Extended Evidence:

Statistics:

Query returned 4 rows

(2.24) 101366 Ensure secure encryption standards are configured(oracle19:1:1621:POHK1TBL) Passed MEDIUM

Instance oracle19:1:1621:POHK1TBL

Previous Status Passed

Evaluation Date 08/04/2024 at 09:54:11 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

10.21.199.138 (hklpdps2b001.hk.standardchartered.com)

Red Hat Enterprise Linux Server 7.9 cpe:/o:redhat: enterprise_linux:7.9::server:

Controls:	784
Passed:	709 (90.43%)
Failed:	75 (9.57%)
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, JAN_2021_ALL_STATUS_HONG_KONG_NON-PROD, ALL_STATUS_HONG_KONG_NON-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, 2021 Q3 Validation Internal, 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, In Scope Asset Groups, OpenSSL-Asia-Prod, Nov_2022_GDC_CDC_NC_scanned, 2022 Q4 Validation Internal, 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, Peb_2023_CDC_GDC_NC_Scanned, Self_Service_AG_UM, 2023 Q1 Validation Internal, Mar_2023_CDC_GDC_NC_Scanned, 2023 Q2 Validation Internal, Jun_2023_CDC_GDC_NC_Scanned, Self_Service_AG_UM, 2023 Q1 Validation Internal, Jun_2023_CDC_GDC_NC_Scanned, Self_Service_AG_UM, 2023_CDC_GDC_NC_Scanned, Self_Service_AG_UM, 2023_CDC_GDC_NC_Scanned, Self_Service_AG_UM, 2023_CDC_GDC_NC_Scanned, Self_Service_AG_UM, 2023_CDC_GDC_NC_Scanned, Self_Service_AG_UM, 2024_GDC_EAST, Jan_2024_CDC_GDC_NC_Scanned, Self_Service_AG_UM, 2024_GDC_EAST, Jan_2024_CD

Oracle 19c

(1.1) 1049 Status of the 'remote_os_authent(remote OS authentication without password)' setting Passed HIGH via SQL query(oracle19:1:1621:POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 I	Evidence:	
NAME	VALUE	
remote_os_authent		FALSE
remote_os_authent		FALSE
remote os authent		FAISE

(1.1) 1049 Status of the 'remote_os_authent(remote OS authentication without password)' setting Passed HIGH via SQL query(oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

Such connections require the value to be PALSE.			
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 E	Extended Evidence:		
NAME	VALUE		
remote_os_authent		FALSE	
remote_os_authent		FALSE	
remote_os_authent FALSE		FALSE	

(1.1) 1049 Status of the 'remote_os_authent(remote OS authentication without password)' setting Passed HIGH via SQL query(oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

outh connections require the value to be tribbe.		
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 E	Evidence:	
NAME	VALUE	
remote_os_authent		FALSE
remote_os_authent		FALSE
remote_os_authent		FALSE

(1.1) 1049 Status of the 'remote_os_authent(remote OS authentication without password)' setting Passed HIGH via SQL query(oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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+05	530)
	FALSE	
Extended E	Extended Evidence:	
NAME		VALUE
remote_os_authent		FALSE
remote_os_authent		FALSE
remote_os_authent FALSE		FALSE

(1.1) 1049 Status of the 'remote_os_authent(remote OS authentication without password)' setting Passed HIGH via SQL query(oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	ted 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 E	Extended Evidence:		
NAME		VALUE	
remote_os_authent		FALSE	
remote_os_authent		FALSE	
remote_os_authent		FALSE	

(1.1) 1049 Status of the 'remote_os_authent(remote OS authentication without password)' setting Passed HIGH via SQL query(oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 E	Extended Evidence:		
NAME	VALUE		
remote_os_authent		FALSE	
remote_os_authent		FALSE	
remote_os_authent		FALSE	

(1.1) 1049 Status of the 'remote_os_authent(remote OS authentication without password)' setting Passed HIGH via SQL query(oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	

(1.1) 1049 Status of the 'remote_os_authent(remote OS authentication without password)' setting Passed HIGH via SQL query(oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

Evnoctod	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:

Exterior 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.hk. Passed HIGH standardchartered.com)

Instance oracle 19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

such connections are not permitted, the value should be FALSE. Expected regular expression match

OD any of the colected values helevy

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 E	Extended Evidence:	
NAME		VALUE
remote_os_roles		FALSE
remote_os_roles		FALSE
remote_os_roles		FALSE

(1.2) 1050 Status of the 'remote_os_roles' setting via SQL query(oracle19:1:1621:POHK3CCD.hk. Passed HIGH standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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+05:	30)
	FALSE	
Extended E	Extended Evidence:	
NAME		VALUE
remote_os_roles		FALSE
remote_os_rc	les	FALSE
remote_os_rc	mote_os_roles FALSE	

(1.2) 1050 Status of the 'remote_os_roles' setting via SQL query(oracle19:1:1621:POHK2CCD.hk. Passed HIGH standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	cted 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 E	Extended Evidence:	
NAME	VALUE	
remote_os_ro	oles	FALSE
remote_os_ro	oles	FALSE

remote_os_roles FALSE

(1.2) 1050 Status of the 'remote_os_roles' setting via SQL query(oracle19:1:1621:POHK1RCT.hk. Passed HIGH standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

regular expression match **Expected 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 FALSE** remote_os_roles **FALSE** remote_os_roles

(1.2) 1050 Status of the 'remote_os_roles' setting via SQL query(oracle19:1:1621:POHK5CCD.hk. Passed HIGH standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 E	Extended Evidence:		
NAME	VALUE		
remote_os_ro	oles	FALSE	
remote_os_ro	note_os_roles FALSE		
remote_os_roles FAI		FALSE	

(1.2) 1050 Status of the 'remote_os_roles' setting via SQL query(oracle19:1:1621:POHK1CAT.hk. Passed HIGH standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(1.2) 1050 Status of the 'remote_os_roles' setting via SQL query(oracle19:1:1621:POHK4CCD.hk. Passed HIGH standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(1.2) 1050 Status of the 'remote_os_roles' setting via SQL query(oracle19:1:1621:POHK1CCD.hk. Passed HIGH standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.hk.standardchartered.com)

Passed HIGH

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

Should be The Lit this face been see.			
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)		
Actual	. ,		
	TRUE		
Extended Evidence:			
NAME	VALUE		
sql92_securit	ql92_security TRUE		

TRUE

TRUE

(1.3) 1057 Status of the 'sql92_security=' (table-level SELECT privileges) in init.ora Passed HIGH (oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

sql92_security

sql92_security

Evaluation Date 08/04/2024 at 10:38:34 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 E	Extended Evidence:	
NAME	VALUE	
sql92_securit	y	TRUE
sql92_securit	у	TRUE
sal92 securit	V	TRUE

(1.3) 1057 Status of the 'sql92_security=' (table-level SELECT privileges) in init.ora (oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

Passed HIGH

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 E	Evidence:		
NAME	1	/ALUE	
sql92_securi	ty	TRUE	
sql92_securi	ty	TRUE	
sql92_securi	ty	TRUE	

(1.3) 1057 Status of the 'sql92_security=' (table-level SELECT privileges) in init.ora Passed (oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

issed HIGH

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(1.3) 1057 Status of the 'sql92_security=' (table-level SELECT privileges) in init.ora (oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Passed HIGH

HIGH

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 E	Evidence:	
NAME		VALUE
sql92_securi	ty	TRUE
sql92_securi	ty	TRUE
sal92 security		TRUE

(1.3) 1057 Status of the 'sql92_security=' (table-level SELECT privileges) in init.ora Passed (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 E	Extended Evidence:	
NAME	VALUE	
sql92_securit	2_security TRUE	

sql92_security	TRUE
sql92_security	TRUE

(1.3) 1057 Status of the 'sql92_security=' (table-level SELECT privileges) in init.ora (oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

Passed HIGH

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	ted 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	0)
	TRUE	
Extended E	Extended Evidence:	
NAME	7	VALUE
sql92_securit	ty	TRUE
sql92_securit	ty	TRUE
sql92_securit	ty	TRUE

(1.3) 1057 Status of the 'sql92_security=' (table-level SELECT privileges) in init.ora (oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Passed HIGH

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

Should be The 2 if the seen seen		
Expected	regular expression match	
	TRUE	
	OR, any of the selected values below:	
	Parameter: SQL92_SECURITY not found	
Actual	ual Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)	
	TRUE	
Extended E	Extended Evidence:	
NAME		VALUE
sql92_securi	zy	TRUE
sql92_securi	zy	TRUE
sql92_securi	security TRUE	

(1.4) 1067 Status of the 'REMOTE_LOGIN_PASSWORD' setting via SQL query(oracle19:1:1621: Passed HIGH POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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+05	30)
	EXCLUSIVE	
Extended E	Extended Evidence:	
NAME		VALUE
remote_login_passwordfile		EXCLUSIVE
remote_login_passwordfile		EXCLUSIVE
remote login passwordfile		EXCLUSIVE

(1.4) 1067 Status of the 'REMOTE_LOGIN_PASSWORD' setting via SQL query(oracle19:1:1621: Passed HIGH POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

io dibabica.	o district.	
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 I	ktended Evidence:	
NAME		VALUE
remote_logir	n_passwordfile	EXCLUSIVE
remote_logir	n_passwordfile	EXCLUSIVE
remote_login_passwordfile EXCLUSIVE		EXCLUSIVE

(1.4) 1067 Status of the 'REMOTE_LOGIN_PASSWORD' setting via SQL query(oracle19:1:1621: Passed HIGH POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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+05	30)
	EXCLUSIVE	
Extended E	Extended Evidence:	
NAME		VALUE
remote_login	_passwordfile	EXCLUSIVE
remote_login	mote_login_passwordfile EXCLUSIVE	
remote_login_passwordfile EXCLUSIVE		EXCLUSIVE

(1.4) 1067 Status of the 'REMOTE_LOGIN_PASSWORD' setting via SQL query(oracle19:1:1621: Passed HIGH POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 E	Extended Evidence:	
NAME		VALUE
remote_login	_passwordfile	EXCLUSIVE
remote_login	te_login_passwordfile EXCLUSIVE	
remote_login	login_passwordfile EXCLUSIVE	

(1.4) 1067 Status of the 'REMOTE_LOGIN_PASSWORD' setting via SQL query(oracle19:1:1621: Passed HIGH POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	Extended Evidence:	
NAME		VALUE
remote_logi	in_passwordfile	EXCLUSIVE
remote_logi	remote_login_passwordfile	
remote_login_passwordfile EXCLUSIVE		EXCLUSIVE

(1.4) 1067 Status of the 'REMOTE_LOGIN_PASSWORD' setting via SQL query(oracle19:1:1621: Passed HIGH POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 E	Extended Evidence:	
NAME	VALUE	
remote_login_passwordfile EXCLUSIVE		EXCLUSIVE
remote_login	mote_login_passwordfile EXCLUSIVE	
remote_login	ote_login_passwordfile EXCLUSIVE	

(1.4) 1067 Status of the 'REMOTE_LOGIN_PASSWORD' setting via SQL query(oracle19:1:1621: Passed HIGH POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

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)
Actual	Last opdated.00/04/2024 at 00.01.03 i iii (Giii 1 + 00.00)
	EXCLUSIVE

Extended Evidence:	
NAME VALUE	
remote_login_passwordfile	EXCLUSIVE
remote_login_passwordfile EXCLUSIVE	
remote_login_passwordfile	EXCLUSIVE

(1.4) 1067 Status of the 'REMOTE_LOGIN_PASSWORD' setting via SQL query(oracle19:1:1621: Passed HIGH POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

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+05	330)
	EXCLUSIVE	
Extended I	Evidence:	
NAME		VALUE
remote_login_passwordfile		EXCLUSIVE
remote_login_passwordfile		EXCLUSIVE
remote logir	n passwordfile	EXCLUSIVE

(1.5) 3462 Permissions set for the 'ORACLE_HOME/bin' directory(oracle19:1:1621:POHK1API.hk. Passed HIGH standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

returned in ti	ie torni owner.group.uirectory permissions.
Expected	matches regular expression list
	.*(\-\-\-\\-\x \-wx r\-\- r\-x rw\- rwx)(\-\-\-\-\r\-x r\-\- \\-x r\-\-\r\-x).*
	OR, any of the selected values below:
	File not found
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)
	oracle:oinstall:rwxr-xr-x:/u01/app/oracle/product/db/19.7.0.0.Apr2020/bin

(1.5) 3462 Permissions set for the 'ORACLE_HOME/bin' directory(oracle19:1:1621:POHK3CCD.hk. Passed HIGH standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

	The state of the s
Expected	matches regular expression list
	.*(\-\-\-\\-\x \-wx r\-\- r\-x rw\- rwx)(\-\-\-\-\r\-x r\-\- \\-x r\-\-\r\-x).*
	OR, any of the selected values below:
	File not found
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)
Motuui	. ,
	oracle:oinstall:rwxr-xr-x:/u01/app/oracle/product/db/19.7.0.0.Apr2020/bin

(1.5) 3462 Permissions set for the 'ORACLE_HOME/bin' directory(oracle19:1:1621:POHK2CCD.hk. Passed HIGH standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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
	.*(\-\-\-\-\-\r\-x r\-\- r\-x r\-\- r\-x r\-\- r\-x r\-\- r\-x r\-\- r\-x .*
	OR, any of the selected values below:
	File not found
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)
	oracle:oinstall:rwxr-xr-x:/u01/app/oracle/product/db/19.7.0.0.Apr2020/bin

(1.5) 3462 Permissions set for the 'ORACLE_HOME/bin' directory(oracle19:1:1621:POHK1RCT.hk. Passed HIGH standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

returned in th	the form owner.group.directory permissions.
Expected	matches regular expression list
	.*(\-\-\-\-\-\-\r\-x \-wx r\-\- r\-x rw\- r\-x r\-\- r\-x).*
	OR, any of the selected values below:
	File not found
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)
	oracle:oinstall:rwxr-xr-x:/u01/app/oracle/product/db/19.7.0.0.Apr2020/bin

(1.5) 3462 Permissions set for the 'ORACLE_HOME/bin' directory(oracle19:1:1621:POHK5CCD.hk. Passed HIGH standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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
	.*(\-\-\-\-\-\r\-x r\-\- r\-x r\-\-
	OR, any of the selected values below:
	File not found
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)
	oracle:oinstall:rwxr-xr-x:/u01/app/oracle/product/db/19.7.0.0.Apr2020/bin

(1.5) 3462 Permissions set for the 'ORACLE_HOME/bin' directory(oracle19:1:1621:POHK1CAT.hk. Passed HIGH standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 \-wx r\-\- r\-x rw\- rwx)(\-\-\-\-\-\r\-x r\-\-\r\-x r\-\-\r\-x).*
	OR, any of the selected values below:
	File not found
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)
	oracle:oinstall:rwxr-xr-x:/u01/app/oracle/product/db/19.7.0.0.Apr2020/bin

(1.5) 3462 Permissions set for the 'ORACLE_HOME/bin' directory(oracle19:1:1621:POHK4CCD.hk. Passed HIGH standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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
	.*(\-\-\-\\-\wx\r\-\-\r\wx)(\-\-\-\r\x)(\\-\-\r\x).*
	OR, any of the selected values below:
	File not found
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)
	oracle:oinstall:rwxr-xr-x:/u01/app/oracle/product/db/19.7.0.0.Apr2020/bin

(1.5) 3462 Permissions set for the 'ORACLE_HOME/bin' directory(oracle19:1:1621:POHK1CCD.hk. Passed HIGH standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

returned in ti	to form owner. group directory permissions.
Expected	matches regular expression list
	.*(\-\-\-\\-\x \\-wx \r\-\- \r\-x \r\wx)(\-\-\-\\-\x \r\-\-\\-\x \r\-\-\\-\x \r\-\-\-\-\x \r\-\-\-\-\x \r\-\-\
	OR, any of the selected values below:
	File not found
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)
, ioiuu.	
	oracle:oinstall:rwxr-xr-x:/u01/app/oracle/product/db/19.7.0.0.Apr2020/bin

(1.6) 3463 Permissions set for the 'ORACLE_HOME' directory(oracle19:1:1621:POHK1API.hk. Passed HIGH standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

group:directory permissions.	
Expected	matches regular expression list
	.*(\-\-\-\\-\\-\\-\\-\\-\\-\\-\\-\\-\\-\\-
	OR, any of the selected values below:
	File not found
A = (=1	L (Ll (((
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)
	oracle:oinstall:rwxr-xr-x:/u01/app/oracle/product/db/19.7.0.0.Apr2020

(1.6) 3463 Permissions set for the 'ORACLE_HOME' directory(oracle19:1:1621:POHK3CCD.hk. Passed HIGH standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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
	.*(\-\-\-\-\-\r\-\r\-\r\-\r\\r\\r\\r\\r\\r\
	OR, any of the selected values below:
	File not found
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)
	oracle:oinstall:rwxr-xr-x:/u01/app/oracle/product/db/19.7.0.0.Apr2020

(1.6) 3463 Permissions set for the 'ORACLE_HOME' directory(oracle19:1:1621:POHK2CCD.hk. Passed HIGH standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

 $.*(\-\-|\-\x|r\-\-|r\-x|r\-\-|r\-x|r\-\-|r\-x|r\-\-|r\-x|r\-\-|r\-x|.*$ OR, any of the selected values below:

File not found

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

oracle:oinstall:rwxr-xr-x:/u01/app/oracle/product/db/19.7.0.0.Apr2020

(1.6) 3463 Permissions set for the 'ORACLE_HOME' directory(oracle19:1:1621:POHK1RCT.hk. Passed HIGH standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

OR, any of the selected values below:

File not found

Actual

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

oracle:oinstall:rwxr-xr-x:/u01/app/oracle/product/db/19.7.0.0.Apr2020

(1.6) 3463 Permissions set for the 'ORACLE_HOME' directory(oracle19:1:1621:POHK5CCD.hk. Passed HIGH standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

(1.6) 3463 Permissions set for the 'ORACLE_HOME' directory(oracle19:1:1621:POHK1CAT.hk. Passed HIGH standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

File not found

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

oracle:oinstall:rwxr-xr-x:/u01/app/oracle/product/db/19.7.0.0.Apr2020

(1.6) 3463 Permissions set for the 'ORACLE_HOME' directory(oracle19:1:1621:POHK4CCD.hk. Passed HIGH standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

OR, any of the selected values below:

File not found

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

oracle:oinstall:rwxr-xr-x:/u01/app/oracle/product/db/19.7.0.0.Apr2020

(1.6) 3463 Permissions set for the 'ORACLE_HOME' directory(oracle19:1:1621:POHK1CCD.hk. Passed HIGH standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

Si oup.un ceto.	y permissions.
Expected	matches regular expression list
	<u>*(\-\-\-\\-wx r\-\- r\-x rw\- r\-x rw\- r\-x r\-\- r\-x).*</u>
	OR, any of the selected values below:
	File not found
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)
	oracle:oinstall:rwxr-xr-x:/u01/app/oracle/product/db/19.7.0.0.Apr2020

(1.7) 3498 Status of the 'SEC_USER_AUDIT_ACTION_BANNER' parameter in sqlnet.ora (oracle19:1:1621:POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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.

MEDIUM

Failed

The followin	g List String value(s) X indicate the fi	le and path defined for the SEC_USER_AUDIT_A	CTION_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	L and I in data de 00/04/2024 at 0	C-04-00 DM (CMT-0520)	
Actual	Last Updated:08/04/2024 at 0	6:01:09 PM (GMT+0530)	
	File not found		
Extended Evidence:			
File name		Setting	Value
/u01/app/grid/product/12cR2/network/admin/ SE sqlnet.ora		SEC_USER_AUDIT_ACTION_BANNER	

Cause of Failure:

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

(1.7) 3498 Status of the 'SEC_USER_AUDIT_ACTION_BANNER' parameter in sqlnet.ora Failed MEDIUM (oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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 fi	le and path defined for the SEC_USER_AUDIT_ACT	ION_BANNER parameter in the sqlnet.ora file.
Expected	does not contain regular exp	ression list	
	NULL		
	OR, any of the selected value	es below:	
	Setting not found		
	File not found		
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)		
	File not found		
Extended Ex	vidence:		
File name		Setting	Value

/u01/app/grid/product/12cR2/network/admin/	SEC_USER_AUDIT_ACTION_BANNER	
sqlnet.ora		

Cause of Failure:

Unexpected
values

Instance

Additional values found in failed controls:

File not found

(1.7) 3498 Status of the 'SEC_USER_AUDIT_ACTION_BANNER' parameter in sqlnet.ora (oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

Failed MEDIUM

oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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:08/04/2024 at 0	6:01:09 PM (GMT+0530)	
710000	File not found	(C (C	
Extended E	vidence:		
File name		Setting	Value
/u01/app/grid/product/12cR2/network/admin/ Salnet ora		SEC_USER_AUDIT_ACTION_BANNER	

Cause of Failure:

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

(1.7) 3498 Status of the 'SEC_USER_AUDIT_ACTION_BANNER' parameter in sqlnet.ora Failed (oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

Failed MEDIUM

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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 value	s below:	
	Setting not found		
	File not found		
Actual	Last Updated:08/04/2024 at 0	6:01:09 PM (GMT+0530)	
	File not found		
Extended Ev	vidence:		
File name		Setting	Value
/u01/app/grid/product/12cR2/network/admin/sqlnet.ora		SEC_USER_AUDIT_ACTION_BANNER	

Cause of Failure:

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

(1.7) 3498 Status of the 'SEC_USER_AUDIT_ACTION_BANNER' parameter in sqlnet.ora Failed MEDIUM (oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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:08/04/2024 at 06:01:09 PM (GMT+0530)

File not found

Extended Evidence:

File name

Setting

Value

/u01/app/grid/product/12cR2/network/admin/
sqlnet.ora

SEC_USER_AUDIT_ACTION_BANNER
sqlnet.ora

Cause of Failure:

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

MEDIUM

(1.7) 3498 Status of the 'SEC_USER_AUDIT_ACTION_BANNER' parameter in sqlnet.ora Passed (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

The sglnet.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 sglnet.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. does not contain regular expression list NULL OR, any of the selected values below: Setting not found File not found Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) **Actual** /u01/app/oracle/local/scripts/BANNER/dbbanner.txt **Extended Evidence:** File name Setting Value /u01/app/oracle/local/network/admin/sqlnet. SEC_USER_AUDIT_ACTION_BANNER /u01/app/oracle/local/scripts/BANNER/ dbbanner.txt ora

3498 Status of the 'SEC USER AUDIT ACTION BANNER' parameter in sqlnet.ora (1.7)(oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

Failed MEDIUM

oracle19:1:1621:POHK4CCD.hk.standardchartered.com Instance

Previous Status

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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 Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) Actual File not found **Extended Evidence:** Value Setting /u01/app/grid/product/12cR2/network/admin/ SEC_USER_AUDIT_ACTION_BANNER sqlnet.ora

Cause of Failure:

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

(1.7) 3498 Status of the 'SEC_USER_AUDIT_ACTION_BANNER' parameter in sqlnet.ora (oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

MEDIUM Failed

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

The sglnet.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 fil	e and path defined for the SEC_USER_AUDIT_ACTI	ON_BANNER parameter in the sqlnet.ora file.
Expected	does not contain regular expression list		
	NULL		
	OR, any of the selected value	es below:	
	Setting not found		
	File not found		
Actual	Last Updated:08/04/2024 at 0	6:01:09 PM (GMT+0530)	
	File not found		
Extended Evidence:			
File name		Setting	Value
/u01/app/grid/product/12cR2/network/admin/sqlnet.ora		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.hk. standardchartered.com)

Passed MEDIUM

oracle19:1:1621:POHK1API.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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 E	vidence:
VALUE	
0	

(1.8) 5601 Status of the RESOURCE_LIMIT parameter(oracle19:1:1621:POHK3CCD.hk. standardchartered.com)

Passed MEDIUM

oracle19:1:1621:POHK3CCD.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 E	vidence:
VALUE	
0	

(1.8) 5601 Status of the RESOURCE_LIMIT parameter(oracle19:1:1621:POHK2CCD.hk. standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:
	<pre>TRUE(0)</pre>
	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 E	vidence:
VALUE	
0	

(1.8) 5601 Status of the RESOURCE_LIMIT parameter(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 10:38:34 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			
(1.8) 5601	Status of the RESOURCE_LIMIT parameter(oracle19:1:1621:POHK5CCD.hk.	Passed	MEDIUM

standardchartered.com)

oracle19:1:1621:POHK5CCD.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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 Ex	vidence:	
VALUE		
0		

(1.8) 5601 Status of the RESOURCE_LIMIT parameter(oracle19:1:1621:POHK1CAT.hk. standardchartered.com)

Passed MEDIUM

Instance oracle 19:1:1621:POHK1CAT.hk. standard chartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 E	vidence:
VALUE	
0	

(1.8) 5601 Status of the RESOURCE_LIMIT parameter(oracle19:1:1621:POHK4CCD.hk. standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 E	vidence:	
VALUE		
0		

(1.8) 5601 Status of the RESOURCE_LIMIT parameter(oracle19:1:1621:POHK1CCD.hk. standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 E	vidence:
VALUE	
0	

(1.9) 5676 Current installed Oracle version(oracle19:1:1621:POHK2CCD.hk.standardchartered. Passed HIGH

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(1.9) 5676 Current installed Oracle version(oracle19:1:1621:POHK1API.hk.standardchartered.com) Passed HIGH

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 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

(1.9) 5676 Current installed Oracle version(oracle19:1:1621:POHK3CCD.hk.standardchartered. Passed HIGH

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 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 E	vidence:
VERSION	
19.2	

(1.9) 5676 Current installed Oracle version(oracle19:1:1621:POHK1RCT.hk.standardchartered. Passed HIGH

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 database version to determine the type of ANSI compliant join syntax used.

