIG_PROFILE:6$
SCB_INFRA_APP.*:UNLIMITED$
SCB_INFRA_SUPP.*:3$
SCB_STATIC_APP.*:UNLIMITED$
SCB_SUPP.*:3$
MGMT_ADMIN_USER_PROFILE:10$
MGMT_INTERNAL_USER_PROFILE:UNLIMITED$

OR, any of the selected values below:

☐ Set status to PASS if no data found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

PROFILE||':'||LIMIT
ORA_STIG_PROFILE:6
SCB_INFRA_SUPP:3
SCB_STATIC_APP:UNLIMITED
SCB_SUPP:3
DEFAULT:UNLIMITED
SCB_STATIC_APP_PSS:UNLIMITED
SCB_STATIC_APP_ATX:UNLIMITED
SCB_INFRA_APP:UNLIMITED

Extended Evidence:

Statistics:

Query returned 8 rows

(2.9) 101336 Status of the login & logoff security events for administrators_SLM-010 (oracle19:1:1621:POHK1API_DG2) — Passed — HIGH

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

Status of the login & logoff security events for administrators_SLM-010

Status of the login & logoff security events for administrators_SLM-010

Scan Parameters:

DBQUERY: SELECT POLICY_NAME,AUDIT_OPTION ,AUDIT_OPTION_TYPE FROM AUDIT_UNIFIED_POLICIES WHERE POLICY_NAME IN(SELECT POLICY_NAME FROM AUDIT_UNIFIED_ENABLED_POLICIES) AND AUDIT_OPTION NOT IN('LOGON','LOGOFF')

Expected

matches regular expression list

DB Column Name: POLICY_NAME

.*

OR, any of the selected values below:

☐ Set status to PASS if no data found

Actual

Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE
SCB_AUDIT_DDL_POLICY	ADMINISTER DATABASE TRIGGER	SYSTEM PRIVILEGE
SCB_AUDIT_DDL_POLICY	ALTER DATABASE	SYSTEM PRIVILEGE
SCB_AUDIT_DDL_POLICY	ALTER SYSTEM	SYSTEM PRIVILEGE
SCB_AUDIT_DDL_POLICY	CREATE TABLE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	CREATE INDEX	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	DROP INDEX	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	ALTER INDEX	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	CREATE SEQUENCE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	ALTER SEQUENCE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	ALTER TABLE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	DROP SEQUENCE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	CREATE SYNONYM	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	DROP SYNONYM	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	CREATE VIEW	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	DROP VIEW	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	CREATE PROCEDURE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	ALTER PROCEDURE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	CREATE DATABASE LINK	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	DROP DATABASE LINK	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	ALTER USER	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	CREATE USER	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	CREATE ROLE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	DROP USER	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	DROP ROLE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	CREATE TRIGGER	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	ALTER TRIGGER	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	DROP TRIGGER	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	CREATE PROFILE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	DROP PROFILE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	ALTER PROFILE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	DROP PROCEDURE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	CREATE TYPE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	DROP TYPE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	ALTER ROLE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	ALTER TYPE	STANDARD ACTION