The following	List string value(s) A indicates the status of the of the database version to determine the type of Aivsi compilant 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 Ex	vidence:
VERSION	
19.2	

(1.9) 5676 Current installed Oracle version(oracle19:1:1621:POHK5CCD.hk.standardchartered. Passed HIGH com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(1.9) 5676 Current installed Oracle version(oracle19:1:1621:POHK1CAT.hk.standardchartered. Passed

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

HIGH

The following List String value(s) X indicates the status 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

HIGH (1.9) 5676 Current installed Oracle version(oracle19:1:1621:POHK4CCD.hk.standardchartered. **Passed**

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 database version to determine the type of ANSI compliant join syntax used.

matches regular expression list **Expected** 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**

(1.9) 5676 Current installed Oracle version(oracle19:1:1621:POHK1CCD.hk.standardchartered. **Passed HIGH** com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

19.2

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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 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 E	vidence:
VERSION	
19.2	

(1.10) 8033 Setting for the 'sec_case_sensitive_logon' parameter(oracle19:1:1621:POHK2CCD.hk. Passed MEDIUM standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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		

(1.10) 8033 Setting for the 'sec_case_sensitive_logon' parameter(oracle19:1:1621:POHK1API.hk. Passed MEDIUM standardchartered.com)

Instance oracle 19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

been imponented.		
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	

anded Fride	
ended Evide UE	nce:
E E	
E	
E	
(1.10) 8033	Setting for the 'sec_case_sensitive_logon' parameter(oracle19:1:1621:POHK3CCD.hk. Passed MEDIUM standardchartered.com)
Instance	oracle19:1:1621:POHK3CCD.hk.standardchartered.com
Previous Statu	s Passed
Evaluation Dat	e 08/04/2024 at 10:38:34 PM (GMT+0530)
login. As us be set acco set this para	ASE_SENSITIVE_LOGON information determines whether or not case-sensitivity is required for passwords during mixed-case passwords can strengthen the database against brute-force login attacks, this value should reding to the needs of the business. WARNING: Due to the security bug CVE-2012-3137 it is recommended ameter to TRUE if the October 2012 CPU/PSU or later was applied. If the patch was not applied it is led to set this parameter to FALSE to avoid this vulnerability.
The following been implem	g List String value X indicates the status of the sec_case_sensitive_logon parameter. A value of TRUE shows that case-sensitive login hented.
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 E	Evidence:
VALUE	
TRUE	
TRUE	
TRUE	
(1.10) 8033 Instance	Setting for the 'sec_case_sensitive_logon' parameter(oracle19:1:1621:POHK1RCT.hk. Passed standardchartered.com) oracle19:1:1621:POHK1RCT.hk.standardchartered.com
Previous Statu	s Passed
Evaluation Dat	e 08/04/2024 at 10:38:34 PM (GMT+0530)
login. As us be set acco set this para	ASE_SENSITIVE_LOGON information determines whether or not case-sensitivity is required for passwords during mixed-case passwords can strengthen the database against brute-force login attacks, this value should rding to the needs of the business. WARNING: Due to the security bug CVE-2012-3137 it is recommended ameter to TRUE if the October 2012 CPU/PSU or later was applied. If the patch was not applied it is led to set this parameter to FALSE to avoid this vulnerability.
The following been implem	g List String value X indicates the status of the sec_case_sensitive_logon parameter. A value of TRUE shows that case-sensitive login had ented.
Expected	matches regular expression list
	TRUE
	OR, any of the selected values below:
	Parameter not found
Actual	Loot Undeted:09/04/2024 at 06:04:00 DM (CMT:0520)
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)
	TRUE
Extended E	Evidence:
VALUE	
TRUE	

Oracle_ATOS - 20240806 page 320

TRUE TRUE

(1.10) 8033 Setting for the 'sec_case_sensitive_logon' parameter(oracle19:1:1621:POHK5CCD.hk. Passed MEDIUM standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

TRUE

TRUE

TRUE

(1.10) 8033 Setting for the 'sec_case_sensitive_logon' parameter(oracle19:1:1621:POHK1CAT.hk. Passed MEDIUM standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

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		

(1.10) 8033 Setting for the 'sec_case_sensitive_logon' parameter(oracle19:1:1621:POHK4CCD.hk. Passed MEDIUM standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

TRUE

TRUE

TRUE

TRUE

(1.10) 8033 Setting for the 'sec_case_sensitive_logon' parameter(oracle19:1:1621:POHK1CCD.hk. Passed MEDIUM standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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: Passed HIGH POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 requirement	st String value X indicates the status of the sec_max_failed_login_attempts parameter. A value of 1 - UNLIMITED shows that the 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)
Extended I	dence:
VALUE	
3	
3	
3	
(1.11)	34 Status of the 'sec_max_failed_login_attempts' parameter setting(oracle19:1:1621: Passed HIGH POHK1API.hk.standardchartered.com)
Instance	oracle19:1:1621:POHK1API.hk.standardchartered.com
Instance Previous	
Evaluati	
Evaluation	Jale 08/04/2024 at 10.36.34 FM (GM1+0330)
the log brute-f	MAX_FAILED_LOGIN_ATTEMPTS parameter determines the number of failed logins that can occur before Oracle closes connection. As not limiting the number of failed login attempts for a user connection can facilitate both be login attacks and the occurrence of Denial-of-Service conditions, this value should be set according to the the organization.
The fol	ring List String value X indicates the status of the sec_max_failed_login_attempts parameter. A value of 1 - UNLIMITED shows that the nt has been implemented.
Exped	matches regular expression list
•	3
	OR, any of the selected values below:
	Parameter not found
	Table not found
Actua	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)
	3
Exten	d Evidence:
VALUE	A LANGUIDO.
3	
3	
3	
3	
(1.11)	34 Status of the 'sec_max_failed_login_attempts' parameter setting(oracle19:1:1621: Passed HIGH POHK3CCD.hk.standardchartered.com)
Instance	oracle19:1:1621:POHK3CCD.hk.standardchartered.com
Previous	
Evaluati	
the log brute-f	MAX_FAILED_LOGIN_ATTEMPTS parameter determines the number of failed logins that can occur before Oracle closes connection. As not limiting the number of failed login attempts for a user connection can facilitate both be login attacks and the occurrence of Denial-of-Service conditions, this value should be set according to the the organization.
The fol	ring List String value X indicates the status of the sec_max_failed_login_attempts parameter. A value of 1 - UNLIMITED shows that the nt has been implemented.
Exped	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 E	vidence:				
VALUE					
3					
3					
3					
(1.11) 8034	Status of the 'sec_max_failed_login_attempts' parameter setting(oracle19:1:1621: POHK1RCT.hk.standardchartered.com)	Passed	HIGH		
Instance	oracle19:1:1621:POHK1RCT.hk.standardchartered.com				
Previous Status					
Evaluation Dat					
	(4.1.1.4.4.4.4.4.4.4.4.4.4.4.4.4.4.4.4.4				
the login col brute-force	AX_FAILED_LOGIN_ATTEMPTS parameter determines the number of failed logins that can nection. As not limiting the number of failed login attempts for a user connection can ogin attacks and the occurrence of Denial-of-Service conditions, this value should be organization.	facilitate bo	oth		
The following requirement	List String value X indicates the status of the sec_max_failed_login_attempts parameter. A value of 1 - Unas been implemented.	NLIMITED sho	ws that the		
Expected	matches regular expression list				
	3				
	OR, any of the selected values below:				
	Parameter not found				
	Table not found				
	Tuble not round				
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)				
	3				
Extended E	vidence:				
VALUE					
3					
3					
3					
(1.11) 8034	Status of the 'sec_max_failed_login_attempts' parameter setting(oracle19:1:1621: POHK5CCD.hk.standardchartered.com)	Passed	HIGH		
Instance	oracle19:1:1621:POHK5CCD.hk.standardchartered.com				
Previous Status					
Evaluation Dat	e 08/04/2024 at 10:38:34 PM (GMT+0530)				
the login col brute-force	AX_FAILED_LOGIN_ATTEMPTS parameter determines the number of failed logins that can nection. As not limiting the number of failed login attempts for a user connection can ogin attacks and the occurrence of Denial-of-Service conditions, this value should be organization.	facilitate bo	oth		
The following requirement	List String value X indicates the status of the sec_max_failed_login_attempts parameter. A value of 1 - U has been implemented.	NLIMITED sho	ws that the		
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 E	Evidence:
VALUE	
3	
3	
(1.11) 8034	Status of the 'sec_max_failed_login_attempts' parameter setting(oracle19:1:1621: Passed HIGH POHK4CCD.hk.standardchartered.com)
Instance	oracle19:1:1621:POHK4CCD.hk.standardchartered.com
Previous Statu	is Passed
Evaluation Dat	te 08/04/2024 at 10:38:34 PM (GMT+0530)
the login co brute-force needs of the	AX_FAILED_LOGIN_ATTEMPTS parameter determines the number of failed logins that can occur before Oracle close innection. As not limiting the number of failed login attempts for a user connection can facilitate both login attacks and the occurrence of Denial-of-Service conditions, this value should be set according to the e organization.
requirement	g List String value X indicates the status of the sec_max_failed_login_attempts parameter. A value of 1 - UNLIMITED shows that the has been implemented.
Expected	matches regular expression list
	3
	OR, any of the selected values below:
	Parameter not found Table not found
	Table not round
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)
	3
VALUE 3	Evidence:
3	
3	
. ,	Status of the 'sec_max_failed_login_attempts' parameter setting(oracle19:1:1621: Passed HIGH POHK1CAT.hk.standardchartered.com)
Instance	oracle19:1:1621:POHK1CAT.hk.standardchartered.com
Previous Statu Evaluation Dat	
the login co brute-force	AX_FAILED_LOGIN_ATTEMPTS parameter determines the number of failed logins that can occur before Oracle close innection. As not limiting the number of failed login attempts for a user connection can facilitate both login attacks and the occurrence of Denial-of-Service conditions, this value should be set according to the e organization.
The following requirement	g List String value X indicates the status of the sec_max_failed_login_attempts parameter. A value of 1 - UNLIMITED shows that the 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 F	Evidence:

Oracle_ATOS - 20240806 page 325

VALUE

3			
3			
3			
(1.11) 8034	Status of the 'sec_max_failed_login_attempts' parameter setting(oracle19:1:1621: POHK1CCD.hk.standardchartered.com)	Passed	HIGH
Instance	oracle19:1:1621:POHK1CCD.hk.standardchartered.com		
Previous Statu	s Passed		
Evaluation Dat	e 08/04/2024 at 10:38:34 PM (GMT+0530)		
the login co brute-force	AX_FAILED_LOGIN_ATTEMPTS parameter determines the number of failed logins that can nection. As not limiting the number of failed login attempts for a user connection can login attacks and the occurrence of Denial-of-Service conditions, this value should be organization.	n facilitate b	oth
The following requirement	g List String value X indicates the status of the sec_max_failed_login_attempts parameter. A value of 1 - U has been implemented.	JNLIMITED sh	ows that the
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 E	ividence:		
VALUE	vidence.		
3			
3			
3			
(1.12) 8035	Status of the 'sec_protocol_error_further_action' parameter setting(oracle19:1:1621: POHK2CCD.hk.standardchartered.com)	Failed	MEDIUM
Instance	oracle19:1:1621:POHK2CCD.hk.standardchartered.com		
Previous Statu	s Failed		
Evaluation Dat	e 08/04/2024 at 10:38:34 PM (GMT+0530)		
The SEC_PI received from system, such	e 08/04/2024 at 10:38:34 PM (GMT+0530) ROTOCOL_ERROR_FURTHER_ACTION setting determines the Oracle's server's response method that the client. As bad packets received from the client can potentially indicate packet as "TCP SYN Flood" or "Smurf" attacks, which may result in a Denial-of-Service coefficient as the needs of the business.	based attac	ks on the
The SEC_PI received from system, such should be second to the system.	ROTOCOL_ERROR_FURTHER_ACTION setting determines the Oracle's server's response method that the client. As bad packets received from the client can potentially indicate packethas "TCP SYN Flood" or "Smurf" attacks, which may result in a Denial-of-Service co	based attac ndition, this	ks on the value
The SEC_PI received from system, such should be second to the system.	ROTOCOL_ERROR_FURTHER_ACTION setting determines the Oracle's server's response me the client. As bad packets received from the client can potentially indicate packet-le as "TCP SYN Flood" or "Smurf" attacks, which may result in a Denial-of-Service coefficient according to the needs of the business. **ELIST String value X indicates the status of the sec_protocol_error_further_action parameter. A value of Total String value X indicates the status of the sec_protocol_error_further_action parameter.	based attac ndition, this	ks on the value
The SEC_PI received fro system, suc should be s	ROTOCOL_ERROR_FURTHER_ACTION setting determines the Oracle's server's response me the client. As bad packets received from the client can potentially indicate packet-lend as "TCP SYN Flood" or "Smurf" attacks, which may result in a Denial-of-Service context according to the needs of the business. **List String value X indicates the status of the sec_protocol_error_further_action parameter. A value of The sec_protocol_error_further_action parameter.	based attac ndition, this	ks on the value

Cause of Failure:

Extended Evidence:

Actual

VALUE CONTINUE CONTINUE Parameter not found

CONTINUE

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

Unexpected values	Additional values found in failed controls:
	CONTINUE
Missing values	Expected values not found in failed controls:
	^\(DROP3\)\$
	OR, any of the selected values below:

(1.12) 8035 Status of the 'sec_protocol_error_further_action' parameter setting(oracle19:1:1621: Failed MEDIUM POHK1API.hk.standardchartered.com)

Instance oracle 19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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
	^\(DROP3\)\$
	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 E	vidence:
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:
	^\(DROP3\)\$
	OR, any of the selected values below:

(1.12) 8035 Status of the 'sec_protocol_error_further_action' parameter setting(oracle19:1:1621: Failed MEDIUM POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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
	^\(DROP3\)\$
	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 Ex	vidence:
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:
	^\(DROP3\)\$
	OR, any of the selected values below:

(1.12) 8035 Status of the 'sec_protocol_error_further_action' parameter setting(oracle19:1:1621: Failed MEDIUM POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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 CONTINUE

Cause of Failure:

Unexpected values	Additional values found in failed controls:
	CONTINUE
Missing values	Expected values not found in failed controls:

^\	(Γ)R	\cap	P١	۱.3	()	(
١.	۱L	,,,	ν,		١)	\ J	

OR, any of the selected values below:

(1.12) 8035 Status of the 'sec_protocol_error_further_action' parameter setting(oracle19:1:1621: Failed MEDIUM POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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.

requirement h	List String value X indicates the status of the sec_protocol_error_further_action parameter. A value of TRUE shows that the last been implemented.		
Expected	matches regular expression list		
	^\(DROP3\)\$		
	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 E	vidence:		
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:
	^\(DROP3\)\$
	OR, any of the selected values below:

(1.12) 8035 Status of the 'sec_protocol_error_further_action' parameter setting(oracle19:1:1621: Failed MEDIUM POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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 Ev	vidence:
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:
	^\(DROP3\)\$
	OR, any of the selected values below:

(1.12) 8035 Status of the 'sec_protocol_error_further_action' parameter setting(oracle19:1:1621: Failed MEDIUM POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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.

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 CONTINUE

Cause of Failure:

Unexpected values	Additional values found in failed controls:
	CONTINUE
Missing values	Expected values not found in failed controls:
	^\(DROP3\)\$
	OR, any of the selected values below:

(1.12) 8035 Status of the 'sec_protocol_error_further_action' parameter setting(oracle19:1:1621: Failed MEDIUM POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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 Liet String value V indicates the status of the see protocol error further action parameter. A value of TDLE shows that the

requirement has been implemented.		
Expected	matches regular expression list	
	^\(DROP3\)\$	
	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 E	vidence:	
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:
	^\(DROP3\)\$
	OR, any of the selected values below:

(1.13) 8036 Status of the 'sec_protocol_error_trace_action' parameter setting(oracle19:1:1621: Failed MEDIUM POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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	
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:

(1.13) 8036 Status of the 'sec_protocol_error_trace_action' parameter setting(oracle19:1:1621: Failed MEDIUM POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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

TRACE

Cause of Failure:

Unexpected values

TRACE

Missing values

LOG\$

OR, any of the selected values below:

(1.13) 8036 Status of the 'sec_protocol_error_trace_action' parameter setting(oracle19:1:1621: Failed MEDIUM POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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 requirement	g List String value(s) X indicate the status of the sec_protocol_error_trace_action parameter. A value of TRACE shows that the 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 E	Evidence:
VALUE	
TRACE	
TRACE	
TRACE	
Cause of F	ailure:
Unexpecte values	d Additional values found in failed controls:
	TRACE
Missing values	Expected values not found in failed controls:
	^LOG\$
	OR, any of the selected values below:
(1.13) 8036	Status of the 'sec_protocol_error_trace_action' parameter setting(oracle19:1:1621: Failed MEDIUM POHK1RCT.hk.standardchartered.com)
Instance	oracle19:1:1621:POHK1RCT.hk.standardchartered.com
Previous Statu	is Failed
Evaluation Dat	te 08/04/2024 at 10:38:34 PM (GMT+0530)
packets rec packets car Denial-of-S	ROTOCOL_ERROR_TRACE_ACTION setting determines the Oracle's server's logging response level to bad/malformed served from the client, by generating ALERT, LOG, or TRACE levels of detail in the log files. As incoming bad no potentially indicate packet-based attacks, such as "TCP SYN Flood" or "Smurf" attacks that may result in a ervice condition, this diagnostic/logging value for ALERT, LOG, or TRACE conditions should be set according sof the business.
The following requirement	g List String value(s) X indicate the status of the sec_protocol_error_trace_action parameter. A value of TRACE shows that the 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 E	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:

(1.13) 8036 Status of the 'sec_protocol_error_trace_action' parameter setting(oracle19:1:1621: Failed MEDIUM POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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 E	vidence:
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:

(1.13) 8036 Status of the 'sec_protocol_error_trace_action' parameter setting(oracle19:1:1621: Failed MEDIUM POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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.

Unexpected values

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 E	vidence:
VALUE	
TRACE	
TRACE TRACE	
TRACE	
Cause of Fa	ilure:
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:
nstance Previous Status Evaluation Date	
	OTOCOL_ERROR_TRACE_ACTION setting determines the Oracle's server's logging response level to bad/malformer
packets receptackets can Denial-of-Se the needs	eived from the client, by generating ALERT, LOG, or TRACE levels of detail in the log files. As incoming bad potentially indicate packet-based attacks, such as "TCP SYN Flood" or "Smurf" attacks that may result in a prvice condition, this diagnostic/logging value for ALERT, LOG, or TRACE conditions should be set according of the business.
packets recepackets can Denial-of-Se the needs	potentially indicate packet-based attacks, such as "TCP SYN Flood" or "Smurf" attacks that may result in a rvice condition, this diagnostic/logging value for ALERT, LOG, or TRACE conditions should be set according
packets recepackets can Denial-of-Se the needs	potentially indicate packet-based attacks, such as "TCP SYN Flood" or "Smurf" attacks that may result in a ervice condition, this diagnostic/logging value for ALERT, LOG, or TRACE conditions should be set according of the business. List String value(s) X indicate the status of the sec_protocol_error_trace_action parameter. A value of TRACE shows that the o create a trace file has been implemented. matches regular expression list
packets rece packets can Denial-of-Se to the needs The following requirement t	potentially indicate packet-based attacks, such as "TCP SYN Flood" or "Smurf" attacks that may result in a cryice condition, this diagnostic/logging value for ALERT, LOG, or TRACE conditions should be set according of the business. List String value(s) X indicate the status of the sec_protocol_error_trace_action parameter. A value of TRACE shows that the o create a trace file has been implemented. matches regular expression list ^LOG\$
packets rece packets can Denial-of-Se to the needs The following requirement t	potentially indicate packet-based attacks, such as "TCP SYN Flood" or "Smurf" attacks that may result in a ervice condition, this diagnostic/logging value for ALERT, LOG, or TRACE conditions should be set according of the business. List String value(s) X indicate the status of the sec_protocol_error_trace_action parameter. A value of TRACE shows that the o create a trace file has been implemented. matches regular expression list
packets rece packets can Denial-of-Se to the needs The following requirement t	potentially indicate packet-based attacks, such as "TCP SYN Flood" or "Smurf" attacks that may result in a cryice condition, this diagnostic/logging value for ALERT, LOG, or TRACE conditions should be set according of the business. List String value(s) X indicate the status of the sec_protocol_error_trace_action parameter. A value of TRACE shows that the o create a trace file has been implemented. matches regular expression list ^LOG\$
packets rece packets can Denial-of-Se to the needs The following requirement t	potentially indicate packet-based attacks, such as "TCP SYN Flood" or "Smurf" attacks that may result in a price condition, this diagnostic/logging value for ALERT, LOG, or TRACE conditions should be set according of the business. List String value(s) X indicate the status of the sec_protocol_error_trace_action parameter. A value of TRACE shows that the create a trace file has been implemented. matches regular expression list ^LOG\$ OR, any of the selected values below:
packets recepackets can Denial-of-Se to the needs The following requirement to Expected	potentially indicate packet-based attacks, such as "TCP SYN Flood" or "Smurf" attacks that may result in a cryice condition, this diagnostic/logging value for ALERT, LOG, or TRACE conditions should be set according of the business. List String value(s) X indicate the status of the sec_protocol_error_trace_action parameter. A value of TRACE shows that the occate a trace file has been implemented. matches regular expression list ^LOG\$ OR, any of the selected values below: Parameter not found Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) TRACE
packets receivance and penial-of-Se to the needs The following requirement to Expected Actual	potentially indicate packet-based attacks, such as "TCP SYN Flood" or "Smurf" attacks that may result in a ervice condition, this diagnostic/logging value for ALERT, LOG, or TRACE conditions should be set according of the business. List String value(s) X indicate the status of the sec_protocol_error_trace_action parameter. A value of TRACE shows that the occate a trace file has been implemented. matches regular expression list ^LOG\$ OR, any of the selected values below: Parameter not found Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) TRACE
packets recepackets can Denial-of-Se to the needs The following requirement to Expected Actual	potentially indicate packet-based attacks, such as "TCP SYN Flood" or "Smurf" attacks that may result in a ervice condition, this diagnostic/logging value for ALERT, LOG, or TRACE conditions should be set according of the business. List String value(s) X indicate the status of the sec_protocol_error_trace_action parameter. A value of TRACE shows that the occate a trace file has been implemented. matches regular expression list ^LOG\$ OR, any of the selected values below: Parameter not found Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) TRACE
cackets receivackets can Denial-of-Se to the needs The following requirement to Expected Actual Extended E VALUE	potentially indicate packet-based attacks, such as "TCP SYN Flood" or "Smurf" attacks that may result in a ervice condition, this diagnostic/logging value for ALERT, LOG, or TRACE conditions should be set according of the business. List String value(s) X indicate the status of the sec_protocol_error_trace_action parameter. A value of TRACE shows that the occate a trace file has been implemented. matches regular expression list ^LOG\$ OR, any of the selected values below: Parameter not found Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) TRACE

Oracle_ATOS - 20240806 page 335

Additional values found in failed controls:

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

(1.13) 8036 Status of the 'sec_protocol_error_trace_action' parameter setting(oracle19:1:1621: Failed MEDIUM POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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 E	vidence:
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 Passed MEDIUM (oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 E	vidence:
VALUE	
FALSE	
FALSE	
FALSE	

(1.14) 8037 Status of the 'sec_return_server_release_banner' parameter setting using SQL query Passed MEDIUM (oracle19:1:1621:POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

EALCE

OR, any of the selected values below:

Parameter not found

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

EVICE

Extended Evidence:

VALUE FALSE

FALSE

FALSE

(1.14) 8037 Status of the 'sec_return_server_release_banner' parameter setting using SQL query Passed MEDIUM (oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:	
ALUE	
ALSE	
ALSE	
ALSE	

(1.14) 8037 Status of the 'sec_return_server_release_banner' parameter setting using SQL query Passed MEDIUM (oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(1.14) 8037 Status of the 'sec_return_server_release_banner' parameter setting using SQL query Passed MEDIUM (oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

FALSE FALSE

Evaluation Date 08/04/2024 at 10:38:34 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 E	vidence:
VALUE	
FALSE	
FALSE	
FALSE	

(1.14) 8037 Status of the 'sec_return_server_release_banner' parameter setting using SQL query Passed MEDIUM (oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

FALSE

FALSE

FALSE

FALSE

FALSE

(1.14) 8037 Status of the 'sec_return_server_release_banner' parameter setting using SQL query Passed MEDIUM (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

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

(1.14) 8037 Status of the 'sec_return_server_release_banner' parameter setting using SQL query Passed (oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

FALSE

Evaluation Date 08/04/2024 at 10:38:34 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 requirement h	List String value X indicates the status of the sec_return_server_release_banner parameter. A value of TRUE shows that the as 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 Ex	vidence:
VALUE	
FALSE	
FALSE	
FALSE	

(1.15) 9597 Ownership and permissions set on \$ORACLE_HOME/network/admin directory and files Passed HIGH (oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

The 'ORACLE_HOME/network/admin' is a directory where oracle Network Configuration files are stored such as Listener.ora, This names or 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.

matches regular expression list ^oracle\oinstall\(0|1|2|3|4|5|6|7)(0|1|4|5).*|^grid\oinstall\(0|1|2|3|4|5|6|7)(0|1|4|5).* OR, any of the selected values below: File(s) not found Actual Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/listener.ora oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/tnsnames.ora oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/tnsnames.ora oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/shrept.lst oracle oinstall 755 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora.nov18 oracle oinstall 755 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora20122021

Extended Evidence:

Owner Group Perm FileName
oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/shrept.lst
oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/sqlnet.ora
oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/thsnames.ora
oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/listener.ora
oracle oinstall 755 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora.nov18
oracle oinstall 755 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora20122021

(1.15) 9597 Ownership and permissions set on \$ORACLE_HOME/network/admin directory and files Passed HIGH (oracle19:1:1621:POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

 $$ \operatorname{constall} (0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).* | \operatorname{constall} (0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).* | \operatorname{constall} (0|1|2|3|4|5|6|7)(0|1|4|5).* | \operatorname{constall} (0|1|4|5).* | \operatorname{const$

OR, any of the selected values below:

File(s) not found

Actual

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

oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/listener.ora oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/sqlnet.ora $oracle\ oinstall\ 644\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/network/admin/samples/tnsnames. oracle oinstall\ 644\ /u01/app/oracle/product/db/19.0. Oracle oinstall\ 644\ /u01/app/oracle oinstall\ 644\ /u01/app/oracle oinstall\ 644\ /u01/app/oracle oinstall\ 644\ /u01/app/oracle oinstal$ oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/shrept.lst oracle oinstall 755 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora.nov18 oracle oinstall 755 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora20122021

Extended Evidence:

Owner Group Perm FileName oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/shrept.lst oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/sqlnet.ora oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/tnsnames.ora oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/listener.ora oracle oinstall 755 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora.nov18 oracle oinstall 755 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora20122021

(1.15) 9597 Ownership and permissions set on \$ORACLE_HOME/network/admin directory and files Passed HIGH (oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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

 $$ \operatorname{coracle} \left(0|1|2|3|4|5|6|7\right) (0|1|4|5) (0|1|4|5). \right] - \left(0|1|2|3|4|5|6|7\right) (0|1|4|5) (0|1|4|5) (0|1|4|5). \right] - \left(0|1|2|3|4|5|6|7\right) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1|4|5) (0|1$

OR, any of the selected values below:

File(s) not found

Actual

Instance

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

oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/listener.ora oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/sqlnet.ora oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/tnsnames.ora oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/shrept.lst oracle oinstall 755 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora.nov18 oracle oinstall 755 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora20122021

Extended Evidence:

Owner Group Perm FileName oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/shrept.lst oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/sqlnet.ora oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/tnsnames.ora oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/listener.ora oracle oinstall 755 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora.nov18

(1.15) 9597 Ownership and permissions set on \$ORACLE_HOME/network/admin directory and files Passed HIGH (oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

The 'ORACLE_HOME/network/admin' is a directory where oracle Network Configuration files are stored such as Listener.ora, This names.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 \circ install \circ (0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).* | ``grid \circ install \circ (0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1$ OR, any of the selected values below: File(s) not found Actual Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/listener.ora oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/sqlnet.ora oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/tnsnames.ora oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/shrept.lst oracle oinstall 755 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora.nov18 oracle oinstall 755 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora20122021 **Extended Evidence:** Owner Group Perm FileName oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/shrept.lst oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/sqlnet.ora oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/tnsnames.ora oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/listener.ora oracle oinstall 755 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora.nov18 oracle oinstall 755 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora20122021

(1.15) 9597 Ownership and permissions set on \$ORACLE_HOME/network/admin directory and files Passed (oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

The 'ORACLE_HOME/network/admin' is a directory where oracle Network Configuration files are stored such as Listener.ora, This names or 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
	$\label{lem:constall} $$\operatorname{coll}(0 1 2 3 4 5 6 7)(0 1 4 5).* ^{\prid} \circ (0 1 2 3 4 5 6 7)(0 1 4 5).*$$
	OR, any of the selected values below:
	File(s) not found
Actual	Loct Undeted 00/04/0004 at 00:04:00 DM (CMT:0500)
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)
	oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/listener.ora
	oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/sqlnet.ora
	oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/tnsnames.ora
	oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/shrept.lst

oracle oinstall 755 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora.nov18
oracle oinstall 755 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora20122021

Extended Evidence:

Owner Group Perm FileName
oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/shrept.lst
oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/sqlnet.ora
oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/tnsnames.ora
oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/listener.ora
oracle oinstall 755 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora.nov18
oracle oinstall 755 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora20122021

(1.15) 9597 Ownership and permissions set on \$ORACLE_HOME/network/admin directory and files Passed HIGH (oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

The 'ORACLE_HOME/network/admin' is a directory where oracle Network Configuration files are stored such as Listener.ora, This names.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

 $$$\operatorname{coracle} \subset (0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).*|\right]$ in the proof of the proo$

OR, any of the selected values below:

File(s) not found

Actual

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

oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/listener.ora oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/sqlnet.ora oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/tnsnames.ora oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/shrept.lst

oracle oinstall 755 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora.nov18 oracle oinstall 755 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora20122021

Extended Evidence:

Owner Group Perm FileName oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/shrept.lst oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/sqlnet.ora oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/tnsnames.ora oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/listener.ora oracle oinstall 755 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora.nov18 oracle oinstall 755 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora20122021

(1.15) 9597 Ownership and permissions set on \$ORACLE_HOME/network/admin directory and files Passed (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

	$\label{lem:constall} $$\operatorname{oinstall} (0 1 2 3 4 5 6 7)(0 1 4 5)(0 1 4 5).* \operatorname{oinstall} (0 1 2 3 4 5 6 7)(0 1 4 5)(0 1 4 5).* $$\operatorname{oinstall} (0 1 2 3 4 5 6 7)(0 1 4 5).* $$\operatorname{oinstall} (0 1 4 5 4 5 4 5 4 5 4 5 4 5 4 5 4 5 4 5 4$
	OR, any of the selected values below:
	File(s) not found
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)
	oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/listener.ora
	oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/sqlnet.ora
	oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/tnsnames.ora
	oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/shrept.lst
	oracle oinstall 755 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora.nov18
	oracle oinstall 755 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora20122021
Extended Ev	vidence:
Owner Group	Perm FileName
oracle oinstall	644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/shrept.lst
oracle oinstall	644/u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/sqlnet.ora
oracle oinstall	644/u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/tnsnames.ora
oracle oinstall	644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/listener.ora
oracle oinstall	755 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora.nov18
oracle oinstall	755 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora20122021

(1.15) 9597 Ownership and permissions set on \$ORACLE_HOME/network/admin directory and files Passed HIGH (oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

The 'ORACLE_HOME/network/admin' is a directory where oracle Network Configuration files are stored such as Listener.ora, Thenames.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 $\DACLE_HOME/network/admin\Darker{Minimum}$ With UNIX these files will NOT have the required permission level of 0750.

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).*|^grid\ oinstall\ (0|1|2|3|4|5|6|7)(0|1|4|5).* OR, any of the selected values below: File(s) not found Actual Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/listener.ora oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/sqlnet.ora oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/tnsnames.ora oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora.nov18 oracle oinstall 755 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora.20122021 Extended Evidence:

Owner Group Perm FileName
oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/shrept.lst
oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/sqlnet.ora
oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/tnsnames.ora
oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/samples/listener.ora
oracle oinstall 755 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora.nov18
oracle oinstall 755 /u01/app/oracle/product/db/19.7.0.0.Apr2020/network/admin/sqlnet.ora20122021

HIGH

(1.16) 9598 Ownership and permissions set on \$ORACLE_HOME/dbs and \$ORACLE_HOME/ Failed dbs/*(oracle19:1:1621:POHK1API.hk.standardchartered.com)

oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Failed

Instance

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.

required peri	nission level of 0750.
Expected	matches regular expression list
	$ ^{\circ} (0 1 2 3 4 5 6 7)(0 1 4 5)(0 1 4 5). ^{\circ} (0 1 2 3 4 5 6 7)(0 1 4 5). ^{\circ} (0 1 2 3 4 5 6 7)(0 1 4 5). ^{\circ} (0 1 2 3 4 5 6 7)(0 1 4 5). ^{\circ} (0 1 2 3 4 5 6 7)(0 1 4 5). ^{\circ} (0 1 2 3 4 5 6 7)(0 1 4 5). ^{\circ} (0 1 2 3 4 5 6 7)(0 1 4 5). ^{\circ} (0 1 2 3 4 5 6 7)(0 1 4 5). ^{\circ} (0 1 2 3 4 5 6 7)(0 1 4 5). ^{\circ} (0 1 2 3 4 5 6 7)(0 1 4 5). ^{\circ} (0 1 2 3 4 5 6 7)(0 1 4 5). ^{\circ} (0 1 2 3 4 5 6 7)(0 1 4 5). ^{\circ} (0 1 4 5 4 5 6 7)(0 1 4 5). ^{\circ} (0 1 4 5 4 5 6 7)(0 1 4 5). ^{\circ} (0 1 4 5 4 5 6 7)(0 1 4 5). ^{\circ} (0 1 4 5 4 5 6 7)(0 1 4 5). ^{\circ} (0 1 4 5 4 5 6 7)(0 1 4 5 4 5 6 7)(0 1 4 5 7)(0 1 4 $
	OR, any of the selected values below:
	File(s) not found
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)
	oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dluumh6c_1_1_14611038828748_27-04-2020
	oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dmuumh6c_1_1_14621038828748_27-04-2020
	oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dpuumhbe_1_1_14651038828910_27-04-2020
	oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/snapcf_DUK31BLD1.f
	oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/spfileRESTOR19.ora
	oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/init.ora
	oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/initPOHK1CCD1.ora
	oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/ps
	oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_DUK31BLD1.dat
	oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_RESTOR19.dat
Extended E	Evidence:
Owner Grou	p Perm FileName
oracle oinsta	ll 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/spfileRESTOR19.ora
oracle oinsta	ll 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_RESTOR19.dat
oracle oinsta	ll 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/init.ora
oracle oinsta	ll 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dmuumh6c_1_1_14621038828748_27-04-2020
oracle oinsta	ll 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dpuumhbe_1_1_1_14651038828910_27-04-2020
oracle oinsta	ll 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/snapcf_DUK31BLD1.f

Cause of Failure:

Unexpected values	Additional values found in failed controls:
	oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_DUK31BLD1.dat oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_RESTOR19.dat
Missing values	Expected values not found in failed controls:
	OR, any of the selected values below:

(1.16) 9598 Ownership and permissions set on \$ORACLE_HOME/dbs and \$ORACLE_HOME/ Failed HIGH dbs/*(oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0. Apr
2020/dbs/hc_DUK31BLD1.dat oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0. Apr
2020/dbs/initPOHK1CCD1.ora

oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/ps

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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

 $$$\operatorname{constall}(0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).*|\operatorname{constall}(0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).*|\operatorname{constall}(0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).*|\operatorname{constall}(0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).*|\operatorname{constall}(0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).*|\operatorname{constall}(0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).*|\operatorname{constall}(0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).*|\operatorname{constall}(0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).*|\operatorname{constall}(0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).*|\operatorname{constall}(0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).*|\operatorname{constall}(0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).*|\operatorname{constall}(0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).*|\operatorname{constall}(0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).*|\operatorname{constall}(0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).*|\operatorname{constall}(0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).*|\operatorname{constall}(0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).*|\operatorname{constall}(0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).*|\operatorname{constall}(0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).*|\operatorname{constall}(0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).*|\operatorname{constall}(0|1|2|3|4|5|6|7)(0|1|4|5).*|\operatorname{constall}(0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5).*|\operatorname{constall}(0|1|2|3|4|5|6|7)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1|4|5)(0|1$

OR, any of the selected values below:

File(s) not found

Actual

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

oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dluumh6c_1_1_14611038828748_27-04-2020 oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dmuumh6c_1_1_1_14621038828748_27-04-2020

oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dpuumhbe_1_1_14651038828910_27-04-2020

oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/snapcf_DUK31BLD1.f

oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/spfileRESTOR19.ora

oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/init.ora

oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/initPOHK1CCD1.ora

oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/ps

oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_DUK31BLD1.dat oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_RESTOR19.dat

Extended Evidence:

Owner Group Perm FileName

oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/spfileRESTOR19.ora

oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_RESTOR19.dat

oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/init.ora

oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dmuumh6c_1_1_14621038828748_27-04-2020

oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/snapcf_DUK31BLD1.f

oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db arch DUK31BLD dluumh6c 1 1 14611038828748 27-04-2020

oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_DUK31BLD1.dat

oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/initPOHK1CCD1.ora

oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/ps

Cause of Failure:

Unexpected values

Additional values found in failed controls:

oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_DUK31BLD1.dat oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_RESTOR19.dat

Missina values

Expected values not found in failed controls:

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:POHK1RCT.hk.standardchartered.com)

Failed

HIGH

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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 $$$ \operatorname{cel} \left(0|1|2|3|4|5|6|7 \right) \left(0|1|4|5 \right) \left(0|1|4|5 \right). $$ \cap \operatorname{cel} \left(0|1|2|3|4|5|6|7 \right) \left(0|1|4|5 \right) \left(0|1|4|5 \right). $$$ OR, any of the selected values below: File(s) not found Actual Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dluumh6c_1_1_14611038828748_27-04-2020 oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dmuumh6c_1_1_1_14621038828748_27-04-2020 oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/ db_arch_DUK31BLD_dpuumhbe_1_1_1_14651038828910_27-04-2020 oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/snapcf_DUK31BLD1.f oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/spfileRESTOR19.ora oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/init.ora $oracle\ oinstall\ 644\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/init POHK 1CCD 1. oracle\ oinstall\ 644\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/init POHK 1CCD 1. oracle\ oinstall\ 644\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/init POHK 1CCD 1. oracle\ oinstall\ 644\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/init POHK 1CCD 1. oracle\ oinstall\ 644\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/init POHK 1CCD 1. oracle\ oinstall\ 644\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/init POHK 1CCD 1. oracle\ oinstall\ 644\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/init POHK 1CCD 1. oracle\ oinstall\ 644\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/init POHK 1CCD 1. oracle\ oinstall\ 644\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/init POHK 1CCD 1. oracle\ oinstall\ 644\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/init POHK 1CCD 1. oracle\ oinstall\ 644\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/init POHK 1CCD 1. oracle\ oinstall\ 0. oracle\ 0.$ oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/ps oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_DUK31BLD1.dat oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_RESTOR19.dat **Extended Evidence:** Owner Group Perm FileName oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/spfileRESTOR19.ora oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_RESTOR19.dat oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/init.ora oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dmuumh6c_1_1_14621038828748_27-04-2020 oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dpuumhbe_1_1_14651038828910_27-04-2020 oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/snapcf_DUK31BLD1.f oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dluumh6c_1_1_14611038828748_27-04-2020 oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_DUK31BLD1.dat oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/initPOHK1CCD1.ora oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/ps

Cause of Failure:

Unexpected values	Additional values found in failed controls:
	oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_DUK31BLD1.dat oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_RESTOR19.dat
Missing values	Expected values not found in failed controls:
	OR, any of the selected values below:

(1.16) 9598 Ownership and permissions set on \$ORACLE_HOME/dbs and \$ORACLE_HOME/ Failed HIGH dbs/*(oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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).*|^oracle\ asmadmin\ (0|1|2|3|4|5|6|7)(0|1|4|5).* OR, any of the selected values below:

	File(s) not found
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)
	oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dluumh6c_1_1_14611038828748_27-04-2020
	oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dmuumh6c_1_1_14621038828748_27-04-2020
	oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dpuumhbe_1_1_14651038828910_27-04-2020
	oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/snapcf_DUK31BLD1.f
	oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/spfileRESTOR19.ora
	oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/init.ora
	oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/initPOHK1CCD1.ora
	oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/ps
	oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_DUK31BLD1.dat
	oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_RESTOR19.dat
Extended E	vidence:
Owner Group	Perm FileName
oracle oinstal	640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/spfileRESTOR19.ora
oracle oinstal	660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_RESTOR19.dat
oracle oinstal	644/u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/init.ora
oracle oinstal	640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dmuumh6c_1_1_14621038828748_27-04-2020
oracle oinstal	640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dpuumhbe_1_1_1_14651038828910_27-04-2020
oracle oinstal	640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/snapcf_DUK31BLD1.f
oracle oinstal	640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dluumh6c_1_1_14611038828748_27-04-2020
oracle oinstal	660/u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_DUK31BLD1.dat
oracle oinstal	644/u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/initPOHK1CCD1.ora
oracle oinstal	644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/ps

Cause of Failure:

Unexpected values	Additional values found in failed controls:
	oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_DUK31BLD1.dat oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_RESTOR19.dat
Missing values	Expected values not found in failed controls:
	OR, any of the selected values below:

(1.16) 9598 Ownership and permissions set on \$ORACLE_HOME/dbs and \$ORACLE_HOME/ Failed HIGH dbs/*(oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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).*|^oracle\ asmadmin\ (0|1|2|3|4|5|6|7)(0|1|4|5).*

OR, any of the selected values below:File(s) not found

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

oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dluumh6c_1_1_14611038828748_27-04-2020

oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dmuumh6c_1_1_14621038828748_27-04-2020 oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dpuumhbe_1_1_14651038828910_27-04-2020

oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/snapcf_DUK31BLD1.f

oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/spfileRESTOR19.ora

oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/init.ora

oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/initPOHK1CCD1.ora

oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/ps

oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0. Apr
2020/dbs/hc_DUK31BLD1.dat oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0. Apr
2020/dbs/hc_RESTOR19.dat

Extended Evidence:

Owner Group Perm FileName

oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/spfileRESTOR19.ora

 $oracle\ oinstall\ 660\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/hc_RESTOR 19. dat$

oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/init.ora

oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dmuumh6c_1_1_14621038828748_27-04-2020 oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dpuumhbe_1_1_14651038828910_27-04-2020

oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/snapcf_DUK31BLD1.f

 $oracle\ oinstall\ 660\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/hc_DUK 31BLD 1. dat$

oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/initPOHK1CCD1.ora

oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/ps

Cause of Failure:

Unexpected values	Additional values found in failed controls:
	oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_DUK31BLD1.dat oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_RESTOR19.dat
Missing values	Expected values not found in failed controls:
	OR, any of the selected values below:

(1.16) 9598 Ownership and permissions set on \$ORACLE_HOME/dbs and \$ORACLE_HOME/ Failed HIGH dbs/*(oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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.

oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/snapcf_DUK31BLD1.f oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/spfileRESTOR19.ora oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/init.ora oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/initPOHK1CCD1.ora oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/ps oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_DUK31BLD1.dat oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc RESTOR19.dat **Extended Evidence:** Owner Group Perm FileName oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/spfileRESTOR19.ora oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc RESTOR19.dat oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/init.ora oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dmuumh6c_1_1_14621038828748_27-04-2020 oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/snapcf_DUK31BLD1.f oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_DUK31BLD1.dat

Cause of Failure:

Unexpected values	Additional values found in failed controls:
	oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_DUK31BLD1.dat oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_RESTOR19.dat
Missing values	Expected values not found in failed controls:
	OR, any of the selected values below:

(1.16) 9598 Ownership and permissions set on \$ORACLE_HOME/dbs and \$ORACLE_HOME/ Failed HIGH dbs/*(oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/initPOHK1CCD1.ora

oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/ps

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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
	$\label{lem:constall} $$\operatorname{oinstall} (0 1 2 3 4 5 6 7)(0 1 4 5)(0 1 4 5).* $$\operatorname{oracle} \ asmadmin \ (0 1 2 3 4 5 6 7)(0 1 4 5).* $$$
	OR, any of the selected values below:
	File(s) not found
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)
	oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dluumh6c_1_1_14611038828748_27-04-2020
	oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dmuumh6c_1_1_14621038828748_27-04-2020
	oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dpuumhbe_1_1_14651038828910_27-04-2020
	oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/snapcf_DUK31BLD1.f
	oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/spfileRESTOR19.ora
	oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/init.ora

oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/initPOHK1CCD1.ora

oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/ps

oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0. Apr
2020/dbs/hc_DUK31BLD1.dat oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0. Apr
2020/dbs/hc_RESTOR19.dat

Extended Evidence:

Owner Group Perm FileName

oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/spfileRESTOR19.ora

oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_RESTOR19.dat

oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/init.ora

oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/snapcf_DUK31BLD1.f

 $oracle\ oinstall\ 660\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/hc_DUK 31BLD 1. dat$

 $oracle\ oinstall\ 644\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/init POHK 1CCD 1. oracle\ oinstall\ 644\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/init POHK 1CCD 1. oracle\ oinstall\ 644\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/init POHK 1CCD 1. oracle\ oinstall\ 644\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/init POHK 1CCD 1. oracle\ oinstall\ 644\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/init POHK 1CCD 1. oracle\ oinstall\ 644\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/init POHK 1CCD 1. oracle\ oinstall\ 644\ /u01/app/oracle/product/db/19.7.0. One of the product/db/19.7.0. One of the product/db/19.7. One of the$

oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/ps

Cause of Failure:

Unexpected Addit values

Additional values found in failed controls:

oracle oinstall $660 / u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_DUK31BLD1.dat$ oracle oinstall $660 / u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_RESTOR19.dat$

Missing values

Expected values not found in failed controls:

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:POHK1CCD.hk.standardchartered.com)

Failed HIGH

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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 $PACLE_HOME/dbs$ directory. With UNIX these files will NOT have the required permission level of 0750.