	SCB_AUDIT_DDL_POLICY	ALTER VIEW	STANDARD ACTION
	SCB_AUDIT_DDL_POLICY	CREATE FUNCTION	STANDARD ACTION
	SCB_AUDIT_DDL_POLICY	ALTER FUNCTION	STANDARD ACTION
	SCB_AUDIT_DDL_POLICY	DROP FUNCTION	STANDARD ACTION
	SCB_AUDIT_DDL_POLICY	CREATE PACKAGE	STANDARD ACTION
	SCB_AUDIT_DDL_POLICY	ALTER PACKAGE	STANDARD ACTION
	SCB_AUDIT_DDL_POLICY	DROP PACKAGE	STANDARD ACTION
	SCB_AUDIT_DDL_POLICY	CREATE PACKAGE BODY	STANDARD ACTION
	SCB_AUDIT_DDL_POLICY	ALTER PACKAGE BODY	STANDARD ACTION
	SCB_AUDIT_DDL_POLICY	DROP PACKAGE BODY	STANDARD ACTION
	SCB_AUDIT_DDL_POLICY	CREATE DIRECTORY	STANDARD ACTION
	SCB_AUDIT_DDL_POLICY	DROP DIRECTORY	STANDARD ACTION
	SCB_AUDIT_DDL_POLICY	CHANGE PASSWORD	STANDARD ACTION
	SCB_AUDIT_DDL_POLICY	ALTER SYNONYM	STANDARD ACTION
	SCB_AUDIT_DDL_POLICY	ALTER DATABASE LINK	STANDARD ACTION
	SCB_AUDIT_DDL_POLICY	CREATE PLUGGABLE DATABASE	STANDARD ACTION
	SCB_AUDIT_DDL_POLICY	ALTER PLUGGABLE DATABASE	STANDARD ACTION
	SCB_AUDIT_DDL_POLICY	DROP PLUGGABLE DATABASE	STANDARD ACTION
	SCB_AUDIT_DDL_POLICY	CREATE LOCKDOWN PROFILE	STANDARD ACTION
	SCB_AUDIT_DDL_POLICY	DROP LOCKDOWN PROFILE	STANDARD ACTION
	SCB_AUDIT_DDL_POLICY	ALTER LOCKDOWN PROFILE	STANDARD ACTION
	SCB_AUDIT_DDL_POLICY	GRANT	STANDARD ACTION
	SCB_AUDIT_DDL_POLICY	REVOKE	STANDARD ACTION
	SCB_AUDIT_DROP_POLICY	DROP TABLE	STANDARD ACTION
	SCB_AUDIT_DDL_POLICY	ALL	OBJECT ACTION

Extended Evidence:

Statistics:

Query returned 60 rows

(2.10) 101339 Status of the PASSWORD_LOCK_TIME resource parameter set in all Oracle profiles (oracle19:1:1621:POHK1API_DG2) — Passed — HIGH

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Status of the PASSWORD_LOCK_TIME resource parameter set in all Oracle profiles

Status of the PASSWORD_LOCK_TIME resource parameter set in all Oracle profiles

Scan Parameters:

DBQUERY: select distinct profile||':'||limit from cdb_profiles where con_id<>2 and resource_name='PASSWORD_LOCK_TIME'

Expected **is contained in regular expression list**

DB Column Name: PROFILE||':'||LIMIT
DEFAULT:UNLIMITED$
ORA_STIG_PROFILE:UNLIMITED$
SCB_INFRA_APP.*:UNLIMITED$
SCB_INFRA_SUPP.*:UNLIMITED$
SCB_STATIC_APP.*:UNLIMITED$
SCB_SUPP.*:UNLIMITED$
MGMT_ADMIN_USER_PROFILE:1$
MGMT_INTERNAL_USER_PROFILE:UNLIMITED$

OR, any of the selected values below:

☐ Set status to PASS if no data found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

PROFILE||':'||LIMIT
ORA_STIG_PROFILE:UNLIMITED
SCB_SUPP:UNLIMITED
SCB_INFRA_SUPP:UNLIMITED
SCB_STATIC_APP:UNLIMITED
DEFAULT:UNLIMITED
SCB_STATIC_APP_PSS:UNLIMITED
SCB_STATIC_APP_ATX:UNLIMITED
SCB_INFRA_APP:UNLIMITED

Extended Evidence:

Statistics:

Query returned 8 rows

(2.11) 101340 Status of the PASSWORD_LIFE_TIME resource parameter set in all Oracle profiles (oracle19:1:1621:POHK1API_DG2) — Passed — HIGH

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Status of the PASSWORD_LIFE_TIME resource parameter set in all Oracle profiles

Status of the PASSWORD_LIFE_TIME resource parameter set in all Oracle profiles

Scan Parameters:

DBQUERY: select distinct profile||':'||limit from cdb_profiles where con_id<>2 and resource_name='PASSWORD_LIFE_TIME'

Expected **is contained in regular expression list**

DB Column Name: PROFILE||':'||LIMIT
DEFAULT:UNLIMITED$
ORA_STIG_PROFILE:83$
SCB_INFRA_APP.*:UNLIMITED$
SCB_INFRA_SUPP.*:83$
SCB_STATIC_APP.*:UNLIMITED$
MGMT_ADMIN_USER_PROFILE:180$
MGMT_INTERNAL_USER_PROFILE:UNLIMITED$
SCB_SUPP.*:83$

OR, any of the selected values below:

☐ Set status to PASS if no data found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

PROFILE||':'||LIMIT
SCB_SUPP:83
ORA_STIG_PROFILE:83
SCB_STATIC_APP:UNLIMITED
DEFAULT:UNLIMITED
SCB_INFRA_SUPP:83
SCB_STATIC_APP_PSS:UNLIMITED
SCB_STATIC_APP_ATX:UNLIMITED
SCB_INFRA_APP:UNLIMITED

Extended Evidence:

Statistics:

Query returned 8 rows

(2.12) 101341 Status of the PASSWORD_REUSE_MAX resource parameter set in all Oracle profiles (oracle19:1:1621:POHK1API_DG2) — Passed — HIGH

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Status of the PASSWORD_REUSE_MAX resource parameter set in all Oracle profiles_12209

Status of the PASSWORD_REUSE_MAX resource parameter set in all Oracle profiles_12209

Scan Parameters:

DBQUERY: select distinct profile||':'||limit from cdb_profiles where con_id<>2 and resource_name='PASSWORD_REUSE_MAX'

Expected **is contained in regular expression list**

DB Column Name: PROFILE||':'||LIMIT
DEFAULT:UNLIMITED$
ORA_STIG_PROFILE:20$
SCB_INFRA_APP.*:UNLIMITED$
SCB_INFRA_SUPP.*:20$
SCB_STATIC_APP.*:UNLIMITED$
SCB_SUPP.*:20$
MGMT_ADMIN_USER_PROFILE:UNLIMITED$
MGMT_INTERNAL_USER_PROFILE:UNLIMITED$

OR, any of the selected values below:

☐ Set status to PASS if no data found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

PROFILE||':'||LIMIT
DEFAULT:UNLIMITED
SCB_INFRA_SUPP:20
SCB_STATIC_APP_PSS:UNLIMITED
SCB_STATIC_APP_ATX:UNLIMITED
SCB_INFRA_APP:UNLIMITED
SCB_STATIC_APP:UNLIMITED
ORA_STIG_PROFILE:20
SCB_SUPP:20

Extended Evidence:

Statistics:

Query returned 8 rows

(2.13) 101342 Status of the PASSWORD_REUSE_TIME resource parameter set in all Oracle profiles (oracle19:1:1621:POHK1API_DG2) — Passed — HIGH

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Status of the PASSWORD_REUSE_TIME resource parameter set in all Oracle profiles

Status of the PASSWORD_REUSE_TIME resource parameter set in all Oracle profiles

Scan Parameters:

DBQUERY: select distinct profile||':'||limit from cdb_profiles where con_id<>2 and resource_name='PASSWORD_REUSE_TIME'

Expected **is contained in regular expression list**

DB Column Name: PROFILE||':'||LIMIT
DEFAULT:UNLIMITED$
ORA_STIG_PROFILE:UNLIMITED$
SCB_STATIC_APP.*:UNLIMITED$
SCB_INFRA_APP.*:UNLIMITED$
SCB_INFRA_SUPP.*:UNLIMITED$
SCB_SUPP.*:UNLIMITED$
MGMT_ADMIN_USER_PROFILE:UNLIMITED$
MGMT_INTERNAL_USER_PROFILE:UNLIMITED$

OR, any of the selected values below:

☐ Set status to PASS if no data found

Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)
	PROFILE||':'||LIMIT
	ORA_STIG_PROFILE:UNLIMITED
	DEFAULT:UNLIMITED
	SCB_STATIC_APP_PSS:UNLIMITED
	SCB_STATIC_APP_ATX:UNLIMITED
	SCB_INFRA_APP:UNLIMITED
	SCB_SUPP:UNLIMITED
	SCB_INFRA_SUPP:UNLIMITED
	SCB_STATIC_APP:UNLIMITED

Extended Evidence:

Statistics:

Query returned 8 rows

(2.14) 101343 Status of the PASSWORD_GRACE_TIME resource parameter set in all Oracle profiles (oracle19:1:1621:POHK1API_DG2) — Passed — MEDIUM