Expected

matches regular expression list

 $$$\operatorname{constall} (0|1|2|3|4|5|6|7)(0|1|4|5). $$\operatorname{constall} (0|1|2|3|4|5|6|7)(0|1|4|5). $$$

OR, any of the selected values below:

File(s) not found

Actual

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

oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dluumh6c_1_1_14611038828748_27-04-2020

oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dmuumh6c_1_1_1_14621038828748_27-04-2020

oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/db_arch_DUK31BLD_dpuumhbe_1_1_14651038828910_27-04-2020

oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/snapcf_DUK31BLD1.f

oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/spfileRESTOR19.ora

oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/init.ora

 $oracle\ oinstall\ 644\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/init POHK 1CCD 1. oracle\ oinstall\ 644\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/init POHK 1CCD 1. oracle\ oinstall\ 644\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/init POHK 1CCD 1. oracle\ oinstall\ 644\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/init POHK 1CCD 1. oracle\ oinstall\ 644\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/init POHK 1CCD 1. oracle\ oinstall\ 644\ /u01/app/oracle/product/db/19.7.0. Oxacle\ oinstall\ 644\ /u01/app/oracle/product/db/19.7. Oxacle\ oinstall\ 044\ /u01/app/oracle/product/db/19.7. Oxacle\ oinstall\ 044\ /u01/app/oracle/product/db/19.7. Oxacle\ oinstall\ 044\ /u01/app/oracle/product/db/19.7. Oxacle\ oinstall\ 044\ /u01/app/oracle/product/db/19.7. Oxacle\ oinstall\ 0$

 $oracle\ oinstall\ 644\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/ps$

 $oracle\ oinstall\ 660\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/hc_DUK 31BLD 1. data and the control of the control$

oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_RESTOR19.dat
Extended Evidence:
Owner Group Perm FileName
oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/spfileRESTOR19.ora
oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_RESTOR19.dat
oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/init.ora
$oracle\ oinstall\ 640\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/db_arch_DUK 31BLD_dmuumh 6c_1_1_14621038828748_27-04-2020$
$oracle\ oinstall\ 640\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/db_arch_DUK 31BLD_dpuumhbe_1_1_14651038828910_27-04-2020$
oracle oinstall 640 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/snapcf_DUK31BLD1.f
$oracle\ oinstall\ 640\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/db_arch_DUK 31BLD_dluum h 6c_1_1_14611038828748_27-04-2020$
oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_DUK31BLD1.dat
oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/initPOHK1CCD1.ora
oracle oinstall 644 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/ps

Cause of Failure:

Unexpected values	Additional values found in failed controls:
	oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_DUK31BLD1.dat oracle oinstall 660 /u01/app/oracle/product/db/19.7.0.0.Apr2020/dbs/hc_RESTOR19.dat
Missing values	Expected values not found in failed controls:
	OR, any of the selected values below:

(1.17) 12623 Status of Unified Auditing mode(oracle19:1:1621:POHK1API.hk.standardchartered.com) Passed MEDIUM

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

The means pure mode of diameter additing is chabled.				
Expected	regular expression match			
	TRUE			
	OR, any of the selected values below:			
	Setting not found			
	Table not found			
Actual	tual Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)			
	TRUE			
Extended Evidence:				
PARAMETER		VALUE		
Unified Audit	ing	TRUE		

(1.17) 12623 Status of Unified Auditing mode(oracle19:1:1621:POHK3CCD.hk.standardchartered. Passed MEDIUM com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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. regular expression match **Expected** 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 (1.17) 12623 Status of Unified Auditing mode(oracle19:1:1621:POHK1RCT.hk.standardchartered. **MEDIUM Passed** com) oracle19:1:1621:POHK1RCT.hk.standardchartered.com Instance Previous Status **Evaluation Date** 08/04/2024 at 10:38:34 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** (1.17) 12623 Status of Unified Auditing mode(oracle19:1:1621:POHK5CCD.hk.standardchartered. **Passed MEDIUM** Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com Previous Status 08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date** 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 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+05	30)
	TRUE	<i>'</i>
Extended Ex	vidence:	
PARAMETER		VALUE
Unified Auditin	ng	TRUE
Instance Previous Status Evaluation Date		om
auditing, Pur difficult to det	e unified auditing: Has only unified auditing. If da	e values are Mixed mode: Has both traditional and unified tabase is not configured to audit then it is more nourred during a system compromise. This should be configured
	String value of X indicate the status of unified auditing set four mode of unified auditing is enabled.	r the database. Note: FALSE means mix mode of unified auditing is enabled
Expected	regular expression match	

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

(1.17) 12623 Status of Unified Auditing mode(oracle19:1:1621:POHK1CAT.hk.standardchartered. Passed MEDIUM com)

TRUE

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Unified Auditing

Evaluation Date 08/04/2024 at 10:38:34 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.

True means pure mode of diffined addicing is chabled.				
Expected	regular expression match			
	TRUE			
	OR, any of the selected values below:			
	Setting not found			
	Table not found			
	L == (Ll== d= (= d=00/0.4/0.00 A = (.00-0.4-0.0 DM / .00-0.0)			
Actual	Lock Undeted-09/04/2024 at 06-04-00 DM (CMT-06-	201		
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+05	30)		
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+05: TRUE	30)		
Actual Extended E	TRUE	30)		
	TRUE	VALUE		

(1.17) 12623 Status of Unified Auditing mode(oracle19:1:1621:POHK2CCD.hk.standardchartered. Passed MEDIUM

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

VALUE

TRUE

(1.17) 12623	Status of Unified Auditing mode(oracle19:1:1621:POHK1CCD.hk.standardchartered.	Passed	MEDIUM
. ,	com)		

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passeo

PARAMETER

Unified Auditing

Evaluation Date 08/04/2024 at 10:38:34 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.

True means p	are mode of diffica additing is chasica.	
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+05	30)
Actual	Last Opuateu.00/04/2024 at 00.01.03 FW (GW11+03-	50)
	TRUE	
Extended E	vidence:	
PARAMETER		VALUE
Unified Audit	ng	TRUE

(1.18) 12624 Status of policies enabled for Unified Auditing(oracle19:1:1621:POHK1API.hk. Passed MEDIUM standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 reg	jular expression list				
	.*:SCB_AUDIT_	DDL_POLICY:.*:.*:				
	.*:SCB_AUDIT_	DROP_POLICY:.*:.*:				
	.*:SCB_LOGON	_ALL_FAILURES:.*:.*:				
	.*:SCB_LOGON	_LOGOFF_PRIVUSER:.*:.*:				
	OR, any of the	he selected values below:				
	Setting not	found				
	Table not fo					
Actual	Last Update	d:08/04/2024 at 06:01:09 F	PM (GMT+0530)			
	ALL USERS:SCI	B_AUDIT_DDL_POLICY:BY USE	ER:YES:YES			
	ALL USERS:SCI	B_AUDIT_DROP_POLICY:BY U	SER:YES:YES			
	ALL USERS:SCB_LOGON_ALL_FAILURES:BY USER:NO:YES					
	ALL USERS:SCI	B_LOGON_LOGOFF_PRIVUSER	:BY USER:YES:YES			
Extended Ev	vidence:					
ENTITY_NAM		POLICY NAME	ENABLED OPTION	SUCCESS	FAILURE	
ALL USERS	ь	SCB LOGON LOGOFF PRIVUSER	_	YES	YES	
ALL USERS		SCB_LOGON_LOGOFF_1 KIV 65EK		NO	YES	
ALL USERS		SCB_LOGON_ALL_TAILORES SCB_AUDIT_DDL_POLICY	BY USER	YES	YES	
ALL USERS		ISCD AUDII DDL I OLICI	DI USEK	ILO	ILO	

(1.18) 12624 Status of policies enabled for Unified Auditing(oracle19:1:1621:POHK3CCD.hk. Passed MEDIUM standardchartered.com)

YES

YES

YES

YES

YES

YES

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

SCB_AUDIT_DDL_POLICY

SCB_AUDIT_DROP_POLICY BY USER

SCB_AUDIT_DROP_POLICY BY USER

Previous Status Passed

ALL USERS

ALL USERS

ALL USERS

Evaluation Date 08/04/2024 at 10:38:34 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.

values of entit	y_name, policy_	name, enabled_option, succes	s, and failure option set for	the unined additing 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	he selected values below:			
	Setting not	found			
	Table not fo	ound			
Actual	Last Update	d:08/04/2024 at 06:01:09 F	PM (GMT+0530)		
	ALL HEEDE CO	A A LIDIT DDI DOI LOV DVI LICI	P·VES·VES		
	ALL USERS:SC	B_AUDIT_DDL_POLICY:BY USE	IV. 1 E.J. 1 E.J		
		B_AUDIT_DDL_POLICY:BY USE B_AUDIT_DROP_POLICY:BY USE			
	ALL USERS:SC		SER:YES:YES		
	ALL USERS:SCI	B_AUDIT_DROP_POLICY:BY U	SER:YES:YES JSER:NO:YES		
Extended E	ALL USERS:SCI ALL USERS:SCI ALL USERS:SCI	B_AUDIT_DROP_POLICY:BY U B_LOGON_ALL_FAILURES:BY U	SER:YES:YES JSER:NO:YES		
Extended E ENTITY_NAM	ALL USERS:SCI ALL USERS:SCI ALL USERS:SCI vidence:	B_AUDIT_DROP_POLICY:BY U B_LOGON_ALL_FAILURES:BY U	SER:YES:YES JSER:NO:YES	SUCCESS	FAILURE
	ALL USERS:SCI ALL USERS:SCI ALL USERS:SCI vidence:	B_AUDIT_DROP_POLICY:BY US B_LOGON_ALL_FAILURES:BY U B_LOGON_LOGOFF_PRIVUSER	SER:YES:YES JSER:NO:YES :BY USER:YES:YES ENABLED_OPTION	SUCCESS YES	FAILURE YES

Oracle_ATOS - 20240806 page 356

BY USER

(1.18) 12624 Status of policies enabled for Unified Auditing(oracle19:1:1621:POHK1RCT.hk. standardchartered.com)

oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Instance

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

contains regular expression list

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.

•					
	.*: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 fo	ound			
Actual	Last Update	d:08/04/2024 at 06:01:09 F	PM (GMT+0530)		
	ALL USERS:SC	B_AUDIT_DDL_POLICY:BY USE	ER:YES:YES		
	ALL USERS:SCB_AUDIT_DROP_POLICY:BY USER:YES:YES				
	ALL USERS:SCB_LOGON_ALL_FAILURES:BY USER:NO:YES				
	ALL USERS:SC	B_LOGON_LOGOFF_PRIVUSER	::BY USER:YES:YES		
Extended E	vidence:				
ENTITY_NAM	1E	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

(1.18) 12624 Status of policies enabled for Unified Auditing(oracle19:1:1621:POHK5CCD.hk. Passed standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

SCB_AUDIT_DROP_POLICY BY USER

Previous Status Passed

ALL USERS

Evaluation Date 08/04/2024 at 10:38:34 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

Oracle_ATOS - 20240806 page 357

Passed MEDIUM

YES

MEDIUM

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

(1.18) 12624 Status of policies enabled for Unified Auditing(oracle19:1:1621:POHK4CCD.hk. standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	he selected values b	pelow:		
	Setting not	found			
	Table not fo	ound			
Actual	Last Update	d:08/04/2024 at 06:0	1:09 PM (GMT+0530)		
	ALL USERS:SCI	B_AUDIT_DDL_POLICY:	BY USER:YES:YES		
	ALL USERS:SCI	B_AUDIT_DROP_POLIC	Y:BY USER:YES:YES		
	ALL USERS:SCI	B_LOGON_ALL_FAILUR	ES:BY USER:NO:YES		
	ALL USERS:SCI	B_LOGON_LOGOFF_PRI	VUSER:BY USER:YES:YES		
Extended E	vidence:				
ENTITY_NAM	Е	POLICY_NAME	ENABLED_OPTION	SUCCESS	FAILURE

(1.10) 1000 1 O(1.1 1.1 1.1 1.1 1.1 1.1 1.1 1.1 1.1 1.1	olicies enabled for Unified	A . 15th (1 . 40 . 4 . 4004	DOUBLE OF L	Passed	MEDIUM
ALL USERS	SCB_AUDIT_DROP_POLICY	BY USER	YES	YES	

BY USER

YES

NO

YES

YES

YES

YES

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

SCB_LOGON_LOGOFF_PRIVUSER BY USER

SCB_LOGON_ALL_FAILURES BY USER

SCB_AUDIT_DDL_POLICY

Previous Status Passed

ALL USERS

ALL USERS

ALL USERS

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

standardchartered.com)

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.

	2- 11 2- 1 21
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 Table not f				
Actual	Last Update	ed:08/04/2024 at 06:01:09 F	PM (GMT+0530)		
	ALL USERS:SC	B_AUDIT_DDL_POLICY:BY USI	ER:YES:YES		
	ALL USERS:SC	B_AUDIT_DROP_POLICY:BY U	SER: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

YES

YES

(1.18) 12624 Status of policies enabled for Unified Auditing(oracle19:1:1621:POHK2CCD.hk. standardchartered.com)

SCB_AUDIT_DROP_POLICY BY USER

BY USER

Passed MEDIUM

YES

YES

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

SCB_AUDIT_DDL_POLICY

Previous Status Passed

ALL USERS

ALL USERS

Evaluation Date 08/04/2024 at 10:38:34 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 E	ividence:

Extended Evidence:						
OPTION SUCCESS	FAILURE					
YES	YES					
NO	YES					
YES	YES					
YES	YES					
	YES NO YES					

(1.18) 12624 Status of policies enabled for Unified Auditing(oracle19:1:1621:POHK1CCD.hk. Passed MEDIUM standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_	.*:SCB_AUDIT_DDL_POLICY:.*:.*:							
	.*:SCB_AUDIT_	DROP_POLICY:.*:.*							
	.*:SCB_LOGON_	_ALL_FAILURES:.*:.*:							
	.*:SCB_LOGON_	_LOGOFF_PRIVUSER:.*:.*:.*							
	OR, any of th	ne selected values below:							
	Setting not for Table not for								
Actual	Last Updated	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)							
	ALL USERS:SCE	ALL USERS:SCB_AUDIT_DDL_POLICY:BY USER:YES:YES							
	ALL USERS:SCE	ALL USERS:SCB_AUDIT_DROP_POLICY:BY USER:YES:YES							
	ALL USERS:SCE	ALL USERS:SCB_LOGON_ALL_FAILURES:BY USER:NO:YES							
	ALL USERS:SCE	ALL USERS:SCB_LOGON_LOGOFF_PRIVUSER:BY USER:YES:YES							
Extended E	vidence:								
ENTITY_NAM	ΙE	POLICY_NAME	ENABLED_OPTION	SUCCESS	FAILURE				
ALL USERS		SCB_LOGON_LOGOFF_PRIVUSEF	R 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 HISERS		SCR AUDIT DROP POLICY	BY LISER	VFS	YFS				

(1.19) 12707 Status of 'extproc' in listener.ora(oracle19:1:1621:POHK1API.hk.standardchartered.	Passed	HIGH
com)		

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:08/04/2024 at 06:01:09 PM (GMT+0530)

String not found

Extended Evidence:

File name

Pattern

/u01/app/grid/product/19c/network/admin/listener.ora

EXTPROC

(1.19) 12707 Status of 'extproc' in listener.ora(oracle19:1:1621:POHK3CCD.hk.standardchartered. Passed HIGH com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:08/04/2024 at 06:01:09 PM (GMT+0530)				
	String not found				
Extended E	Extended Evidence:				
File name	le name Pattern				
/u01/app/grid	/u01/app/grid/product/19c/network/admin/listener.ora EXTPROC				

(1.19) 12707 Status of 'extproc' in listener.ora(oracle19:1:1621:POHK1RCT.hk.standardchartered. Passed HIGH com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

EXPROC

OR, any of the selected values below:

String not found
File not found

Actual

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

String not found

Extended Evidence:

File name

Pattern

/u01/app/grid/product/19c/network/admin/listener.ora

EXTPROC

(1.19) 12707 Status of 'extproc' in listener.ora(oracle19:1:1621:POHK5CCD.hk.standardchartered. Passed HIGH com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:08/04/2024 at 06:01:09 PM (GMT+0530)			
	String not found			
Extended	Evidence:			
File name		Pattern		
/u01/app/g	grid/product/19c/network/admin/listener.ora	EXTPROC		

(1.19) 12707 Status of 'extproc' in listener.ora(oracle19:1:1621:POHK4CCD.hk.standardchartered. Passed HIGH

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	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:08/04/2024 at 06:01:09 PM (GMT-	-0530)				
	String not found					
Extended Evidence:						
File name		Pattern				
/u01/app/gri	d/product/19c/network/admin/listener.ora	EXTPROC				

(1.19) 12707 Status of 'extproc' in listener.ora(oracle19:1:1621:POHK1CAT.hk.standardchartered. Passed HIGH

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:08/04/2024 at 06:01:09 PM (GMT+0530)

String not found

Extended Evidence:			
File name	Pattern		
/u01/app/oracle/local/network/admin/listener.ora	EXTPROC		

(1.19) 12707 Status of 'extproc' in listener.ora(oracle19:1:1621:POHK1CCD.hk.standardchartered. Passed HIGH

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	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:08/04/2024 at 06:01:09 PM (GMT+05	30)			
	String not found				
Extended E	Extended Evidence:				
File name		Pattern			
/u01/app/gri	d/product/19c/network/admin/listener.ora	EXTPROC			

(1.19) 12707 Status of 'extproc' in listener.ora(oracle19:1:1621:POHK2CCD.hk.standardchartered. Passed HIGH com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	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:08/04/2024 at 06:01:09 PM (GMT+0530)			
	String not found			
Extended Evidence:				
File name		Pattern		
/u01/app/gri	d/product/19c/network/admin/listener.ora	EXTPROC		

(1.20) 14340 Status of auditing for 'CREATE USER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_type, success, failure, enabled_option, and entity_name.

Expected matches regular expression list

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 Ev	Extended Evidence:							
POLICY_NAME		AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_DE	DL_P-	CREATE USER	STANDARD ACTION	YES	YES	BY USER	ALL USERS	

(1.20) 14340 Status of auditing for 'CREATE USER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

separateu vait	separated values of policy_name, addit_option_type, success, failure, enabled_option, and entry_name.							
Expected	matc	hes regular expres	ssion list					
	.*:CRE	ATE USER:.*:YES:YES:	*.*					
	OR, any of the selected values below:							
	Setting not found							
	Tal	ble not found						
				·				
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM ((GMT+0530)				
	SCB_A	AUDIT_DDL_POLICY:0	REATE USER:STANDA	ARD ACTION:YES:YES:	BY USER:ALL USERS			
Extended E	Extended Evidence:							
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_D OLICY	DL_P-	CREATE USER	STANDARD ACTION	YES	YES	BY USER	ALL USERS	

(1.20) 14340 Status of auditing for 'CREATE USER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	matc	hes regular expres	ssion list					
	.*:CRE	ATE USER:.*:YES:YES:	*.*					
	OR, a	any of the selected	l values below:					
	Setting not found Table not found							
A . 4 1				OMT OFOO				
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM (GM I +0530)				
	SCB_AUDIT_DDL_POLICY:CREATE USER:STANDARD ACTION:YES:YES:BY USER:ALL USERS							
Extended E	viden	e:						
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_D OLICY	DL_P-	CREATE USER	STANDARD ACTION	YES	YES	BY USER	ALL USERS	

(1.20) 14340 Status of auditing for 'CREATE USER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

•	•	J = 1			- ·	5 —			
Expected	matc	hes regular expres	ssion list						
	.*:CRE	ATE USER:.*:YES:YES:	*.*						
	OR, any of the selected values below:								
	Setting not found								
	Tal	ole not found							
Actual	Lact		24 at 06:01:00 DM /	CMT - 0530\					
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 E	vidend	ce:							
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_D OLICY	DL_P-	CREATE USER	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.20) 14340 Status of auditing for 'CREATE USER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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							
	Tal	ole not found						
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)							
	SCB_A	AUDIT_DDL_POLICY:C	REATE USER:STANDA	RD ACTION:YES:YES:I	BY USER:ALL USERS			
Extended Ev	/idend	ce:						
POLICY_NAMI	3	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_D: OLICY	DL_P-	CREATE USER	STANDARD ACTION	YES	YES	BY USER	ALL USERS	

(1.20) 14340 Status of auditing for 'CREATE USER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

Expected matches regular expression list

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.

	.*:CRE	ATE USER:.*:YES:YES:	*.*						
	OR, a	ny of the selected	I values below:						
	Setting not found								
	Table not found								
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM (GMT+0530)					
	SCB_AUDIT_DDL_POLICY:CREATE USER:STANDARD ACTION:YES:YES:BY USER:ALL USERS								
	SCB_A	UDIT_DDL_POLICY:C	REATE USER:SYSTEM	PRIVILEGE:YES:YES:I	BY USER:ALL USERS				
Extended Ex	videnc	e:							
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_D OLICY	DL_P-	CREATE USER	SYSTEM PRIVILEGE	YES	YES	BY USER	ALL USERS		
SCB_AUDIT_D OLICY	DL_P-	CREATE USER	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.20) 14340 Status of auditing for 'CREATE USER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

separated vait	ies 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 L	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)								
S	SCB_AUDIT_DDL_POLICY:CREATE USER:STANDARD ACTION:YES:YES:BY USER:ALL USERS								
Extended Evid	lence:								
POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCB_AUDIT_DDI	_P- CREATE USER	STANDARD ACTION	YES	YES	BY USER	ALL USERS			

(1.20) 14340 Status of auditing for 'CREATE USER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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: Passed MEDIUM POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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. matches regular expression list **Expected** .*: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:** AUDIT_OPTION_TYPE SUCCESS POLICY_NAME AUDIT_OPTION **FAILURE** ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P- ALTER USER STANDARD ACTION YES BY USER ALL USERS YES

(1.21) 14341 Status of auditing for 'ALTER USER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_type, success, failure, enabled_option, and entity_name. matches regular expression list *:ALTER USER:.*:YES:YES:.*:.* OR, any of the selected values below: Setting not found Table not found Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) Actual SCB_AUDIT_DDL_POLICY:ALTER USER:STANDARD ACTION:YES:YES:BY USER:ALL USERS **Extended Evidence:** POLICY_NAME AUDIT_OPTION_TYPE SUCCESS AUDIT_OPTION **FAILURE** ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P- ALTER USER STANDARD ACTION YES YES BY USER **ALL USERS** OLICY

(1.21) 14341 Status of auditing for 'ALTER USER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 Eviden	Extended Evidence:								
POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCB_AUDIT_DDL_P-OLICY	- ALTER USER	STANDARD ACTION	YES	YES	BY USER	ALL USERS			

(1.21) 14341 Status of auditing for 'ALTER USER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 separated value	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	matc	hes regular expres	ssion list					
	.*:ALTER USER:.*:YES:YES:.**							
	OR, any of the selected values below:							
	Set	ting not found						
	Tal	ole not found						
Actual		-	24 at 06:01:09 PM (•	W LICED, ALL LICEDO			
	SCB_F	IUDIT_DDL_POLICY:A	LTER USER:STANDAR	ED ACTION: YES: YES:B	Y USER:ALL USERS			
Extended Ev	idend	e:						
POLICY_NAMI	3	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_DI	DL_P-	ALTER USER	STANDARD ACTION	YES	YES	BY USER	ALL USERS	

(1.21) 14341 Status of auditing for 'ALTER USER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

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 ALTER USER statement is used to change database users' password, lock accounts, and expire passwords. Logging and mo

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

(1.21) 14341 Status of auditing for 'ALTER USER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	mato	hes regular expre	ssion list						
	.*:ALTER USER:.*:YES:YES:.*.*								
	OR,	any of the selected	d values below:						
	Se	tting not found							
	Ta	ble not found							
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM ((GMT+0530)					
		SCB_AUDIT_DDL_POLICY:ALTER USER:STANDARD ACTION:YES:YES:BY USER:ALL USERS							
Extended E	viden	ce:							
POLICY_NAM	ΙE	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
COD ALIDITE I	ם זמנ	ALTER USER	STANDARD ACTION	VES	YES	BY USER	ALL USERS		
OLICY	JDL_P-	ALTER OSER	STANDARD ACTION	TLS	TES	DI CSER	ALL USERS		
OLICY	Statu	us of auditing for '	ALTER USER' privi		1	- 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3			
OLICY 1. 21) 1434 1	Statu	us of auditing for 'A K1CCD.hk.standar	ALTER USER' privi	ilege (Unified Aud		- 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3			
OLICY	Statu POH	us of auditing for 'A K1CCD.hk.standar	ALTER USER' privi	ilege (Unified Aud		- 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3			
OLICY 1.21) 14341 astance	Statu POH	us of auditing for 'A K1CCD.hk.standar oracle19:1:1621:POF Passed	ALTER USER' privi	ilege (Unified Aud		- 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3			

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_type, success, failure, enabled_option, and entity_name.

Expected r	natches regular expre	ssion list								
,	*:ALTER USER:.*:YES:YES:.*	. *								
	OR, any of the selected values below:									
	Setting not found									
	Table not found									
Astual		04 =4 00-04-00 DM	(OMT : 0500)							
Actual L	_ast Updated:08/04/20	24 at 06:01:09 PM ((GMT+0530)							
S	SCB_AUDIT_DDL_POLICY:ALTER USER:STANDARD ACTION:YES:YES:BY USER:ALL USERS									
Extended Evi	dence:									
POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME				
SCB_AUDIT_DD	L_P- ALTER USER	STANDARD ACTION	YES	YES	BY USER	ALL USERS				

(1.21) 14341 Status of auditing for 'ALTER USER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 separated value	List String value(s) of X indicates the status of the ALTER USER audit option type defined on the database. The output contains colon es 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

, ioiaa.		opuatouroro nzoz	at 0010 1100 1 III (C III 1 1 0 0 0 0 7			
	SCB_A	AUDIT_DDL_POLICY:A	LTER USER:STANDAR	D ACTION:YES:YES:BY	Y USER:ALL USERS		
Extended Ex	viden	ce:					
POLICY_NAMI	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_D	DL_P-	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: Passed MEDIUM POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

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

Previous Status Passed

Actual

Evaluation Date 08/04/2024 at 10:38:34 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 ENTITY_NAME **FAILURE** ENABLED_OPTION SCB_AUDIT_DDL_P- DROP USER OLICY STANDARD ACTION YES YES BY USER ALL USERS

(1.22) 14342 Status of auditing for 'DROP USER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Actual

Evaluation Date 08/04/2024 at 10:38:34 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_type, success, failure, enabled_option, and entity_name.