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Status of the PASSWORD_GRACE_TIME resource parameter set in all Oracle profiles

Status of the PASSWORD_GRACE_TIME resource parameter set in all Oracle profiles

Scan Parameters:

DBQUERY: select distinct profile||':'||limit from cdb_profiles where con_id<>2 and resource_name='PASSWORD_GRACE_TIME'

Expected	is contained in regular expression list
	DB Column Name: PROFILE||':'||LIMIT
	DEFAULT:7$
	ORA_STIG_PROFILE:7$
	SCB_INFRA_APP.*:7$
	SCB_INFRA_SUPP.*:7$
	SCB_STATIC_APP.*:7$
	SCB_SUPP.*:7$
	MGMT_ADMIN_USER_PROFILE:7$
	MGMT_INTERNAL_USER_PROFILE:UNLIMITED$
	OR, any of the selected values below:
	☐ Set status to PASS if no data found

Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)
	PROFILE||':'||LIMIT
	SCB_INFRA_APP:7
	SCB_SUPP:7
	SCB_STATIC_APP_ATX:7
	SCB_INFRA_SUPP:7
	DEFAULT:7
	SCB_STATIC_APP:7
	SCB_STATIC_APP_PSS:7
	ORA_STIG_PROFILE:7

Extended Evidence:

Statistics:

Query returned 8 rows

(2.15) 101344 Ensure No Users Are Assigned the 'DEFAULT' Profile_(CIS-32)(oracle19:1:1621: POHK1API_DG2) — Failed — HIGH

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Failed

Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

test_control_101116

test_control_101116

Scan Parameters:

DBQUERY: SELECT A.USERNAME,CON_ID FROM CDB_USERS A WHERE A.PROFILE='DEFAULT' AND A.ACCOUNT_STATUS='OPEN' AND A.ORACLE_MAINTAINED = 'N' and CON_ID<>2

Expected **any of the selected values below:**

☑ Set status to PASS if no data found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

USERNAME	CON_ID
D42ULADM	3

Extended Evidence:

Statistics:

Query returned 1 rows

(2.16) 101345 Ensure 'GRANT ANY OBJECT PRIVILEGE' Is Revoked from Unauthorized 'GRANTEE' (CIS-58)(oracle19:1:1621:POHK1API_DG2) Passed HIGH

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Ensure 'GRANT ANY OBJECT PRIVILEGE' Is Revoked from Unauthorized 'GRANTEE'(CIS-58)

Ensure 'GRANT ANY OBJECT PRIVILEGE' Is Revoked from Unauthorized 'GRANTEE'(CIS-58)

Scan Parameters:

DBQUERY: SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS
WHERE PRIVILEGE='GRANT ANY OBJECT PRIVILEGE' AND GRANTEE NOT IN (SELECT USERNAME FROM DBA_USERS WHERE ORACLE_MAINTAINED='Y') AND GRANTEE NOT IN (SELECT ROLE FROM DBA_ROLES WHERE ORACLE_MAINTAINED='Y')
AND GRANTEE not in ('SECADMIN', 'SCB_ADMIN','PUPPETAM', 'ORDS_ADMIN')

Expected **any of the selected values below:**

☑ Set status to PASS if no data found

Actual **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.17) 101347 Ensure 'GRANT ANY PRIVILEGE' Is Revoked from Unauthorized 'GRANTEE'(CIS-60) (oracle19:1:1621:POHK1API_DG2) Passed HIGH

Instance oracle19:1:1621:POHK1API_DG2
Previous Status Passed
Evaluation Date 08/04/2024 at 10:49:35 PM (GMT+0530)

Ensure 'GRANT ANY PRIVILEGE' Is Revoked from Unauthorized 'GRANTEE'(CIS-60)

Ensure 'GRANT ANY PRIVILEGE' Is Revoked from Unauthorized 'GRANTEE'(CIS-60)_101104

Scan Parameters:

DBQUERY: SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS
WHERE PRIVILEGE='GRANT ANY PRIVILEGE' AND GRANTEE NOT IN (SELECT USERNAME FROM DBA_USERS WHERE ORACLE_MAINTAINED='Y') AND GRANTEE NOT IN (SELECT ROLE FROM DBA_ROLES WHERE ORACLE_MAINTAINED='Y')
AND GRANTEE not in ('SECADMIN', 'SCB_ADMIN','PUPPETAM','HCVPWDMANID_ROOT','HCVPWDMANID')

Expected **any of the selected values below:**

☑ Set status to PASS if no data found

Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.18) 101352 Ensure '_trace_files_public'Is Set to 'FALSE'(oracle19:1:1621:POHK1API_DG2) Passed HIGH

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

Ensure '_trace_files_public'Is Set to 'FALSE'

Ensure '_trace_files_public'Is Set to 'FALSE'

Scan Parameters:

DBQUERY: select name,value from v$system_parameter where name='_trace_files_public';

Expected	**matches regular expression list**
	DB Column Name: VALUE
	FALSE
	OR, any of the selected values below:
	☑ Set status to PASS if no data found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.19) 101354 Ensure password complexity as per standards(oracle19:1:1621:POHK1API_DG2) Passed HIGH

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

password length

password length

Scan Parameters:

DBQUERY: select name,max(instr(text,'ora_complexity_check(password, chars => 25, uppercase => 1, lowercase => 1,digit => 1, special => 1)')) Position from dba_source where
name in(select distinct limit from cdb_profiles where resource_name='PASSWORD_VERIFY_FUNCTION' and limit like 'SCB_19C_PWD_VERIFY_FUNCTION_%' escape '\' and con_id<>2 and limit<>'FROM ROOT')
group by name

Expected	**match all equal to**
	DB Column Name: POSITION
	11
	OR, any of the selected values below:
	☑ Set status to PASS if no data found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.20) 101356 Status of 'DBA' role granted to grantees (roles)(CIS-63)(oracle19:1:1621: POHK1API_DG2) — Passed — HIGH

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

Status of 'DBA' role granted to grantees (roles)(CIS-63)

Status of 'DBA' role granted to grantees (roles)(CIS-63)

Scan Parameters:

DBQUERY:
```
SELECT 'GRANT' AS PATH, GRANTEE, GRANTED_ROLE,CON_ID FROM CDB_ROLE_PRIVS A
WHERE GRANTED_ROLE='DBA' AND GRANTEE NOT IN ('SYS', 'SYSTEM','GGADMIN', 'PDBADMIN', 'AOGEMS_DBA', 'DBSNMP',
'HCVPWDMANID_ROOT')
UNION
SELECT 'PROXY', PROXY || '-' || CLIENT, 'DBA',CON_ID FROM CDB_PROXIES A
WHERE CLIENT IN (SELECT GRANTEE FROM CDB_ROLE_PRIVS B WHERE GRANTED_ROLE = 'DBA' AND A.CON_ID = B.CON_ID)
```

Expected — **any of the selected values below:**

☑ Set status to PASS if no data found

Actual — **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.21) 101361 Ensure 'GRANT ANY ROLE' Is Revoked from Unauthorized 'GRANTEE'(CIS-59) (oracle19:1:1621:POHK1API_DG2) — Passed — HIGH

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

Ensure 'GRANT ANY ROLE' Is Revoked from Unauthorized 'GRANTEE'(CIS-59)

Ensure 'GRANT ANY ROLE' Is Revoked from Unauthorized 'GRANTEE'(CIS-59)

Scan Parameters:

DBQUERY:
```
SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS
WHERE PRIVILEGE='GRANT ANY ROLE' AND GRANTEE NOT IN (SELECT USERNAME FROM DBA_USERS WHERE
ORACLE_MAINTAINED='Y') AND GRANTEE NOT IN (SELECT ROLE FROM DBA_ROLES WHERE ORACLE_MAINTAINED='Y')
AND GRANTEE not in ('SECADMIN', 'SCB_ADMIN', 'SPATIAL_WFS_ADMIN_USR','SPATIAL_CSW_ADMIN_USR','PUPPETAM',
'HCVPWDMANID_ROOT','HCVPWDMANID')
```

Expected — **any of the selected values below:**

☑ Set status to PASS if no data found

Actual — **Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.22) 101367 Ensure 'ALL' Is Revoked on 'Sensitive' Tables(CIS-44)(oracle19:1:1621: POHK1API_DG2) — Passed — HIGH

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

Ensure 'ALL' Is Revoked on 'Sensitive' Tables(CIS-44)

Ensure 'ALL' Is Revoked on 'Sensitive' Tables(CIS-44)

Scan Parameters:

DBQUERY:
```
SELECT TABLE_NAME, PRIVILEGE, GRANTEE,CON_ID
FROM CDB_TAB_PRIVS WHERE GRANTEE IN (SELECT USERNAME FROM CDB_USERS WHERE ORACLE_MAINTAINED='Y')
AND TABLE_NAME IN (SELECT TABLE_NAME FROM CDB_TABLES WHERE OWNER='SYS' AND TABLE_NAME LIKE '%SEC%'
OR TABLE_NAME LIKE '%AUDIT%' OR TABLE_NAME LIKE '%PWD%' OR TABLE_NAME IN ('USERS', 'USER_HISTORY', 'SAVEPOINTS')
AND OWNER= 'SYS'
AND GRANTEE NOT IN (SELECT USERNAME FROM DBA_USERS WHERE
ORACLE_MAINTAINED='Y')
AND GRANTEE NOT IN (SELECT ROLE FROM DBA_ROLES WHERE ORACLE_MAINTAINED='Y')
AND GRANTEE NOT IN ('CCS_SCAN','SCB_ADMIN') and GRANTEE not like 'PATROL%' and GRANTEE not like 'SCIDC%'
```

Expected	**any of the selected values below:**
	☑ Set status to PASS if no data found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.23) 101337 Status of DB admin audit options_SLM-010(oracle19:1:1621:POHK1API_DG2) Passed MEDIUM

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

Status of DB admin audit options_11g&below_SLM-010

Status of DB admin audit options_11g&below_SLM-010

Scan Parameters:

DBQUERY: SELECT POLICY_NAME FROM AUDIT_UNIFIED_ENABLED_POLICIES WHERE FAILURE ='YES'

Expected	**contains regular expression list**
	DB Column Name: POLICY_NAME ^SCB_AUDIT_DDL_POLICY$ ^SCB_AUDIT_DROP_POLICY$ ^SCB_LOGON_ALL_FAILURES$ ^SCB_LOGON_LOGOFF_PRIVUSER$
	OR, any of the selected values below:
	☐ Set status to PASS if no data found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**

POLICY_NAME
SCB_LOGON_LOGOFF_PRIVUSER
SCB_LOGON_ALL_FAILURES
SCB_AUDIT_DDL_POLICY
SCB_AUDIT_DROP_POLICY

Extended Evidence:

Statistics:

Query returned 4 rows

(2.24) 101366 Ensure secure encryption standards are configured(oracle19:1:1621:POHK1API_DG2) Passed MEDIUM

Instance	oracle19:1:1621:POHK1API_DG2
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:49:35 PM (GMT+0530)

Ensure secure encryption standards are configured

Ensure secure encryption standards are configured

Scan Parameters:

DBQUERY: select network_service_banner from v$session_connect_info where sid=(select sid from v$mystat where rownum = 1) and network_service_banner like '%AES256%'

Expected	**contains regular expression list**
	DB Column Name: NETWORK_SERVICE_BANNER AES256
	OR, any of the selected values below:
	☐ Set status to PASS if no data found

Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	NETWORK_SERVICE_BANNER
	AES256 Encryption service adapter for Linux: Version 19.0.1.0.0 - Production

Extended Evidence:

Statistics:

Query returned 1 rows

10.21.199.153 (hklpdss2b003.hk.standardchartered.com) - cpe:/o:redhat:enterprise_linux:7.9::server:

Controls:	196
Passed:	180 (91.84%)
Failed:	16 (8.16%)
Error:	0
Approved Exceptions:	0
Pending Exceptions:	0
Last Scan Date:	08/06/2024 at 07:06:38 AM (GMT+0530)
Tracking Method:	IP
Qualys Host ID:	-