Expected matches regular expression list

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

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

OR, any of the selected values below:

Setting not found

Table not found

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_P- DROP USER STANDARD ACTION YES YES BY USER ALL USERS

(1.22) 14342 Status of auditing for 'DROP USER' privilege (Unified Auditing)(oracle19:1:1621: POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) Actual SCB_AUDIT_DDL_POLICY:DROP USER:STANDARD ACTION:YES:YES:BY USER:ALL USERS **Extended Evidence:** POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS ENABLED_OPTION ENTITY_NAME **FAILURE** SCB_AUDIT_DDL_P- DROP USER ALL USERS STANDARD ACTION YES YES BY USER OLICY

(1.22) 14342 Status of auditing for 'DROP USER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

SCB_AUDIT_DDL_P- DROP USER STANDARD ACTION YES YES BY USER ALL USERS	POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
02101	SCB_AUDIT_DDL_P- OLICY	DROP USER	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.22) 14342 Status of auditing for 'DROP USER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

The 'DROP USER' statement is used to drop Oracle database accounts and schemas associated with them. Logging and

Oracle_ATOS - 20240806 page 372

Passed

MEDIUM

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.

-	<u> </u>							
Expected	matc	hes regular expre	ssion list					
	.*:DRC	OP 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)								
Actual	Lasi	Opuateu.00/04/20	24 at 00.01.03 1 W	GW1 +0330)				
	SCB_AUDIT_DDL_POLICY:DROP USER:STANDARD ACTION:YES:YES:BY USER:ALL USERS							
	SCB_A	AUDIT_DDL_POLICY:	DROP USER:SYSTEM P	RIVILEGE:YES:YES:BY	USER:ALL USERS			
Extended E	viden	ce:						
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_D OLICY	DL_P-	DROP USER	SYSTEM PRIVILEGE	YES	YES	BY USER	ALL USERS	
SCB_AUDIT_D OLICY	DL_P-	DROP USER	STANDARD ACTION	YES	YES	BY USER	ALL USERS	

(1.22) 14342 Status of auditing for 'DROP USER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_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_P- DROP USER STANDARD ACTION YES YES BY USER ALL USERS

(1.22) 14342 Status of auditing for 'DROP USER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

		ression list				
	.*:DROP USER:.*:YES:YES					
	OR, any of the select	ted values below:				
	Setting not found					
	Table not found					
Actual	Last Updated:08/04/2	2024 at 06:01:09 PM ((GMT+0530)			
	SCB_AUDIT_DDL_POLIC	Y:DROP USER:STANDARI	D ACTION:YES:Y	ES:BY USER:ALL USE	RS	
Extended E	vidence:					
POLICY_NAM	ME AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_I OLICY	DDL_P- DROP USER	STANDARD ACTION	YES	YES	BY USER	ALL USERS
1.22) 14342	2 Status of auditing fo POHK2CCD.hk.stand	or 'DROP USER' privil dardchartered.com)	ege (Unified /	Auditing)(oracle19	:1:1621: Passe	ed MEDIUN
stance		POHK2CCD.hk.standardcl	hartered.com			
revious Status	s Passed					
aluation Date	e 08/04/2024 at 10	0:38:34 PM (GMT+0530))			
idences a	bout potential suspici	ious/unauthorized ad	ctivities. This	logging requireme	ent should be set as a	ppropriate to
ne needs o	f the business.		DDOD LICED out	dit antion type define	d on the detabase The outr	out contains solon
ne needs o	f the business.		DROP USER au be, success, failu	dit option type defined re, enabled_option, ar	d on the database. The outp nd entity_name.	out contains colon
ne needs o	f the business.	ndicates the status of the _option, audit_option_typ	DROP USER au oe, success, failu	lit option type defined re, enabled_option, ar	d on the database. The outp nd entity_name.	out contains colon
ne needs of The following separated val	f the business. g List String value(s) of X in ues of policy_name, audit_	ndicates the status of the _option, audit_option_typ oression list	DROP USER au De, success, failu	dit option type definer re, enabled_option, ar	d on the database. The outp nd entity_name.	out contains colon
ne needs of The following separated val	f the business. g List String value(s) of X in ues of policy_name, audit_ matches regular exp	ndicates the status of the option, audit_option_typeression list	DROP USER au be, success, failu	lit option type defined re, enabled_option, ar	d on the database. The outp nd entity_name.	out contains colon
ne needs of The following separated val	f the business. g List String value(s) of X in ues of policy_name, audit_ matches regular exp .*:DROP USER:.*:YES:YES	ndicates the status of the option, audit_option_typeression list	DROP USER au De, success, failu	dit option type definer re, enabled_option, ar	d on the database. The outp nd entity_name.	out contains colon
e needs of the following the f	g List String value(s) of X in ues of policy_name, audit_ matches regular exp .*:DROP USER:.*:YES:YES OR, any of the select Setting not found	ndicates the status of the coption, audit_option_typeression list S:.*:.* ted values below:		lit option type defined re, enabled_option, ar	d on the database. The outp nd entity_name.	out contains colon
ne needs of the following separated values	f the business. g List String value(s) of X in ues of policy_name, audit_ matches regular exp .*:DROP USER:.*:YES:YES OR, any of the select Setting not found Table not found	ndicates the status of the coption, audit_option_typeression list Sanda values below:	(GMT+0530)			out contains colon
ne needs of The following separated val	g List String value(s) of X in ues of policy_name, audit_ matches regular exp .*:DROP USER:.*:YES:YES OR, any of the select Setting not found Table not found Last Updated:08/04/2 SCB_AUDIT_DDL_POLICE	ndicates the status of the coption, audit_option_typeression list Sanda values below:	(GMT+0530)			out contains colon
ne needs of The following separated value Expected	f the business. g List String value(s) of X in use of policy_name, audit_ matches regular exp .*:DROP USER:.*:YES:YES OR, any of the select Setting not found Table not found Last Updated:08/04/2 SCB_AUDIT_DDL_POLICE Evidence:	ndicates the status of the coption, audit_option_typeression list Sanda values below:	(GMT+0530) D ACTION:YES:Y			

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 type success failure enabled option and entity name.

eparated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.							
matches regular expression list							
.*:CREATE ROLE:.*:YES:YES:.*:.*							
OR, any of the selected values below:							
Setting not found							
Table not found							

Actual L	Last Opdated:08/04/2024 at 06:01:09 PM (GMT+0530)							
S	CB_AUDIT_DDL_POLICY:	CREATE ROLE:STAND	ARD ACTION:YES:YES:	BY USER:ALL USERS				
Extended Evid	lence:							
POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_DDI	_P- CREATE ROLE	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.23) 14343 Status of auditing for 'CREATE ROLE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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)								
Actual	Last	Updated:08/04/202	24 at 06:01:09 PW (GINI I +0530)					
	SCB_A	AUDIT_DDL_POLICY:0	CREATE ROLE:STANDA	ARD ACTION:YES:YES:	BY USER:ALL USERS				
Extended E	vidend	ce:							
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_D OLICY	DL_P-	CREATE ROLE	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.23) 14343 Status of auditing for 'CREATE ROLE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

separated values	parated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.								
Expected r	matches regular expression list								
	:CRE	ATE ROLE:.:YES:YES:	*.*						
	OR, a	ny of the selected	l values below:						
	Setting not found								
	Table not found								
Actual L	Last l	Updated:08/04/202	24 at 06:01:09 PM (GMT+0530)					
S	SCB_A	UDIT_DDL_POLICY:C	REATE ROLE:STANDA	ARD ACTION:YES:YES:I	BY USER:ALL USERS				
Extended Evi	Extended Evidence:								
POLICY_NAME		AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_DD	L_P-	CREATE ROLE	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.23) 14343 Status of auditing for 'CREATE ROLE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:								
	Sett	ting not found							
Table not found									
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)								
Last Opuated:00/04/2024 at 00:01:09 FM (GMT+0530)									
	SCB_A	UDIT_DDL_POLICY:C	REATE ROLE:STANDA	ARD ACTION:YES:YES:I	BY USER:ALL USERS				
Extended Ev	/idenc	e:							
POLICY_NAME	3	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_DI	DL_P-	CREATE ROLE	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.23) 14343 Status of auditing for 'CREATE ROLE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	matc	hes regular expre	ssion list						
	.*:CREATE ROLE:.*:YES:YES:.*:.*								
	OR, any of the selected values below:								
	Setting not found								
	Tal	ole not found							
Actual	Last	Updated:08/04/20	24 at 06:01:09 PM ((GMT+0530)					
	SCB_A	AUDIT_DDL_POLICY:(CREATE ROLE:STANDA	ARD ACTION:YES:YES	S:BY USER:ALL USERS				
	SCB_AUDIT_DDL_POLICY:CREATE ROLE:SYSTEM PRIVILEGE:YES:YES:BY USER:ALL USERS								
Extended E	Extended Evidence:								
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_D OLICY	DL_P-	CREATE ROLE	SYSTEM PRIVILEGE	YES	YES	BY USER	ALL USERS		
SCB_AUDIT_D OLICY	DL_P-	CREATE ROLE	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.23) 14343 Status of auditing for 'CREATE ROLE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_P- CREATE ROLE STANDARD ACTION YES YES BY USER ALL USERS

(1.23) 14343 Status of auditing for 'CREATE ROLE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

matches regular expression list **Expected** *: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_P- CREATE ROLE STANDARD ACTION YES YES BY USER ALL USERS

(1.23) 14343 Status of auditing for 'CREATE ROLE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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, a	any of the selected	l values below:					
	Setting not found							
	Table not found							
Actual Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)								
	SCB_A	AUDIT_DDL_POLICY:C	REATE ROLE:STANDA	ARD ACTION:YES:YES:	BY USER:ALL USERS			
Extended Evidence:								
POLICY_NAMI	3	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_DIOLICY	DL_P-	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: Passed MEDIUM POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	matc	matches regular expression list									
	.*:ALT	.*:ALTER ROLE:.*:YES:YES:.**									
	OR, any of the selected values below:										
	Set	Setting not found									
Table not found											
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)										
	SCB_A	SCB_AUDIT_DDL_POLICY:ALTER ROLE:STANDARD ACTION:YES:YES:BY USER:ALL USERS									
Extended E	Extended Evidence:										
POLICY_NAM	Е	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME				
SCB_AUDIT_D OLICY	DL_P-	ALTER ROLE	STANDARD ACTION	YES	YES	BY USER	ALL USERS				

(1.24) 14344 Status of auditing for 'ALTER ROLE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

p	F, <u>,</u> ,						
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			

(1.24) 14344 Status of auditing for 'ALTER ROLE' privilege (Unified Auditing)(oracle19:1:1621: **Passed MEDIUM** POHK1RCT.hk.standardchartered.com)

oracle19:1:1621:POHK1RCT.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 separated value	llowing List String value(s) of X indicates the status of the ALTER ROLE audit option type defined on the database. The output contains colon ted values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.										
Expected	matc	hes regular expre	ession list								
	.*:ALT	ER ROLE:.*:YES:YES:.	*.*								
	OR, any of the selected values below:										
	Setting not found										
Table not found											
Actual	Last	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)									
	SCB_A	SCB_AUDIT_DDL_POLICY:ALTER ROLE:STANDARD ACTION:YES:YES:BY USER:ALL USERS									
Extended E	vidend	ce:									
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME				
SCR AUDIT DDI P		ALTER ROLE	STANDARD ACTION	VFS	VES	BY HSER	ALL HSERS				

(1.24) 14344 Status of auditing for 'ALTER ROLE' privilege (Unified Auditing)(oracle19:1:1621: **Passed MEDIUM** POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

OLICY

Evaluation Date 08/04/2024 at 10:38:34 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 separated value	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 eparated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.									
Expected	matc	hes regular expre	ssion list							
	.*:ALT	ER ROLE:.*:YES:YES:.	*.*							
	OR, a	any of the selecte	d values below:							
	Set	Setting not found								
	Tal	Table not found								
Actual		•	24 at 06:01:09 PM (•						
	SCB_A	AUDIT_DDL_POLICY:.	ALTER ROLE:STANDAF	RD ACTION:YES:YES:E	BY USER:ALL USERS					
Extended E	vidend	ce:								
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCB_AUDIT_D	DL_P-	ALTER ROLE	STANDARD ACTION	YES	YES	BY USER	ALL USERS			

(1.24) 14344 Status of auditing for 'ALTER ROLE' privilege (Unified Auditing)(oracle19:1:1621: **Passed** POHK1CAT.hk.standardchartered.com)

MEDIUM

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	matc	hes regular expre	ssion list						
	.*:ALT	ER ROLE:.*:YES:YES:.*	· * ··						
	OR, a	any of the selected	d values below:						
	Set	Setting not found							
	Ta	Table not found							
Astual	1	Llm data d.00/04/201	04 -4 0C-04-00 DM /	CMT. 0520)					
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM (GIVI I +0530)					
	SCB_A	AUDIT_DDL_POLICY:A	ALTER ROLE:STANDAR	RD ACTION:YES:YES:B	Y USER:ALL USERS				
Extended	Extended Evidence:								
POLICY_NA	AME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT	Γ_DDL_P-	ALTER ROLE	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.24) 14344 Status of auditing for 'ALTER ROLE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

scparated vari	separated values of policy_name, addit_option_type, success, failure, chabled_option, and chety_name.									
Expected	matc	hes regular expres	ssion list							
	.*:ALT	ER ROLE:.*:YES:YES:.*	. * 							
	OR, a	any of the selected	I values below:							
	Setting not found									
	Table not found									
A . 4 1			14 . 4 00 04 00 DN	(OMT OFOO)						
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM ((GM I +0530)						
	SCB_A	AUDIT_DDL_POLICY:A	LTER ROLE:STANDAF	RD ACTION:YES:YES:B	Y USER:ALL USERS					
Extended Evidence:										
POLICY_NAM	Е	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCB_AUDIT_D OLICY	DL_P-	ALTER ROLE	STANDARD ACTION	YES	YES	BY USER	ALL USERS			

(1.24) 14344 Status of auditing for 'ALTER ROLE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

.*: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— ALTER ROLE STANDARD ACTION YES YES BY USER ALL USERS OLICY	Expected	ues of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name. matches regular expression list										
OR, any of the selected values below: Setting not found Actual Last Updated:08/04/2024 at 08:01:09 PM (GMT+0530) SCB AUDIT DOL POLICYALTER ROLE-STANDARD ACTION YES YESRY USERALL USERS Extended Evidence: ROLEY, NAME AUDIT.OPTION AUDIT.OPTION, TYPE SUCCESS FAILURE FNARIED, OPTION FNTTY, NAME AUDIT.OPTION FOR STANDARD ACTION YES YES BY USER AUDIT.OPTION FOR AUDIT.OPTION, TYPE SUCCESS FAILURE FNARIED, OPTION FNTTY, NAME AUDIT.OPTION FOR STANDARD ACTION YES YES BY USER AUDIT.OPTION FOR AUDIT.OPTION FOR STANDARD ACTION YES YES BY USER AUDIT.OPTION FOR FOR AUDIT.OPTION FOR FOR AUDIT.OPTION FOR FOR FOR AUDIT.OPTION FOR	-xheoren											
Setting not found												
Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)			•	Talada bolow.								
SCR_ALIDIT_DDL_POLICYALITE ROLE-STANDARD ACTION/YES/YES/BY USERALL USERS Extended Evidence: POLICY NAME AUDIT_OPTION AUDIT_OPTION Type SUCCESS FAILURE STANDARD ACTION YES YES BY USER ALL USERS BY USER ALL USERS MEDIUM POHKZCD.h.k.standardchartered.com) Instance Oracle 19:11621: Passed MEDIUM POHKZCD.h.k.standardchartered.com) Passed OR/O4/2024 at 10:38:34 PM (GMT-0530) The 'ALTER ROLE' command is a powerful database tool, allowing the alteration of a 'role' that can be assigned to a larg 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 color separated values of policy_name, audit_option_type, success, failure, enabled_option, and entity_name. Expected activities Audit Doll Policy Policy												
SCR_AUDIT_DDI_POLICY_AITER ROLE_STANDARD ACTION_VTS_VES.BY_USER_ALL_USERS Extended Evidence: POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE_SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME ALL USERS MEDIUM AUDIT_OPTION AUDIT_OPTION_TYPE_SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME ALL USERS MEDIUM AUDIT_OPTION_TYPE_SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME ALL USERS MEDIUM AUDIT_OPTION_TYPE_SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME ALL USERS MEDIUM AUDIT_OPTION_TYPE_SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME SCR_AUDIT_OPTION_POLICY_AUTREROLESTANDARD_ACTION_YES_YES_BY_USER_ALL USERS Extended Evidence: POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE_SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME SCR_AUDIT_OPTION_TYPE_SUCCESS ENTITY_TYPE_SUCCESS ENTITY_TYPE_SUCCESS ENTITY_TYPE_SUCCESS ENTITY_TYPE_SUCCESS ENTITY_TYPE_SUCCESS ENTITY_TYPE_SUCCESS ENTITY_TYPE_SUCCESS ENTITY_TYPE_SUCCESS ENTITY_TYPE_SUC	Actual	Last	Updated:08/04/20)24 at 06:01:09 PM (GMT+0530)							
POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P- ALTER ROLE STANDARD ACTION YES YES BY USER ALL USERS (1.24) 14344 Status of auditing for 'ALTER ROLE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHIACZCD_INk_standardchartered.com Porollary Porollary Policy Policy 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 color separated values of policy_name, andit_option_type, success, failure, enabled_option, and entity_name. Expected Matches regular expression list			-			ES:BY USER:ALL USERS						
SCB_AUDTL_DDL_P- ALTER ROLE STANDARD ACTION YES YES BY USER ALL USERS (1.24) 14344 Status of auditing for 'ALTER ROLE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK2CCD.hk.standardchartered.com Previous Status Previous Status Passed 08/04/2024 at 10:38:34 PM (CMT-0530) The 'ALTER ROLE' command is a powerful database tool, allowing the alteration of a 'role' that can be assigned to a lan numbers of users who need the same object/system privileges. Logging and monitoring of alternotes, whether successful, or unsuccessful, or unsuccessful, or unsuccessful or unsucce	Extended Ex	viden	ce:									
(1.24) 14344 Status of auditing for 'ALTER ROLE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK2CCD.hk.standardchartered.com) Previous Status oracle 91:1621:POHK2CCD.hk.standardchartered.com Previous Status oracle 91:1621:POHK2CCD.hk.standardchartered.com Passed 08:704/2024 at 10:38:34 PM (GMT+0530) The 'ALTER ROLE' command is a powerful database tool, allowing the alteration of a 'role' that can be assigned to a largument 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_type, success, failure, enabled_option, and entity_name. Expected **ALTER ROLE**YESYES-*** 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) SCE AUDIT_DDL_POLICY-ALTER ROLE-STANDARD ACTION.YESYES-BY USER-ALL USERS Extended Evidence: POLICY_NAME SCB_AUDIT_DDL_POLICY-ALTER ROLE-STANDARD ACTION.YES YES BY USER ALL USERS Linear Control of Auditing for 'DROP ROLE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM OR/OH/CD24 at 10:38:34 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 o	POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME				
POHKZCCD.hk.siandardchartered.com) Instance oracle 19:1:1621.POHKZCCD.hk.standardchartered.com Previous Status Passed Previous Status Passed Previous Status No. Actual Last Updated:08/04/2024 at 10:38:34 PM (GMT+0530) SCB_AUDIT_DDL_POLICY.ALTER ROLE-STANDARD ACTION YES YES BY USER ALL USERS Extended Evidence Expected Status Actual Last Updated:08/04/2024 at 10:38:34 PM (GMT+0530) SCB_AUDIT_DDL_POLICY.ALTER ROLE-STANDARD ACTION YES YES BY USER ALL USERS Extended Evidence Folicy in Asses Audit (PDP) ALTER ROLE STANDARD ACTION YES YES BY USER ALL USERS Extended Evidence Folicy has additing for 'DROP ROLE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUN POHK14P)hk.standardchartered.com) Instance oracle 19:1:1621-POHK1AP1hk.standardchartered.com POHKY APA BY AUDIT_OPTION AUDIT_OPTION YES YES BY USER ALL USERS Extended Evidence: The IDROP 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 un user 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 IDROP 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 un usuccessful, any 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, and entity_name. Expected matches required by the state of the DROP ROLE addit option, and entity_name. Expected matches required by the state of the DROP ROLE addit option, and entity_name. Expected by th	SCB_AUDIT_D					YES	BY USER	ALL USERS				
Instance oracle 19:1:1621:POHK2CCD.hk.standardchartered.com Previous Status Passed Previous Status Passed 08/04/2024 at 10:38:34 PM (6MT+0530) The 'ALTER ROLE' command is a powerful database tool, allowing the alteration of a 'role' that can be assigned to a larg 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 color separated values of policy_name. audit_option_undic_und	(1.24) 14344	Statu	is of auditing for	'ALTER ROLE' privi	lege (Unified A	Auditing)(oracle19:1	:1621: Passe	ed MEDIUM				
Previous Status Passed Vorduction Date 08/04/2024 at 10:38:34 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 adult option type defined on the database. The output contains color separated values of policy_name, audit_option_type, success, failure, enabled_option, and entity_name. Expected matches regular expression list	netanaa	РОН		•	partared com							
The 'ALTER ROLE' command is a powerful database tool, allowing the alteration of a 'role' that can be assigned to a larnumbers 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_type, success, failure, enabled_option, and entity_name. Expected matches regular expression list _*ALTER ROLE.**YESYES.**.* OR, any of the selected values below: Setting nor found Table not found Actual Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) SCB_AUDIT_DDL_POLICY:ALTER ROLESTANDARD ACTION YES_YES.BY USERALL USERS Extended Evidence: POLICY_NAME				JHK2CCD.nk.standardcr	iartered.com							
## Numbers of users who need the same object/system privileges. Logging and monitoring of all attempts to alier 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 color separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name. Expected				38:34 PM (GMT+0530)								
numbers of users who need the same object/system privileges. Logging and monitoring of all attempts to alier 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 color separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name. Expected **ALTER ROLE.**YESYES.**.** OR, any of the selected values below: Setting not found Actual Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) SCB_AUDIT_DDL_POLICY_ALTER ROLESTANDARD ACTION_YES_YES_BY USERALL USERS Extended Evidence: POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P—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: Passed MEDIUN POHK1API.hk.standardchartered.com) Instance oracle19:1:1621:POHK1API.hk.standardchartered.com Possed 08/04/2024 at 10:38:34 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. Expected matches regular expression list **DROP ROLE:**YESYES.**:* OR, any of the selected values below: Setting not found				,								
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												
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 color separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name. Expected matches regular expression list ALTER ROLE **TESYPES.*** OR, any of the selected values below:												
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_type, success, failure, enabled_option, and entity_name. Expected matches regular expression list .**ALTER ROLE.*YESYES.**.** 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) SCE_AUDIT_DDL_POLICY:ALTER ROLE-STANDARD ACTION:YESYESBY USER:ALL USERS Extended Evidence: POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME SCE_AUDIT_DDL_P- OLICY (1.25) 14345 Status of auditing for 'DROP ROLE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1API.hk.standardchartered.com) Instance oracle 19:1:1621:POHK1API.hk.standardchartered.com Previous Status Passed 08/04/2024 at 10:38:34 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_type, success, failure, enabled_option, and entity_name. Expected matches regular expression list .*DROP ROLE.*YESYES.*E.*.* OR, any of the selected values below: Setting not found								s/unautnorized				
Expected matches regular expression list **ALTER ROLE.**YES.YES.*.** OR, any of the selected values below: Setting not found Table not found Table 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 USERALL USERS Extended Evidence: POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P- ALTER ROLE STANDARD ACTION YES YES BY USER C(1.25) 14345 Status of auditing for 'DROP ROLE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUN POHK1API.hk.standardchartered.com) Instance oracle 19:1:1621:POHK1API.hk.standardchartered.com Previous Status Evaluation Date 08/04/2024 at 10:38:34 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	activities. Th	is log	ging requirement	t should be set as t	αρριοριίαιο το	the needs of the be	3311033.					
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 USERALL USERS Extended Evidence: POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P- 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: Passed MEDIUN POHK1API.hk.standardchartered.com) Instance oracle19:1:1621:POHK1API.hk.standardchartered.com Passed 08/04/2024 at 10:38:34 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_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	The following	List St	ring value(s) of X ind	licates the status of the	ALTER ROLE au	dit option type defined o	on the database. The out	put contains colon				
: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 USERALL USERS Extended Evidence: POLICY_NAME	•				c, success, ranur	e, enabled_option, and e	nerty_name.					
OR, any of the selected values below: Setting not found Table 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- 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: Passed MEDIUN POHK1API.hk.standardchartered.com) Instance oracle 19:1:1621:POHK1API.hk.standardchartered.com Previous Status Passed Evaluation Date 08/04/2024 at 10:38:34 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_type, success, failure, enabled_option, and entity_name. Expected matches regular expression list												
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- 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: Passed MEDIUN POHK1API.hk.standardchartered.com) Instance oracle19:1:1621:POHK1API.hk.standardchartered.com Previous Status Passed Evaluation Date 08/04/2024 at 10:38:34 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:*YESYES:*:** OR, any of the selected values below: Setting 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			•	, a value 5 5 10 111								
Extended Evidence: POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P- 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: Passed MEDIUM POHK1API.hk.standardchartered.com) Instance oracle19:1:1621:POHK1API.hk.standardchartered.com Previous Status Passed Evaluation Date 08/04/2024 at 10:38:34 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 Setting												
Extended Evidence: POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P- 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: Passed MEDIUM POHK1API.hk.standardchartered.com) Instance oracle19:1:1621:POHK1API.hk.standardchartered.com Previous Status Passed Evaluation Date 08/04/2024 at 10:38:34 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 Setting	Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)										
Extended Evidence: POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P- 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: Passed MEDIUN POHK1API.hk.standardchartered.com Previous Status Passed Evaluation Date 08/04/2024 at 10:38:34 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_type, success, failure, enabled_option, and entity_name. Expected matches regular expression list	riotaui			-	•	ES:BY USER:ALL USERS						
POLICY_NAME SCB_AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P— 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: Passed MEDIUN POHK1API.hk.standardchartered.com) Instance oracle19:1:1621:POHK1API.hk.standardchartered.com Passed 08/04/2024 at 10:38:34 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	Extended Ex			ELECTRIC ROBE.	D 11011.120.1	EO.DT COERCIEE COERC						
SCB_AUDIT_DDL_P- OLICY (1.25) 14345 Status of auditing for 'DROP ROLE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUN POHK1API.hk.standardchartered.com) Instance oracle19:1:1621:POHK1API.hk.standardchartered.com Previous Status Passed 08/04/2024 at 10:38:34 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_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				AUDIT ODTION TVDE	CITCCECC	EVILLIDE	EMADLED ODTION	ENTITY NAME				
(1.25) 14345 Status of auditing for 'DROP ROLE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUN POHK1API.hk.standardchartered.com) Instance oracle19:1:1621:POHK1API.hk.standardchartered.com Previous Status Passed 08/04/2024 at 10:38:34 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_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	_		_					_				
POHK1API.hk.standardchartered.com) Instance oracle19:1:1621:POHK1API.hk.standardchartered.com Previous Status Passed Evaluation Date 08/04/2024 at 10:38:34 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		DL_P-	ALIER ROLE	STANDARD ACTION	IES	IES	DI USEK	ALL USERS				
Instance oracle19:1:1621:POHK1API.hk.standardchartered.com Previous Status Passed Evaluation Date 08/04/2024 at 10:38:34 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	(1 OF) 1 10 1F	04.4				1141 1140 4	1004					
Instance oracle19:1:1621:POHK1API.hk.standardchartered.com Previous Status Passed Evaluation Date 08/04/2024 at 10:38:34 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	(1.25) 14345	POH	is of auditing for K1API.hk.standar	'DROP ROLE' privil	ege (Unified A	uditing)(oracle19:1:	1621: Passe	ed MEDIUM				
Previous Status Passed 08/04/2024 at 10:38:34 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_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	Instance			•	artered.com							
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												
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	Evaluation Date		08/04/2024 at 10:3	38:34 PM (GMT+0530)								
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												
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												
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												
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								5/41144111011264				
Expected matches regular expression list .*:DROP ROLE.*:YES:YES:.*:* OR, any of the selected values below: Setting not found		Ŭ										
Expected matches regular expression list .*:DROP ROLE.*:YES:YES:.*:* OR, any of the selected values below: Setting not found	The following	List Str	ring value(s) of X ind	licates the status of the	DROP ROLE and	it option type defined or e enabled option, and e	n the database. The outp	out contains colon				
.*:DROP ROLE.:*:YES:YES:.*:* OR, any of the selected values below: Setting not found	separated valu	100 01			c, success, fundi	e, enablea_option, and e	nercy_name.					
OR, any of the selected values below: Setting not found		matches regular expression list										
Setting not found												
_ ~		.*:DRC	OP ROLE:.*:YES:YES:.	*. *								
		.*:DR0	OP ROLE:.*:YES:YES:.* any of the selecte	*. *								