Asset Tags:
ALL ASSET GROUPS, Vulnerability Management, Engineering Build, Internal Asset, CLOUD POC, SUBNET-HONG KONG, Oracle PC - AG, Policy Compliance - OS SAT/CCM, ICV-Scan-OS- HK1, Production Support, AG_SelfService, SVLM, Metrics Internal Facing IPs, ESC ATM, Test CCM Scan Key update - UNIX, ZINT-SERVER-INVENTORY-ALL, ALL_STATUS_HONG_KONG_PROD, 2021 Q1 Validation Internal, ICV-OS-Red Hat Enterprise Linux, RBI DB Cindy 2021, SGF total IP scanned of the month, MAP_HK 2/3, temp-all-server2, 2021 Q4 Validation Internal, Dec_2021_CDC_GDC_NC_Scanned, Jan_2022_CDC_GDC_NC_Scanned, Feb_2022_CDC_GDC_NC_Scanned, 2022 Q1 Validation Internal, Total IP scanned for the month of Feb 2022, Mar_2022_CDC_GDC_NC_Scanned, SGF IP not scanned of the month, Apr_2022_CDC_GDC_NC_Scanned, May_2022_GDC_CDC_NC_scanned, 2022 Q2 Validation Internal, Jun_2022_GDC_CDC_NC_scanned, Jul_2022_GDC_CDC_NC_scanned, 2022 Q3 Validation Internal, Aug_2022_GDC_CDC_NC_scanned, Sep_2022_GDC_CDC_NC_scanned, OpenSSL-Asia-Prod, Nov_2022_GDC_CDC_NC_scanned, 2022 Q4 Validation Internal, Purge Activity, Jan_2023_CDC_GDC_NC_Scanned, Feb_2023_CDC_GDC_NC_Scanned, Self_Service_AG_UM, 2023 Q1 Validation Internal, Mar_2023_CDC_GDC_NC_Scanned, Apr_2023_CDC_GDC_NC_Scanned, AG-ICV Scans-OS_Web [HK - Begins with 10.21.1], Database_Group, Anantha-HK, May_2023_CDC_GDC_NC_Scanned, 2023 Q2 Validation Internal, Jun_2023_CDC_GDC_NC_Scanned, Sep_2023_CDC_GDC_NC_Scanned, Oct_2023_CDC_GDC_NC_Scanned, 2023 Q4 Validation Internal, Nov_2023_CDC_GDC_NC_Scanned, JAN_2024_GDC_EAST, Jan_2024_CDC_GDC_NC_Scanned, FEB_2024_GDC_EAST, Feb_2024_CDC_GDC_NC_Scanned, MAR_2024_GDC_EAST, 2024 Q1 Validation Internal, Mar_2024_CDC_GDC_NC_Scanned, APR_2024_GDC_EAST, April_2024_CDC_GDC_NC_Scanned, MAY_2024_GDC_EAST, May_2024_CDC_GDC_NC_Scanned, 2024 Q2 Validation Internal, JUN_2024_GDC_EAST, Jun_2024_CDC_GDC_NC_Scanned, JUL_2024_GDC_EAST, July_2024_CDC_GDC_NC_Scanned

Oracle 19c

1. Database Controls

(1.1) 1049 Status of the 'remote_os_authent(remote OS authentication without password)' setting via SQL query(oracle19:1:1621:POHK1CAT_DG.hk.standardchartered.com) **Passed** **HIGH**

Instance	oracle19:1:1621:POHK1CAT_DG.hk.standardchartered.com
Previous Status	Passed
Evaluation Date	08/04/2024 at 10:03:13 PM (GMT+0530)

The 'REMOTE_OS_AUTHENT=TRUE' setting in the 'init.ora' file allows a connection to be made to the database instance as a specific user via OS-based, rather than database-local authentication. Oracle allows this connection, assuming the user was authenticated by the remote OS. This capability could allow a malicious user to impersonate another when OS credentials have been compromised. When this is set to FALSE (as recommended by the manufacturer), remote user connections will not be allowed without database-local credentials.

The String value X indicates the current state of the remote_os_authent setting in init.ora (remote OS authentication without password). Prohibiting such connections require the value to be FALSE.

Expected	**regular expression match**
	FALSE
	OR, any of the selected values below:
	☑ Parameter: REMOTE_OS_AUTHENT not found
Actual	**Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)**
	FALSE