Actual La	Actual Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)								
SC	B_AUDIT_DDL_POLICY:	DROP ROLE:STANDAR	D 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 OLICY	P- DROP ROLE	STANDARD ACTION	YES	YES	BY USER	ALL USERS			

(1.25) 14345 Status of auditing for 'DROP ROLE' privilege (Unified Auditing)(oracle19:1:1621: Passed **MEDIUM** POHK3CCD.hk.standardchartered.com)

oracle19:1:1621:POHK3CCD.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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. matches regular expression list *:DROP ROLE:.*:YES:YES:.*:.* OR, any of the selected values below: Setting not found Table not found Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) Actual SCB_AUDIT_DDL_POLICY:DROP ROLE:STANDARD ACTION:YES:YES:BY USER:ALL USERS **Extended Evidence:** POLICY_NAME AUDIT_OPTION_TYPE SUCCESS ENABLED_OPTION ENTITY_NAME AUDIT_OPTION FAILURE. ALL USERS SCB_AUDIT_DDL_P- DROP ROLE STANDARD ACTION YES YES BY USER OLICY

(1.25) 14345 Status of auditing for 'DROP ROLE' privilege (Unified Auditing)(oracle19:1:1621: **Passed MEDIUM** POHK1RCT.hk.standardchartered.com)

oracle19:1:1621:POHK1RCT.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 value	separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.								
Expected	matc	hes regular expres	ssion list						
	.*:DRC	OP ROLE:.*:YES:YES:.*:	*						
	OR, a	any of the selected	d values below:						
	Setting not found								
	Table not found								
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM (GMT+0530)					
	SCB_A	AUDIT_DDL_POLICY:E	ROP ROLE:STANDAR	D ACTION:YES:YES:BY	USER:ALL USERS				
Extended E	viden	ce:							
POLICY_NAM	Е	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_D	DL_P-	DROP ROLE	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.25) 14345 Status of auditing for 'DROP ROLE' privilege (Unified Auditing)(oracle19:1:1621: POHK5CCD.hk.standardchartered.com)

oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Instance

Evaluation Date 08/04/2024 at 10:38:34 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.

Extended Evidence:

POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME

SCB_AUDIT_DDL_PDROP ROLE STANDARD ACTION YES YES BY USER ALL USERS

(1.25) 14345 Status of auditing for 'DROP ROLE' privilege (Unified Auditing)(oracle19:1:1621: POHK1CAT.hk.standardchartered.com)

Passed MEDIUM

Passed

MEDIUM

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(1.25) 14345 Status of auditing for 'DROP ROLE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	matc	matches regular expression list									
	.*:DRC	.*:DROP ROLE::*:YES:YES::*:*									
	OR, a	OR, any of the selected values below:									
Setting not found											
	Table not found										
A = 1 1	1 1	l ll - (l - 00/04/00/	04 -4 00-04-00 DM	OMT . 0500)							
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)										
	SCB_A	SCB_AUDIT_DDL_POLICY:DROP ROLE:STANDARD ACTION:YES:YES:BY USER:ALL USERS									
Extended E	Extended Evidence:										
POLICY_NAM	Ε	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME				
SCB_AUDIT_I OLICY	DL_P-	DROP ROLE	STANDARD ACTION	YES	YES	BY USER	ALL USERS				

(1.25) 14345 Status of auditing for 'DROP ROLE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_type, success, failure, enabled_option, and entity_name.

separateu vait	separated values of policy_name, addit_option_type, success, failure, enabled_option, and endty_name.								
Expected	pected matches regular expression list								
	.*:DROP ROLE:.*:YES:YES:.*:.*								
	OR, any of the selected values below:								
	Set	tting not found							
	Ta	ble not found							
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM ((GMT+0530)					
	SCB_A	AUDIT_DDL_POLICY:I	ROP ROLE:STANDAR	D ACTION:YES:YES:BY	USER:ALL USERS				
Extended E	Extended Evidence:								
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_D OLICY	DL_P-	DROP ROLE	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.25) 14345 Status of auditing for 'DROP ROLE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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									
	Tal	ole 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 Ev	Extended Evidence:									
POLICY_NAMI	3	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCB_AUDIT_D	DL_P-	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. **MEDIUM Passed** hk.standardchartered.com)

oracle19:1:1621:POHK1API.hk.standardchartered.com Instance

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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_P- GRANT STANDARD ACTION YES YES BY USER ALL USERS OLICY

(1.26) 14346 Status of auditing for 'GRANT' privilege (Unified Auditing)(oracle19:1:1621:POHK3CCD. Passed **MEDIUM** hk.standardchartered.com)

oracle19:1:1621:POHK3CCD.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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

separateu vaiu	eparated values of policy_name, addit_option, addit_option_type, success, failure, enabled_option, and enuty_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	AUD	IT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_DD OLICY	L_P- GRAI	NT	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.26) 14346 Status of auditing for 'GRANT' privilege (Unified Auditing)(oracle19:1:1621:POHK1RCT. Passed MEDIUM hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	d 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 Evi	idence:									
POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME				
SCB_AUDIT_DD OLICY	L_P- GRANT	STANDARD ACTION	YES	YES	BY USER	ALL USERS				

(1.26) 14346 Status of auditing for 'GRANT' privilege (Unified Auditing)(oracle19:1:1621:POHK5CCD. Passed MEDIUM hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

.*: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:** AUDIT_OPTION_TYPE SUCCESS POLICY_NAME AUDIT_OPTION **FAILURE** ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P- GRANT STANDARD ACTION YES YES BY USER ALL USERS OLICY

(1.26) 14346 Status of auditing for 'GRANT' privilege (Unified Auditing)(oracle19:1:1621:POHK1CAT. Passed MEDIUM hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 CRANT 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									
	.*:GRA	.*:GRANT:.*:YES:YES:.*:.*								
	OR, any of the selected values below:									
	Set	ting not found								
	Tal	ole not found								
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM (GMT+0530)						
	SCB_A	AUDIT_DDL_POLICY:0	GRANT:STANDARD AC	TION:YES:YES:BY USE	R:ALL USERS					
Extended Ev	videnc	ce:								
POLICY_NAMI	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCB_AUDIT_DI	DL_P-	GRANT	STANDARD ACTION	YES	YES	BY USER	ALL USERS			

(1.26) 14346 Status of auditing for 'GRANT' privilege (Unified Auditing)(oracle19:1:1621:POHK4CCD. Passed MEDIUM hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:** AUDIT_OPTION_TYPE SUCCESS POLICY_NAME AUDIT_OPTION **FAILURE** ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P- GRANT STANDARD ACTION YES YES BY USER ALL USERS OLICY

(1.26) 14346 Status of auditing for 'GRANT' privilege (Unified Auditing)(oracle19:1:1621:POHK1CCD. Passed MEDIUM hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 CRANT audit ontion type defined on the database. The output contains colon

separated values of policy_name, audit_option, type, success, failure, enabled_option, and entity_name.									
Expected n	matches regular expression list								
*	.*:GRANT:.*:YES:YES:.*:.*								
C	OR, any of the selected values below:								
	Setting not found								
	Table not found								
Actual L	ast Updated:08/04/20	24 at 06:01:09 PM ((GMT+0530)						
S	CB_AUDIT_DDL_POLICY:	GRANT:STANDARD AC	TION:YES:YES:BY USE	R:ALL USERS					
Extended Evid	lence:								
POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCB_AUDIT_DDI	_P- GRANT	STANDARD ACTION	YES	YES	BY USER	ALL USERS			

(1.26) 14346 Status of auditing for 'GRANT' privilege (Unified Auditing)(oracle19:1:1621:POHK2CCD. Passed MEDIUM hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 separated value	following List String value(s) of X indicates the status of the GRANT audit option type defined on the database. The output contains colon arated 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 L	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)								
S	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_DDI	_P- GRANT	STANDARD ACTION	YES	YES	BY USER	ALL USERS			

(1.27) 14347 Status of auditing for 'REVOKE' privilege (Unified Auditing)(oracle19:1:1621:POHK1API. Passed MEDIUM hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 separated valu	following List String value(s) of X indicates the status of the REVOKE audit option type defined on the database. The output contains colon trated 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, a	any of the selected	l values below:						
	Set	ting not found							
	Tal	ble not found							
Actual		<u> </u>	24 at 06:01:09 PM (•	ED.ALI LICEDO				
	SCB_F	AUDIT_DDL_POLICY:R	EVUKE:STANDARD A	CTION:YES:YES:BY US	EK:ALL USEKS				
Extended Ev	/idend	e:							
POLICY_NAMI	3	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_D OLICY	DL_P-	REVOKE	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.27) 14347 Status of auditing for 'REVOKE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 r	matches regular expression list							
.*	.*:REVOKE:.*:YES:YES:.**							
C	OR, any of the selected	d values below:						
	Setting not found							
	Table not found							
Actual L	_ast Updated:08/04/20	24 at 06:01:09 PM (GMT+0530)					
S	SCB_AUDIT_DDL_POLICY:I	REVOKE:STANDARD A	CTION:YES:YES:BY US	ER:ALL USERS				
Extended Evidence:								
POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_DDI	L_P- REVOKE	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.27) 14347 Status of auditing for 'REVOKE' privilege (Unified Auditing)(oracle19:1:1621:POHK1RCT. **MEDIUM** Passed hk.standardchartered.com)

oracle19:1:1621:POHK1RCT.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 ontion 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:							
	Set	tting not found						
	Ta	ble not found						
Actual	Last	Updated:08/04/20	24 at 06:01:09 PM (GMT+0530)				
	SCB_A	AUDIT_DDL_POLICY:I	REVOKE:STANDARD A	CTION:YES:YES:BY U	SER:ALL USERS			
Extended E	Extended Evidence:							
POLICY_NAM	1E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_I OLICY	DDL_P-	REVOKE	STANDARD ACTION	YES	YES	BY USER	ALL USERS	

(1.27) 14347 Status of auditing for 'REVOKE' privilege (Unified Auditing)(oracle19:1:1621: **MEDIUM Passed** POHK5CCD.hk.standardchartered.com)

oracle19:1:1621:POHK5CCD.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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 RFVOKF audit option type defined on the database. The output contains colon

separated valu	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 E	Extended Evidence:								
POLICY_NAM	E AUDIT_OPTION	AUDIT_OPTION_TYPE SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME				

SCB_AUDIT_DDL_P- REVOKE OLICY (1.27) 14347 Status of auditing for 'REVOKE' privilege (Unified Auditing)(oracle19:1:1621: **Passed MEDIUM**

YES

BY USER

ALL USERS

STANDARD ACTION YES

POHK1CAT.hk.standardchartered.com) Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_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:** AUDIT OPTION TYPE SUCCESS ENABLED OPTION POLICY NAME AUDIT OPTION **FAILURE** ENTITY_NAME

YES

BY USER

ALL USERS

MEDIUM

(1.27) 14347 Status of auditing for 'REVOKE' privilege (Unified Auditing)(oracle19:1:1621: Passed POHK4CCD.hk.standardchartered.com)

STANDARD ACTION YES

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

SCB_AUDIT_DDL_P- REVOKE

Evaluation Date 08/04/2024 at 10:38:34 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.

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

(1.27) 14347 Status of auditing for 'REVOKE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

separated vare	separated values of policy_name, addit_option, addit_option_type, success, name e, enabled_option, and enabled_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_A	AUDIT_DDL_POLICY:F	REVOKE:STANDARD A	CTION:YES:YES:BY US	ER:ALL USERS				
Extended Evidence:									
POLICY_NAM	Е	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_D OLICY	DL_P-	REVOKE	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.27) 14347 Status of auditing for 'REVOKE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:									
	Set	ting not found								
	Tal	ole not found								
Actual	Lact		04 at 06:01:00 DM /	CMT - 0530\						
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_NAMI	3	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCB_AUDIT_D OLICY	DL_P-	REVOKE	STANDARD ACTION	YES	YES	BY USER	ALL USERS			

(1.28) 14348 Status of auditing for 'CREATE PROFILE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

colon separate	d 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 Ev	vidence:

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

(1.28) 14348 Status of auditing for 'CREATE PROFILE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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, a	OR, any of the selected values below:								
	Set	ting not found								
	Tal	ole not found								
Actual	Loot	l Indoted .00/04/201	04 at 06:04:00 DM /	CMT - 0520\						
Actual	Last	Updated:06/04/20/	24 at 06:01:09 PM (GIVI I +0530)						
	SCB_AUDIT_DDL_POLICY:CREATE PROFILE:STANDARD ACTION:YES:YES:BY USER:ALL USERS									
Extended Evidence:										
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCB_AUDIT_D	DL_P-	CREATE PROFILE	STANDARD ACTION	YES	YES	BY USER	ALL USERS			

(1.28) 14348 Status of auditing for 'CREATE PROFILE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

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:							
	Set	ting not found						
	Tal	ole not found						
Actual	1	l lin data d.00/04/201	04 -4 0C-04-00 DM /	CMT - 0520\				
Actual	Last	Updated:08/04/20/	24 at 06:01:09 PM (GIVI I +0530)				
	SCB_A	AUDIT_DDL_POLICY:0	CREATE PROFILE:STAN	NDARD ACTION:YES:Y	ES:BY USER:ALL USEF	RS		
Extended Evidence:								
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_D OLICY	DL_P-	CREATE PROFILE	STANDARD ACTION	YES	YES	BY USER	ALL USERS	

(1.28) 14348 Status of auditing for 'CREATE PROFILE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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- CREATE PROFILE STANDARD ACTION YES YES BY USER ALL USERS

(1.28) 14348 Status of auditing for 'CREATE PROFILE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

OLICY

Evaluation Date 08/04/2024 at 10:38:34 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 SCB_AUDIT_DDL_POLICY:CREATE PROFILE:SYSTEM PRIVILEGE:YES:YES:BY USER:ALL USERS **Extended Evidence:** POLICY_NAME AUDIT_OPTION_TYPE SUCCESS **FAILURE** ENABLED_OPTION ENTITY_NAME AUDIT_OPTION SCB_AUDIT_DDL_P- CREATE PROFILE SYSTEM PRIVILEGE YES YES BY USER ALL USERS OLICY SCB_AUDIT_DDL_P- CREATE PROFILE STANDARD ACTION YES YES BY USER ALL USERS

(1.28) 14348 Status of auditing for 'CREATE PROFILE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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. matches regular expression list **Expected** *:CREATE PROFILE:.*:YES:YES:.*:.* OR, any of the selected values below: Setting not found Table not found Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) Actual 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- CREATE PROFILE OLICY STANDARD ACTION YES YES BY USER ALL USERS (1.28) 14348 Status of auditing for 'CREATE PROFILE' privilege (Unified Auditing)(oracle19:1:1621: **MEDIUM Passed** POHK1CCD.hk.standardchartered.com) oracle19:1:1621:POHK1CCD.hk.standardchartered.com Instance Previous Status Passed **Evaluation Date** 08/04/2024 at 10:38:34 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. matches regular expression list *:CREATE PROFILE:.*:YES:YES:.*:.* OR, any of the selected values below: Setting not found Table not found Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) Actual 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- CREATE PROFILE STANDARD ACTION YES BY USER ALL USERS (1.28) 14348 Status of auditing for 'CREATE PROFILE' privilege (Unified Auditing)(oracle19:1:1621: **Passed MEDIUM** POHK2CCD.hk.standardchartered.com) oracle19:1:1621:POHK2CCD.hk.standardchartered.com Instance Previous Status **Evaluation Date** 08/04/2024 at 10:38:34 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:

Oracle ATOS - 20240806 page 395

Setting not found

	Tal	Table not found							
Actual	Last	ast 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 Ev	videnc	e:							
POLICY_NAME	3	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_DI OLICY	DL_P-	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: Passed MEDIUM POHK1API.hk.standardchartered.com)

Instance oracle 19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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, a	OR, any of the selected values below:							
	Setting not found								
	Tal	ble not found							
Actual	Loct		04 at 06:01:00 BM	CMT . 0520\					
Actual		Updated:08/04/202		•					
	SCB_AUDIT_DDL_POLICY:ALTER PROFILE:STANDARD ACTION:YES:YES:BY USER:ALL USERS								
Extended Ex	Extended Evidence:								
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_D OLICY	DL_P-	ALTER PROFILE	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.29) 14349 Status of auditing for 'ALTER PROFILE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

OLICY

Evaluation Date 08/04/2024 at 10:38:34 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.

separated valu	es or policy_name, audit_op	otion, audit_option_typ	e, success, failure, en	abied_option, and ent	пу_патте.			
Expected	matches regular expre	ession list						
	.*:ALTER PROFILE:.*:YES:YES:.**							
	OR, any of the selected values below:							
	Setting not found							
	Table not found							
Actual	Last Updated:08/04/20	24 at 06:01:00 PM (GMT+0530)					
Actual	Last Opuated.00/04/20	24 at 00.01.03 1 m (CW1+0550)					
	SCB_AUDIT_DDL_POLICY:	ALTER PROFILE:STAND	OARD ACTION:YES:YE	S:BY USER:ALL USER	S			
Extended Ev	vidence:							
POLICY_NAMI	E AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCR AUDIT D	OL P_ ALTER PROFILE	STANDARD ACTION	VEC	VEC	BA HEED	VII LICEDO		

(1.29) 14349 Status of auditing for 'ALTER PROFILE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	matc	hes regular expres	ssion list						
	.*:ALT	.*:ALTER PROFILE:.*:YES:YES:.*:.*							
	OR, any of the selected values below:								
	Set	tting not found							
	Ta	ble not found							
				(ALIT ALIA)					
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM ((GMT+0530)					
	SCB_A	AUDIT_DDL_POLICY:A	ALTER PROFILE:STANI	DARD ACTION:YES:YE	S:BY USER:ALL USERS	5			
Extended E	Extended Evidence:								
POLICY_NAM	ſΕ	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_I OLICY	DDL_P-	ALTER PROFILE	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.29) 14349 Status of auditing for 'ALTER PROFILE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 TYPE SUCCESS FAIL LIPE FINARLED OPTION ENTITY NAME

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		

(1.29) 14349 Status of auditing for 'ALTER PROFILE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	matc	hes regular expre	ssion list						
	.*:ALT	ER PROFILE:.*:YES:YE	S:.*:.*						
	OR, any of the selected values below:								
	Set	ting not found							
	Tal	ble not found							
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM ((GMT+0530)					
	SCB_A	SCB_AUDIT_DDL_POLICY:ALTER PROFILE:STANDARD ACTION:YES:YES:BY USER:ALL USERS							
	SCB_A	AUDIT_DDL_POLICY: <i>A</i>	ALTER PROFILE:SYSTE	M PRIVILEGE:YES:YE	ES:BY USER:ALL USERS	5			
Extended Ev	/iden	ce:							
POLICY_NAMI	3	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_D: OLICY	DL_P-	ALTER PROFILE	SYSTEM PRIVILEGE	YES	YES	BY USER	ALL USERS		
SCB_AUDIT_D: OLICY	DL_P-	ALTER PROFILE	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.29) 14349 Status of auditing for 'ALTER PROFILE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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- ALTER PROFILE STANDARD ACTION YES YES BY USER ALL USERS

(1.29) 14349 Status of auditing for 'ALTER PROFILE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	matc	hes regular expr	ession list						
	.*:ALTER PROFILE:.*:YES:YES:.*:.*								
	OR, any of the selected values below:								
	Set	tting not found							
	Tal	ble not found							
Actual	Last	Updated:08/04/20	024 at 06:01:09 PM ((GMT+0530)					
	SCB_A	AUDIT_DDL_POLICY	:ALTER PROFILE:STANI	DARD ACTION:YES	S:YES:BY USER:ALL USI	ERS			
Extended E	Evidend	ce:							
POLICY_NAN	ИE	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_I OLICY	DDL_P-	ALTER PROFILE	STANDARD ACTION		YES	BY USER	ALL USERS		
20) 1/3/	Stati	is of auditing for	'ALTER PROFILE' p	vrivilana (I Inifia	d Auditing)(oracle1	9:1:1621: Passe	ed MEDIUM		
1.23) 1434	POH	K2CCD.hk.standa	ardchartered.com)	nivilege (Online	a Additing/(oracle)	3.1.1021. Fasse	EG IVILDIOW		
stance		oracle19:1:1621:PC	DHK2CCD.hk.standardcl	hartered.com					
revious Statu	S	Passed							
valuation Dat Pracle data omplexity	base prules a	08/04/2024 at 10: profiles are used and reuse restrict	tions. Logging and	e usage limits a monitoring of a	all attempts to alter	ssword policies such profiles, whether su	uccessful or		
valuation Dat Oracle data omplexity insuccessful equiremen	base prules aul, may	08/04/2024 at 10: profiles are used nd reuse restrict provide clues a d be set as appr	to enforce resourc tions. Logging and and forensic eviden copriate to the need	e usage limits monitoring of a ces about pote is of the busine	all attempts to alter ential suspicious/ur ess.	r profiles, whether sunauthorized activities	uccessful or s. This logging		
valuation Data Oracle data omplexity nsuccessfuequiremen The following separated value	base prules a ul, may t shoul	08/04/2024 at 10: profiles are used nd reuse restrict provide clues a d be set as appr	to enforce resource tions. Logging and and forensic evident ropriate to the need dicates the status of the option, audit_option_typ	e usage limits monitoring of a ces about pote is of the busine	all attempts to alter ential suspicious/ur ess.	r profiles, whether sunauthorized activities	uccessful or s. This logging		
valuation Data Oracle data omplexity nsuccessfuequiremen The following separated value	base prules a ul, may t shoul	orofiles are used nd reuse restrict provide clues a d be set as appropring value(s) of X incoolicy_name, audit_o	to enforce resource tions. Logging and and forensic eviden repriate to the need dicates the status of the option, audit_option_typession list	e usage limits monitoring of a ces about pote is of the busine	all attempts to alter ential suspicious/ur ess.	r profiles, whether sunauthorized activities	uccessful or s. This logging		
valuation Data Oracle data omplexity nsuccessfuequirement The following separated value	base prules a ul, may t shoul g List Strues of p matc .*:ALT	08/04/2024 at 10: profiles are used nd reuse restrict provide clues a d be set as approring value(s) of X incolicy_name, audit_o thes regular expressions.	to enforce resource tions. Logging and and forensic eviden repriate to the need dicates the status of the option, audit_option_typession list	e usage limits monitoring of a ces about pote is of the busine	all attempts to alter ential suspicious/ur ess.	r profiles, whether sunauthorized activities	uccessful or s. This logging		
omplexity nsuccessforments	base prules a ul, may t shoul g List Strues of p	one of the second of the second reuse restrict of provide clues and be set as approximately provide set as approximately provide set as approximately provide set as approximately one of the second o	to enforce resource tions. Logging and and forensic eviden repriate to the need dicates the status of the option, audit_option_typession list	e usage limits monitoring of a ces about pote is of the busine	all attempts to alter ential suspicious/ur ess.	r profiles, whether sunauthorized activities	uccessful or s. This logging		
valuation Data Oracle data omplexity nsuccessfuequirement The following separated value	base prules a ul, may t shoul g List Struces of p matc *:ALT OR, a	one of the selected	to enforce resource tions. Logging and and forensic eviden repriate to the need dicates the status of the option, audit_option_typession list	e usage limits monitoring of a ces about pote is of the busine	all attempts to alter ential suspicious/ur ess.	r profiles, whether sunauthorized activities	uccessful or s. This logging		
valuation Date Oracle data omplexity of the sequirement The following separated valuations Expected	base prules a ul, may t shoul g List Structures of p matc *:ALT OR, a Set	one of the selected ting not found found in the set as approximate a set as approximate and the set as a set as	to enforce resource tions. Logging and and forensic eviden repriate to the need dicates the status of the option, audit_option_typession list	e usage limits monitoring of a ces about pote is of the busine ALTER PROFILE a pe, success, failure,	all attempts to alter ential suspicious/ur ess.	r profiles, whether sunauthorized activities	uccessful or s. This logging		
valuation Date Oracle data omplexity nsuccessfrequirement The following separated valuation Expected	base prules a ul, may t shoul g List Struces of p matc .*:ALT OR, a Set Tal	one of the selected and found reuse restrict of provide clues and be set as approximately provide (s) of X incolicy_name, audit_outless regular expressive any of the selected ting not found ble not found the one of the selected the outless of the selected	to enforce resource tions. Logging and and forensic evident ropriate to the need dicates the status of the option, audit_option_typession list YES: *: * ed values below:	e usage limits monitoring of a ces about pote is of the busined ALTER PROFILE abe, success, failure, (GMT+0530)	all attempts to alter ential suspicious/ur ess. audit option type defin , enabled_option, and e	r profiles, whether sunauthorized activities ed on the database. The entity_name.	uccessful or s. This logging		
valuation Date Oracle data omplexity nsuccessfrequirement The following separated valuate Expected Actual	base prules a ul, may t shoul g List Structures of p matc .*:ALT OR, a Set Tal	one of the selected ting not found by confiles are used and reuse restrict of provide clues and be set as approximately provide clues and be set as approximately of X incoolicy_name, audit_outless regular expressive any of the selected ting not found be be not found by confile in the selected ting not found be not found by confirmation of the selected ting not found by confile in the selected ting not found by confirmation of the selected ting not found the select	to enforce resource tions. Logging and and forensic evident propriate to the need dicates the status of the option, audit_option_typession list VES:*:* ed values below:	e usage limits monitoring of a ces about pote is of the busined ALTER PROFILE abe, success, failure, (GMT+0530)	all attempts to alter ential suspicious/ur ess. audit option type defin , enabled_option, and e	r profiles, whether sunauthorized activities ed on the database. The entity_name.	uccessful or s. This logging		
valuation Data Oracle data omplexity nsuccessfuequirement The following separated value	base prules a ul, may t shoul g List Struces of p matc .*:ALT OR, a Set Tal Last SCB_A	one of the selected ting not found by confiles are used and reuse restrict of provide clues and be set as approximately provide clues and be set as approximately of X incoolicy_name, audit_outless regular expressive any of the selected ting not found be be not found by confile in the selected ting not found be not found by confirmation of the selected ting not found by confile in the selected ting not found by confirmation of the selected ting not found the select	to enforce resource tions. Logging and and forensic evident propriate to the need dicates the status of the option, audit_option_typession list VES:*:* ed values below:	e usage limits monitoring of a ces about pote is of the busined ALTER PROFILE abe, success, failure, and action: YES	all attempts to alter ential suspicious/ur ess. audit option type defin , enabled_option, and e	r profiles, whether sunauthorized activities ed on the database. The entity_name.	uccessful or s. This logging		

(1.30) 14350 Status of auditing for 'DROP PROFILE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

separated val	ues 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						

Aotaai	Euce opudiod.00/04/2024 at 00.01.00 f iii (Oiii 1 0000)								
S	SCB_AUDIT_DDL_POLICY:DROP PROFILE:STANDARD ACTION:YES:YES:BY USER:ALL USERS								
Extended Evi	Extended Evidence:								
POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCB_AUDIT_DD	L_P- DROP PROFILE	STANDARD ACTION	YES	YES	BY USER	ALL USERS			

(1.30) 14350 Status of auditing for 'DROP PROFILE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

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

Previous Status Passed

Actual

Evaluation Date 08/04/2024 at 10:38:34 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	matc	hes regular expre	ssion list						
	.*:DRC	.*:DROP PROFILE::*:YES:YES::*:.*							
	OR, a	OR, any of the selected values below:							
	Set	tting not found							
	Ta	ble not found							
Actual	Look Undeted-00/04/2024 at 00:04:00 PM (CMT: 0520)								
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)								
	SCB_A	SCB_AUDIT_DDL_POLICY:DROP PROFILE:STANDARD ACTION:YES:YES:BY USER:ALL USERS							
Extended E	viden	ce:							
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_D	DL_P-	DROP PROFILE	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.30) 14350 Status of auditing for 'DROP PROFILE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

separated values	of policy_name, audit_op	tion, audit_option_typ	oe, success, failure, ena	abled_option, and enti	ity_name.	•		
Expected m	atches regular expre	ssion list						
.*:]	.*:DROP PROFILE:.*:YES:YES:.*:.*							
OI	OR, any of the selected values below:							
	Setting not found							
	Table not found							
Actual La	st Updated:08/04/20	24 at 06:01:09 PM ((GMT+0530)					
SC	B_AUDIT_DDL_POLICY:I	DROP PROFILE:STAND	ARD ACTION:YES:YES	:BY USER:ALL USERS				
Extended Evid	Extended Evidence:							
POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_DDL_	P- DROP PROFILE	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.30) 14350 Status of auditing for 'DROP PROFILE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_type, success, failure, enabled_option, and entity_name.

Expected	matc	hes regular expres	ssion list						
	.*:DRC	OP PROFILE:.*:YES:YES	5:.*:.*						
	OR, any of the selected values below:								
	Setting not found								
	Tal	ble not found							
Actual	Lact	Undated:09/04/201	24 at 06:01:09 PM ((CMT : 0530)					
Actual		-		•					
	SCB_AUDIT_DDL_POLICY:DROP PROFILE:STANDARD ACTION:YES:YES:BY USER:ALL USERS								
Extended E	viden	ce:							
POLICY_NAM	ΙE	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_I	DDL_P-	DROP PROFILE	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.30) 14350 Status of auditing for 'DROP PROFILE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 separated value	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	matc	hes regular expre	ssion list				
	.*:DRC	OP PROFILE:.*:YES:YE	5:.*:.*				
	OR, a	any of the selected	d values below:				
	Set	ting not found					
	Tal	ble not found					
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM (GMT+0530)			
	SCB_A	AUDIT_DDL_POLICY:I	OROP PROFILE:STAND	ARD ACTION:YES:YES	S:BY USER:ALL USERS		
	SCB_A	AUDIT_DDL_POLICY:I	DROP PROFILE:SYSTE	M PRIVILEGE:YES:YES	S:BY USER:ALL USERS		
Extended E	vidend	ce:					
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_D OLICY	DL_P-	DROP PROFILE	SYSTEM PRIVILEGE	YES	YES	BY USER	ALL USERS
SCB_AUDIT_D OLICY	DL_P-	DROP PROFILE	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.30) 14350 Status of auditing for 'DROP PROFILE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 n	matches regular expression list									
.*	.*:DROP PROFILE::*:YES:YES::*:*									
C	OR, any of the selected values below:									
	Setting not found									
	Table not found									
Actual L	ast Updated:08/04/20	24 at 06:01:09 PM (GMT+0530)							
S	CB_AUDIT_DDL_POLICY:	DROP PROFILE:STAND	ARD ACTION:YES:YES	:BY USER:ALL USERS						
Extended Evid	dence:									
POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME				
SCB_AUDIT_DDI OLICY	_P- DROP PROFILE	STANDARD ACTION	YES	YES	BY USER	ALL USERS				

(1.30) 14350 Status of auditing for 'DROP PROFILE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

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

(1.30) 14350 Status of auditing for 'DROP PROFILE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

	.*:DR0	.*:DROP PROFILE:.*:YES:YES::*:.*									
	OR, any of the selected values below:										
	Se	tting not found									
	Ta	ble not found									
Actual	Last	Updated:08/04/20	24 at 06:01:09 PM (GMT+0530)							
	SCB_	AUDIT_DDL_POLICY:1	DROP PROFILE:STAND	ARD ACTION:YES:Y	ES:BY USER:ALL USERS						
Extended E	Eviden	ce:									
POLICY_NAN	ЛE	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME				
SCB_AUDIT_I	DDL_P-	DROP PROFILE	STANDARD ACTION	YES	YES	BY USER	ALL USERS				
(1.31) 1435	1 Stati (orad	us of auditing for ' cle19:1:1621:POHI	CREATE DATABAS K1API.hk.standard	SE LINK' privilege chartered.com)	e (Unified Auditing)	Passe	ed MEDIUM				
Instance		oracle19:1:1621:PO	HK1API.hk.standardch	artered.com							
Previous Statu	S	Passed									
Evaluation Dat	ie.	08/04/2024 at 10:3	38:34 PM (GMT+0530)	1							
available wi database lir	thout t nks, wl	urther authentica nether successful	tion once the link i or unsuccessful, i	s established. L may provide clue	nnections to other ogging and monito es and forensic evidence set as appropriate	ring of all attempt dences about pot	s to create ential				

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	matc	hes regular expres	ssion list							
	.*:CREATE DATABASE LINK:.*:YES:YES**									
	OR, any of the selected values below:									
	Setting not found									
	Table not found									
Astual	Last	l lo dete d.00/04/00	04 -4 0C-04-00 DM /	(CMT - 0520)						
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM ((GIVI I +0530)						
	SCB_A	AUDIT_DDL_POLICY:0	CREATE DATABASE LII	NK:STANDARD ACTIO	N:YES:YES:BY USER:A	LL USERS				
Extended E	Extended Evidence:									
POLICY_NAM	Έ	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCB_AUDIT_D	DL_P-	CREATE DATABASE	STANDARD ACTION	YES	YES	BY USER	ALL USERS			

(1.31) 14351 Status of auditing for 'CREATE DATABASE LINK' privilege (Unified Auditing) Passed MEDIUM (oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_type, success, failure, enabled_option, and entity_name.

Expected matches regular expression list

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_P- OLICY	CREATE DATABASE LINK	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.31) 14351 Status of auditing for 'CREATE DATABASE LINK' privilege (Unified Auditing) (oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

Passed MEDIUM

oracle19:1:1621:POHK1RCT.hk.standardchartered.com Instance

Passed Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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:** AUDIT_OPTION_TYPE SUCCESS ENABLED_OPTION POLICY_NAME AUDIT_OPTION **FAILURE** ENTITY_NAME SCB_AUDIT_DDL_P- CREATE DATABASE STANDARD ACTION YES YES BY USER ALL USERS

(1.31) 14351 Status of auditing for 'CREATE DATABASE LINK' privilege (Unified Auditing) (oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Passed Previous Status

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

LINK

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 Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) Actual 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_P- CREATE DATABASE STANDARD ACTION YES OLICY YES BY USER ALL USERS

(1.31) 14351 Status of auditing for 'CREATE DATABASE LINK' privilege (Unified Auditing) (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	matc	matches regular expression list								
	.*:CRE	ATE DATABASE LINK	:.*:YES:YES:.*:.*							
	OR, any of the selected values below:									
	Setting not found									
	Table not found									
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM (GMT+0530)						
	SCB_A	AUDIT_DDL_POLICY:0	CREATE DATABASE LI	NK:STANDARD ACTIO	N:YES:YES:BY USER:A	LL USERS				
	SCB_A	AUDIT_DDL_POLICY:0	REATE DATABASE LI	NK:SYSTEM PRIVILEG	E:YES:YES:BY USER:A	LL USERS				
Extended Ex	viden	ce:								
POLICY_NAM	Е	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCB_AUDIT_D OLICY	DL_P-	CREATE DATABASE LINK	SYSTEM PRIVILEGE	YES	YES	BY USER	ALL USERS			
SCB_AUDIT_D OLICY	DL_P-	CREATE DATABASE LINK	STANDARD ACTION	YES	YES	BY USER	ALL USERS			

(1.31) 14351 Status of auditing for 'CREATE DATABASE LINK' privilege (Unified Auditing) (oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

contains color	contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.								
Expected	matc	hes regular expre	ssion list						
	.*:CRE	ATE DATABASE LINK	:.*:YES:YES:.*:.*						
	OR, a	any of the selected	d values below:						
	Setting not found								
	Table not found								
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM (GMT+0530)					
	SCB_A	AUDIT_DDL_POLICY:(CREATE DATABASE LI	NK:STANDARD	ACTION:YES:YES:BY USER	:ALL USERS			
Extended E	vidend	ce:							
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_D OLICY	DL_P-	CREATE DATABASE LINK	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.31) 14351 Status of auditing for 'CREATE DATABASE LINK' privilege (Unified Auditing) (oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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									
	Tal	Table not found								
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)									
	SCB_A	AUDIT_DDL_POLICY:0	CREATE DATABASE LIN	NK:STANDARD ACT	TION:YES:YES:BY US	ER:ALL USERS				
Extended Ev	vidend	e:								
POLICY_NAMI	3	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCB VIIDIT D	חו ס	CDEATE DATABASE	STANDARD ACTION	VEC	VEC	BA HCED	ALL HICEDS			

(1.31) 14351 Status of auditing for 'CREATE DATABASE LINK' privilege (Unified Auditing) (oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

OLICY

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

LINK

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.

contains color	n separated values of policy ₋	_name, audit_option, a	udit_option_typ	e, success, failure, enat	oled_option, and entity_na	me.		
Expected	matches regular expre	ession list						
	.*:CREATE DATABASE LINE	<:.*:YES:YES:.*:.*						
	OR, any of the selecte	d values below:						
	Setting not found							
	Table not found							
			·					
Actual	Last Updated:08/04/20	24 at 06:01:09 PM	(GMT+0530)					
	SCB_AUDIT_DDL_POLICY:	CREATE DATABASE LI	NK:STANDARD	ACTION:YES:YES:BY US	ER:ALL USERS			
Extended E	vidence:							
POLICY_NAM	IE AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_I OLICY	DDL_P- 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.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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, a	any of the selected	d values below:					
	Setting not found							
	Tal	ble not found						
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM ((GMT+0530)				
	SCB_A	AUDIT_DDL_POLICY:/	ALTER DATABASE LINI	K:STANDARD ACTION	:YES:YES:BY USER:ALI	L USERS		
Extended Ex	viden	ce:						
POLICY_NAM	Е	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_D OLICY	DL_P-	ALTER 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:POHK3CCD.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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								
	.*:ALT	ER DATABASE LINK:.*	:YES:YES:.*:.*						
	OR, any of the selected values below:								
Setting not found									
	Tal	ole not found							
Actual	Last !	Updated:08/04/202	24 at 06:01:09 PM (GMT+0530)					
		•	LTER DATABASE LINI	•	YES:YES:BY USER:ALI	. USERS			
Extended Ev	idenc	e:							
POLICY_NAME		AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_DI OLICY		ALTER DATABASE LINK	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.32) 14352 Status of auditing for 'ALTER DATABASE LINK' privilege (Unified Auditing) Passed (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 10:38:34 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.

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 Ex	vidence:

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

(1.32) 14352 Status of auditing for 'ALTER DATABASE LINK' privilege (Unified Auditing) (oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:.	.*:ALTER DATABASE LINK::*:YES:YES:.*:.*								
	OR, any of the selected values below:									
	Setting not found									
	Table not found									
Actual	Last Updated:08/04/20	24 at 06:01:09 PM ((GMT+0530)							
	SCB_AUDIT_DDL_POLICY:	ALTER DATABASE LIN	K:STANDARD ACTION	:YES:YES:BY USER:AL	L USERS					
Extended E	vidence:									
POLICY_NAM	E AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME				
SCB_AUDIT_I OLICY	DDL_P- ALTER 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:POHK1CAT.hk.standardchartered.com)

Passed MEDIUM

oracle19:1:1621:POHK1CAT.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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 Y indicates the status of the ALTER DATARASE LINK audit ontion type defined on the database. The output

contains colon	separated values of policy_	name, audit_option, au	udit_option_type, suc	ccess, failure, enabled	option, and entity_na	me.		
Expected	matches regular expression list							
	.*:ALTER DATABASE LINK:.*:YES:YES:.**							
	OR, any of the selecte	d values below:						
	Setting not found							
	Table not found							
Actual	Last Updated:08/04/20	24 at 06:01:09 PM ((GMT+0530)					
	SCB_AUDIT_DDL_POLICY:	ALTER DATABASE LINI	K:STANDARD ACTIO	N:YES:YES:BY USER:A	LL USERS			
Extended Ev	vidence:							
POLICY_NAMI	E AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCR AUDIT D	DI P_ ALTER DATABASE	STANDARD ACTION	YFS	VFS	BY HSFR	ALL LISERS		

(1.32) 14352 Status of auditing for 'ALTER DATABASE LINK' privilege (Unified Auditing) (oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

LINK

OLICY

Evaluation Date 08/04/2024 at 10:38:34 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 contains color	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	mato	hes regular expre	ssion list				
	.*:ALT	ER DATABASE LINK:.*	*:YES:YES:.*:.*				
	OR,	any of the selected	d values below:				
	Se	tting not found					
	Ta	ble not found					
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM (GMT+0530)			
	SCB_AUDIT_DDL_POLICY:ALTER DATABASE LINK:STANDARD ACTION:YES:YES:BY USER:ALL USERS						
Extended E	Extended Evidence:						
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_D OLICY	DL_P-	ALTER 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:POHK1CCD.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) Actual SCB_AUDIT_DDL_POLICY:ALTER DATABASE LINK:STANDARD ACTION:YES:YES:BY USER:ALL USERS **Extended Evidence:** AUDIT_OPTION_TYPE SUCCESS **FAILURE** ENABLED_OPTION ENTITY_NAME POLICY_NAME AUDIT_OPTION SCB_AUDIT_DDL_P- ALTER DATABASE STANDARD ACTION YES ALL USERS YES BY USER LINK

(1.32) 14352 Status of auditing for 'ALTER DATABASE LINK' privilege (Unified Auditing) (oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	matche	es regular expre	ssion list				
	.*:ALTER DATABASE LINK:.*:YES:YES:.*:*						
	OR, an	y of the selected	d values below:				
		ng not found					
	Table	not found					
Actual	Last Up	odated:08/04/20	24 at 06:01:09 PM (GMT+0530)			
	SCB_AU	DIT_DDL_POLICY:/	ALTER DATABASE LIN	K:STANDARD ACTION	:YES:YES:BY USER:AL	L USERS	
Extended E	vidence	:					
POLICY_NAM	1E A	UDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_I OLICY		LTER DATABASE NK	STANDARD ACTION	YES	YES	BY USER	ALL USERS
(1.33) 14353	Status (oracle	of auditing for '	DROP DATABASE (1API.hk.standard	LINK' privilege (U	nified Auditing)	Passe	d MEDIUM
Instance	-		HK1API.hk.standardch	=			
Previous Status		issed	intini iimotanaaraci	arterea.com			
Evaluation Date	e 08	3/04/2024 at 10:3	8:34 PM (GMT+0530))			
						databases. These	
						ring of all attempts dences about pote	
						e to the needs of	
Suspicious/c	an laati loi	izea dolivities.	Triis logging requi	Terrierit Griodia Be	oct do appropriat	e to the needs of	aric business.
The following contains color	g List Strin n separate	g value(s) of X indi d values of policy_	cates the status of the name, audit_option, a	DROP DATABASE LIN udit_option_type, succ	IK audit option type d cess, failure, enabled_	lefined on the databas option, and entity_nar	e. The output ne.
Expected	matche	es regular expre	ssion list				
	.*:DROP	DATABASE LINK:.*	:YES:YES:.*:.*				
	OR, an	y of the selected	d values below:				
	Settir	ng not found					
	Table	not found					
Actual	Last U	odated:08/04/20	24 at 06:01:09 PM (GMT+0530)			
	SCB_AU	DIT_DDL_POLICY:I	DROP DATABASE LINK	:STANDARD ACTION:	YES:YES:BY USER:ALL	. USERS	
Extended E	vidence						
POLICY_NAM		UDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
_		ROP DATABASE	STANDARD ACTION		YES	BY USER	ALL USERS
OLICY		NK	OTTHVDTHED THE TION	110	120	DI COLK	THE COLIG
(1.33) 14353	Status	of auditing for '	DROP DATABASE	LINK' privilege (U	nified Auditing)	Passe	d MEDIUM
Instance	-		K3CCD.hk.standar d HK3CCD.hk.standardcl				
Instance Previous Status		acie19.1.1621.POI assed	TKSCCD.HK.Standardc	nartered.com			
Evaluation Date			8:34 PM (GMT+0530)	1			
Evaluation Date		5, 0 1, 202 1 dt 10.0	0.011111 (0111110000)				
Oracle datal	base link	s are used to e	establish database	-to-database con	nections to other	databases. These	connections are
						ring of all attempts	
						dences about pote	
suspicious/u	unauthor	ized activities.	This logging requi	rement should be	set as appropriat	e to the needs of	the business.
The following	g List Strin	g value(s) of X indi	cates the status of the	DROP DATABASE LIN	JK audit option type d	lefined on the databas	e. The output
contains color	n separate	d values of policy_	name, audit_option, a	udit_option_type, suc	cess, failure, enabled_	option, and entity_nar	ne.
Expected	matche	es regular expre	ssion list				
	.*:DROP	DATABASE LINK:.*	:YES:YES:.*:.*				
	OR, an	y of the selected	d values below:				
		ng 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:** AUDIT_OPTION_TYPE SUCCESS POLICY_NAME AUDIT_OPTION **FAILURE** ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P- DROP DATABASE STANDARD ACTION YES YES BY USER ALL USERS OLICY LINK

(1.33) 14353 Status of auditing for 'DROP DATABASE LINK' privilege (Unified Auditing) (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 10:38:34 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 Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) Actual SCB_AUDIT_DDL_POLICY:DROP DATABASE LINK:STANDARD ACTION:YES:YES:BY USER:ALL USERS **Extended Evidence:** AUDIT_OPTION_TYPE SUCCESS POLICY_NAME AUDIT_OPTION **FAILURE** ENTITY_NAME ENABLED OPTION SCB_AUDIT_DDL_P- DROP DATABASE LINK STANDARD ACTION YES YES BY USER ALL USERS

(1.33) 14353 Status of auditing for 'DROP DATABASE LINK' privilege (Unified Auditing) Passed (oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:** AUDIT_OPTION_TYPE SUCCESS POLICY_NAME AUDIT_OPTION **FAILURE** ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P- DROP DATABASE STANDARD ACTION YES BY USER ALL USERS YES

(1.33) 14353 Status of auditing for 'DROP DATABASE LINK' privilege (Unified Auditing) (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

oracle19:1:1621:POHK1CAT.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_TYPE SUCCESS **FAILURE** ENABLED_OPTION ENTITY_NAME AUDIT_OPTION SCB_AUDIT_DDL_P- DROP DATABASE ALL USERS STANDARD ACTION YES YES BY USER OLICY LINK

(1.33) 14353 Status of auditing for 'DROP DATABASE LINK' privilege (Unified Auditing) (oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

Passed MEDIUM

MEDIUM

oracle19:1:1621:POHK4CCD.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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_	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_P- OLICY	DROP DATABASE LINK	STANDARD ACTION	YES	YES	BY USER	ALL USERS			

(1.33) 14353 Status of auditing for 'DROP DATABASE LINK' privilege (Unified Auditing) **Passed** (oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

Oracle database links are used to establish database-to-database connections to other databases. These connections are

Oracle_ATOS - 20240806 page 412

Passed

MEDIUM

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. matches regular expression list **Expected** *: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:

AUDIT OPTION TYPE SUCCESS ENABLED OPTION POLICY NAME AUDIT OPTION **FAILURE** ENTITY_NAME STANDARD ACTION YES SCB_AUDIT_DDL_P- DROP DATABASE BY USER ALL USERS YES LINK

(1.33) 14353 Status of auditing for 'DROP DATABASE LINK' privilege (Unified Auditing) (oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

oracle19:1:1621:POHK2CCD.hk.standardchartered.com

MEDIUM

Passed

Passed Previous Status

Instance

Evaluation Date 08/04/2024 at 10:38:34 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.

matches regular expression list Expected

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

OR, any of the selected values below:

Setting not found Table not found

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

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_P- DROP DATABASE STANDARD ACTION YES YES BY USER ALL USERS LINK

(1.34) 14354 Status of auditing for 'CREATE SYNONYM' privilege (Unified Auditing)(oracle19:1:1621: Passed **MEDIUM** POHK1API.hk.standardchartered.com)

oracle19:1:1621:POHK1API.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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							
	Tal	ole not found						
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)							
	SCB_A	AUDIT_DDL_POLICY:0	REATE SYNONYM:ST	ANDARD ACTION:YES	:YES:BY USER:ALL US	ERS		
Extended Ev	/idend	ce:						
POLICY_NAMI	IE AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME							
SCB_AUDIT_D: OLICY	DL_P-	CREATE SYNONYM	STANDARD ACTION	YES	YES	BY USER	ALL USERS	

(1.34) 14354 Status of auditing for 'CREATE SYNONYM' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	matc	matches regular expression list							
	.*:CREATE SYNONYM:.*:YES:YES:.*:*								
	OR, a	any of the selected	I values below:						
	Set	ting not found							
	Tal	ole not found							
Actual	Last	Undated:08/04/202	24 at 06:01:09 PM (GMT+0530)					
, 101001	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 Ex						-			
Exteriueu E	/iueii	.e.							
POLICY_NAMI	3	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_D OLICY	DL_P-	CREATE SYNONYM	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.34) 14354 Status of auditing for 'CREATE SYNONYM' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

colon separat	ed 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 F	vidence:

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

(1.34) 14354 Status of auditing for 'CREATE SYNONYM' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	matche	matches regular expression list								
	.*:CREAT	ΓΕ SYNONYM:.*:YES	S:YES:.*:.*							
	OR, an	OR, any of the selected values below:								
	Settir	ng not found								
	Table	e not found								
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)									
	SCB_AU	DIT_DDL_POLICY:C	REATE SYNONYM:ST.	ANDARD ACTION:YES	:YES:BY USER:ALL US	ERS				
Extended E	vidence	:								
POLICY_NAM	IE Al	UDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCB_AUDIT_I OLICY	DDL_P- Cl	REATE SYNONYM	STANDARD ACTION	YES	YES	BY USER	ALL USERS			

(1.34) 14354 Status of auditing for 'CREATE SYNONYM' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

colon separate	ed values	s of policy_name, au	dit_option, audit_option	on_type, success, failt	ire, enabled_option, a	ind entity_name.				
Expected	matches regular expression list									
	.*:CREA	ATE SYNONYM:.*:YES	S:YES:.*:.*							
	OR, any of the selected values below:									
	Setti	ing not found								
	Tabl	le not found								
Actual	Last U	Jpdated:08/04/202	24 at 06:01:09 PM ((GMT+0530)						
	SCB_AU	UDIT_DDL_POLICY:C	CREATE SYNONYM:ST	ANDARD ACTION:YES	S:YES:BY USER:ALL U	SERS				
Extended Ex	vidence	e:								
POLICY_NAM	E A	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCB AUDIT D	DL P- (CREATE SYNONYM	STANDARD ACTION	YES	YES	BY USER	ALL USERS			

(1.34) 14354 Status of auditing for 'CREATE SYNONYM' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

OLICY

Evaluation Date 08/04/2024 at 10:38:34 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.

matches regular expression list								
:CREATE SYNONYM:.*:YES	S:YES:.*:.*							
R, any of the selected	d values below:							
Setting not found								
Table not found								
ast Updated:08/04/202	24 at 06:01:09 PM ((GMT+0530)						
CB_AUDIT_DDL_POLICY:0	CREATE SYNONYM:ST	ANDARD ACTION:YES	S:YES:BY USER:ALL US	ERS				
dence:								
	ALIDIT ODTION TVDD	CHOODEC	DAILUDE	ENABLED ODTION	DAIDIDA ALAAM			
AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
_P- CREATE SYNONYM	STANDARD ACTION	YES	YES	BY USER	ALL USERS			
	CREATE SYNONYM:.*:YES OR, any of the selected Setting not found Table not found ast Updated:08/04/20: CB_AUDIT_DDL_POLICY: dence: AUDIT_OPTION	CREATE SYNONYM:.*:YES:YES:.*:* OR, any of the selected values below: Setting not found Table not found ast Updated:08/04/2024 at 06:01:09 PM (CB_AUDIT_DDL_POLICY:CREATE SYNONYM:ST dence: AUDIT_OPTION AUDIT_OPTION_TYPE	CREATE SYNONYM*:YES:YES:.*.* OR, any of the selected values below: Setting not found Table not found ast Updated:08/04/2024 at 06:01:09 PM (GMT+0530) CB_AUDIT_DDL_POLICY:CREATE SYNONYM:STANDARD ACTION:YES dence:	CREATE SYNONYM:.*:YES:YES:.*:* OR, any of the selected values below: Setting not found Table not found ast Updated:08/04/2024 at 06:01:09 PM (GMT+0530) CB_AUDIT_DDL_POLICY:CREATE SYNONYM:STANDARD ACTION:YES:YES:BY USER:ALL USIDE dence: AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE	CREATE SYNONYM:.*:YES:YES:.*:.* OR, any of the selected values below: Setting not found Table not found Cast Updated:08/04/2024 at 06:01:09 PM (GMT+0530) CB_AUDIT_DDL_POLICY:CREATE SYNONYM:STANDARD ACTION:YES:YES:BY USER:ALL USERS dence: AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION			

(1.34) 14354 Status of auditing for 'CREATE SYNONYM' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:** AUDIT_OPTION_TYPE SUCCESS ENABLED_OPTION ENTITY_NAME POLICY_NAME AUDIT_OPTION **FAILURE** SCB_AUDIT_DDL_P- CREATE SYNONYM STANDARD ACTION YES ALL USERS YES BY USER

(1.34) 14354 Status of auditing for 'CREATE SYNONYM' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	mato	hes regular expre	ssion list				
	.*:CRI	EATE SYNONYM:.*:YES	S:YES:.*:.*				
	OR,	any of the selected	d values below:				
	Se	tting not found					
		ble not found					
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM ((GMT+0530)			
	SCB_	AUDIT_DDL_POLICY:0	CREATE SYNONYM:ST	ANDARD ACTION:YES	:YES:BY USER:ALL US	ERS	
Extended E	Eviden	ce:					
POLICY_NAM	1E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_I OLICY	DDL_P-	CREATE SYNONYM	STANDARD ACTION	YES	YES	BY USER	ALL USERS
(1.35) 14355	5 State	us of auditing for '. K1API.hk.standard	ALTER SYNONYM' dchartered.com)	privilege (Unified	Auditing)(oracle19	9:1:1621: Passe	ed MEDIUM
Instance		oracle19:1:1621:POI	HK1API.hk.standardch	artered.com			
Previous Status	S	Passed					
Evaluation Dat	e	08/04/2024 at 10:3	8:34 PM (GMT+0530)				
java object o unsuccessfu	or eve ul, ma	n another synony y provide clues ar	ed to create an alt m, etc. Logging ar nd forensic eviden opriate to the need	nd monitoring of a ces about potenti	all attempts to alter al suspicious/unau	r synonyms, whet	ther successful or
The fellowing	Tiot Ct	ring value(s) of V indi	cates the status of the	ATTED CVNONVM or	dit option type define	d on the detabase Th	a autnut contains

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_P- ALTER SYNONYM STANDARD ACTION YES YES BY USER ALL USERS

(1.35) 14355 Status of auditing for 'ALTER SYNONYM' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

colon separat	ed 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 L	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)										
S	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	_P- ALTER SYNONYM	STANDARD ACTION	YES	YES	BY USER	ALL USERS					

(1.35) 14355 Status of auditing for 'ALTER SYNONYM' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:										
	Set	tting not found									
	Ta	ble not found									
Astual	Last	Um dete d.00/04/20	0.4 -+ 0.C.04.00 DM /	(CMT - 0520)							
Actual	Last	Updated:08/04/20	24 at 06:01:09 PM ((GIVI I +0530)							
	SCB_A	AUDIT_DDL_POLICY:AUDIT_DDL_POLICY:A	ALTER SYNONYM:STA	NDARD ACTION:YES	:YES:BY USER:ALL USE	RS					
Extended E	viden	ce:									
POLICY_NAM	ΙE	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME				
SCB_AUDIT_I	DL_P-	ALTER SYNONYM	STANDARD ACTION	YES	YES	BY USER	ALL USERS				

(1.35) 14355 Status of auditing for 'ALTER SYNONYM' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:** AUDIT_OPTION_TYPE SUCCESS POLICY_NAME AUDIT_OPTION **FAILURE** ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P- ALTER SYNONYM STANDARD ACTION YES BY USER ALL USERS YES

(1.35) 14355 Status of auditing for 'ALTER SYNONYM' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) Actual 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 ALL USERS SCB_AUDIT_DDL_P- ALTER SYNONYM STANDARD ACTION YES YES BY USER OLICY

(1.35) 14355 Status of auditing for 'ALTER SYNONYM' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_type, success, failure, enabled_option, and entity_name.

matches regular expression list									
`. *. * 									
alues below:									
at 06:01:09 PM (GMT+0530)									
ER SYNONYM:STANDARD ACTION:YES:YES:BY USER:ALL USERS									
7									

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

(1.35) 14355 Status of auditing for 'ALTER SYNONYM' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	ted matches regular expression list											
	.*:ALT	.*:ALTER SYNONYM:.*:YES:YES:.*:.*										
	OR, a	any of the selected	d values below:									
	Set	tting not found										
	Tal	ble not found										
				(OLIT OFOO)								
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM ((GMT+0530)								
	SCB_A	AUDIT_DDL_POLICY:/	ALTER SYNONYM:STA	NDARD ACTION:YES:	YES:BY USER:ALL USE	RS						
Extended E	vidend	ce:										
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME					
SCB_AUDIT_D	DL_P-	ALTER SYNONYM	STANDARD ACTION	YES	YES	BY USER	ALL USERS					

(1.35) 14355 Status of auditing for 'ALTER SYNONYM' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

colon separat	.eu vaiu	es or policy_name, au	dit_option, audit_option	on_type, success, ram	are, enabled_option, al	na entity_name.				
Expected	Expected matches regular expression list									
	.*:ALTER SYNONYM:.*:YES:YES:.*:.*									
	OR, any of the selected values below:									
	Set	ting not found								
	Tal	ble not found								
				(OLIT 0700)						
Actual	Last	Updated:08/04/20	24 at 06:01:09 PM ((GMT+0530)						
	SCB_A	AUDIT_DDL_POLICY:	ALTER SYNONYM:STA	NDARD ACTION:YES:	YES:BY USER:ALL USE	RS				
Extended E	Extended Evidence:									
POLICY_NAM	1E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCB_AUDIT_I OLICY	ODL_P-	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: Passed MEDIUM POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

colon separati	values of poney_name, dudit_option_type, success, familie, enabled_option, and entity_name.						
Expected	matches regular expression list						
	.*:DROP SYNONYM:.*:YES:YES:.*:.*						

	OR, a	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_A	AUDIT_DDL_POLICY:E	ROP SYNONYM:STAN	NDARD ACTION:YES:Y	ES:BY USER:ALL USEF	S S				
Extended Evidence:										
POLICY_NAM	Е	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCB_AUDIT_D OLICY	DL_P-	DROP SYNONYM	STANDARD ACTION	YES	YES	BY USER	ALL USERS			

(1.36) 14356 Status of auditing for 'DROP SYNONYM' privilege (Unified Auditing)(oracle19:1:1621: **MEDIUM Passed** POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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.

colori separated various of poney_name, addit_option_type, success, families_option, and entity_name.								
Expected	matc	hes regular expres	ssion list					
	.*:DROP SYNONYM:.*:YES:YES:.*:.*							
	OR, any of the selected values below:							
	Set	ting not found						
	Ta	ble not found						
Actual	L == (Llm d= (= d-00/04/0004 = (00.04-00 DM /OMT = 0000)							
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_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_D OLICY	DL_P-	DROP SYNONYM	STANDARD ACTION	YES	YES	BY USER	ALL USERS	

(1.36) 14356 Status of auditing for 'DROP SYNONYM' privilege (Unified Auditing)(oracle19:1:1621: **Passed MEDIUM** POHK1RCT.hk.standardchartered.com)

oracle19:1:1621:POHK1RCT.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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 separat	olon 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 E	vidence:									

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

(1.36) 14356 Status of auditing for 'DROP SYNONYM' privilege (Unified Auditing)(oracle19:1:1621: **Passed MEDIUM** POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	matc	hes regular expres	ssion list					
	.*:DRC	P SYNONYM:.*:YES:Y	ES:.*:.*					
	OR, any of the selected values below:							
	Setting not found							
	Tab	ole 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 Ev	Extended Evidence:							
POLICY_NAME		AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_DI OLICY	DL_P-	DROP SYNONYM	STANDARD ACTION	YES	YES	BY USER	ALL USERS	

(1.36) 14356 Status of auditing for 'DROP SYNONYM' privilege (Unified Auditing)(oracle19:1:1621: **Passed MEDIUM** POHK5CCD.hk.standardchartered.com)

oracle19:1:1621:POHK5CCD.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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 ontion type defined on the database. The output contains

colon separate	colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.							
Expected	matc	hes regular expre	ssion list					
	.*:DROP SYNONYM:.*:YES:YES:.*:.*							
	OR, any of the selected values below:							
	Set	ting not found						
	Tal	ole not found						
Actual		<u> </u>	24 at 06:01:09 PM (•				
	SCB_A	AUDIT_DDL_POLICY:I	DROP SYNONYM:STAN	NDARD ACTION:YES:Y	ES:BY USER:ALL USER	<u>S</u>		
Extended E	vidend	ce:						
POLICY_NAM	Е	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_D OLICY	DL_P-	DROP SYNONYM	STANDARD ACTION	YES	YES	BY USER	ALL USERS	

(1.36) 14356 Status of auditing for 'DROP SYNONYM' privilege (Unified Auditing)(oracle19:1:1621: **Passed MEDIUM** POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) Actual SCB AUDIT DDL POLICY:DROP SYNONYM:STANDARD ACTION:YES:YES:BY USER:ALL USERS **Extended Evidence:** ENTITY_NAME POLICY_NAME AUDIT OPTION AUDIT_OPTION_TYPE SUCCESS **FAILURE** ENABLED_OPTION SCB_AUDIT_DDL_P- DROP SYNONYM STANDARD ACTION YES YES BY USER ALL USERS

(1.36) 14356 Status of auditing for 'DROP SYNONYM' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

OLICY

Evaluation Date 08/04/2024 at 10:38:34 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:** AUDIT_OPTION_TYPE SUCCESS ENABLED_OPTION ENTITY_NAME POLICY_NAME AUDIT_OPTION **FAILURE** ALL USERS SCB_AUDIT_DDL_P- DROP SYNONYM STANDARD ACTION YES YES BY USER

(1.36) 14356 Status of auditing for 'DROP SYNONYM' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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										
	.*:DR0	OP SYNONYM:.*:YES	:YES:.*:.*								
	OR, any of the selected values below:										
		ting not found ble not found									
Actual	Last	Undated:08/04/20	024 at 06:01:09 PM ((GMT+0530)							
		•	:DROP SYNONYM:STAN		YES:YES:BY USER:ALL	. USERS					
Extended E											
POLICY_NAM		AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_O	PTION	ENTITY_NAME			
		DROP SYNONYM	STANDARD ACTION		YES	BY USER		ALL USERS			
.37) 1435	9 Statu	is of auditing for	'ALTER SYSTEM' prdchartered.com)	rivilege (Unifi	ed Auditing)(oracl	e19:1:1621:	Passe	d MEDIUI			
stance	- 011		T denartered.com) DHK1API.hk.standardch	artered.com							
evious Statu	IS	Passed	STITTI IIII.Staridarder	iar ter ea.com							
aluation Dat	te	08/04/2024 at 10:	:38:34 PM (GMT+0530))							
erformanc estem com atements, espicious/	e or no mands , wheth unauth	ormal operation of using undocume her successful or orized activities.	lows the user to choof the database. Acented Oracle function unsuccessful, may This logging requi	Iditionally, the nality. Logging y provide clue rement shoul	ALTER SYSTEM and monitoring of as and forensic events and set as appro-	I privilege may to all attempts to exidences about private to the needs	execute potential eds of	d to run opera ALTER SYST al the business.			
erformanc ystem com atements, uspicious/ The following separated va	e or no mands wheth unauth g List Sta lues of p	ormal operation of using undocume using undocume user successful or orized activities. Tring value(s) of X incolory_name, audit_colory_name.	of the database. Acented Oracle function unsuccessful, may This logging requidicates the status of the option, audit_option_type	Iditionally, the nality. Logging y provide clue rement shoul	ALTER SYSTEM and monitoring of as and forensic events d be set as appro	I privilege may to all attempts to exidences about private to the needs	execute potential eds of	d to run opera ALTER SYST al the business.			
erformanc ystem com atements, uspicious/ The following eparated va	e or no mands , wheth unauth g List Str lues of p matc	ormal operation of using undocume using undocume user successful or orized activities. It is a successful or orized activities. It is a successful or orized activities. It is a successful or orized activities.	of the database. Accepted Oracle function unsuccessful, may This logging requidicates the status of the option, audit_option_typession list	Iditionally, the nality. Logging y provide clue rement shoul	ALTER SYSTEM and monitoring of as and forensic events d be set as appro	I privilege may to all attempts to exidences about private to the needs	execute potential eds of	d to run opera ALTER SYST al the business.			
erformanc /stem com atements, uspicious/	e or no mands wheth unauth g List Str lues of p matc .*:ALT	ormal operation of using undocume her successful or orized activities. Tring value(s) of X incolicy_name, audit_colicy_name, audit_colicy_name.	of the database. Acented Oracle function unsuccessful, may This logging requidicates the status of the option, audit_option_typession list	Iditionally, the nality. Logging y provide clue rement shoul	ALTER SYSTEM and monitoring of as and forensic events d be set as appro	I privilege may to all attempts to exidences about private to the needs	execute potential eds of	d to run opera ALTER SYST al the business.			
erformanc ystem com atements, uspicious/ The following separated va	e or no mands , wheth unauth g List Str lues of p matc .*:ALT OR, a	ormal operation of using undocume using undocume user successful or orized activities. In the second of X into policy_name, audit_complete the second of the selection of the selection using the selection of the selec	of the database. Acented Oracle function unsuccessful, may This logging requidicates the status of the option, audit_option_typession list	Iditionally, the nality. Logging y provide clue rement shoul	ALTER SYSTEM and monitoring of as and forensic events d be set as appro	I privilege may to all attempts to exidences about private to the needs	execute potential eds of	d to run opera ALTER SYST al the business.			
erformanc ystem com atements, uspicious/ The following eparated va	e or no mands , wheth unauth g List Str lues of p matc .*:ALT OR, a	ormal operation of using undocume her successful or orized activities. Tring value(s) of X incolicy_name, audit_colicy_name, audit_colicy_name.	of the database. Acented Oracle function unsuccessful, may This logging requidicates the status of the option, audit_option_typession list	Iditionally, the nality. Logging y provide clue rement shoul	ALTER SYSTEM and monitoring of as and forensic events d be set as appro	I privilege may to all attempts to exidences about private to the needs	execute potential eds of	d to run opera ALTER SYST al the business.			
erformancestem com atements, uspicious/ The following eparated va Expected	e or no mands , wheth unauth g List Str lues of p matc .*:ALT OR, a	ormal operation of using undocume using undocume user successful or orized activities. It is value(s) of X incolory_name, audit_colory_name, audit_colory_name. The regular express regular	of the database. Acented Oracle function unsuccessful, may This logging requidicates the status of the option, audit_option_typession list	Iditionally, the nality. Logging y provide clue rement shoul ALTER SYSTEM pe, success, failur	ALTER SYSTEM and monitoring of as and forensic events d be set as appro	I privilege may to all attempts to exidences about private to the needs	execute potential eds of	d to run opera ALTER SYST al the business.			
erformance stem com atements, uspicious/ The following separated va	e or no mands , wheth unauth g List Str lues of p matc .*:ALT OR, a Set Ta	ormal operation of using undocume using undocume user successful or orized activities. Iring value(s) of X incolory_name, audit_colory_name, audit_colory_name, audit_colory_name is regular express SYSTEM:*:YES:Yeany of the selected ting not found ble not found Updated:08/04/20	of the database. Acented Oracle function unsuccessful, may This logging requidicates the status of the option, audit_option_typession list	Iditionally, the nality. Logging y provide clue rement shoul ALTER SYSTEM be, success, failure (GMT+0530)	ALTER SYSTEM and monitoring of es and forensic ev d be set as appro audit option type de re, enabled_option, ar	I privilege may be all attempts to exidences about privilege to the need fined on the databased entity_name.	execute potential eds of	d to run opera ALTER SYST al the business.			
erformance/stem come atements, uspicious/office following experted Expected Actual	e or no mands , wheth unauth g List Str lues of p matc .*:ALT OR, a See Ta	ormal operation of using undocume using undocume user successful or orized activities. Iring value(s) of X incolory_name, audit_colory_name, audi	of the database. Acented Oracle function unsuccessful, may This logging requidicates the status of the option, audit_option_typession list VES:.*:* ed values below: 024 at 06:01:09 PM (Iditionally, the nality. Logging y provide clue rement shoul ALTER SYSTEM be, success, failure (GMT+0530)	ALTER SYSTEM and monitoring of es and forensic ev d be set as appro audit option type de re, enabled_option, ar	I privilege may be all attempts to exidences about privilege to the need fined on the databased entity_name.	execute potential eds of	d to run opera ALTER SYST al the business.			
erformance/stem come attements, uspicious/office following separated value. Expected Actual	e or no mands , wheth unauth g List Str lues of p matc .*:ALT OR, a Set Ta Last SCB_A	ormal operation of using undocume using undocume user successful or orized activities. In the second of X incolory, name, audit, or the segular express SYSTEM:*:YES:Yeany of the selected ting not found ble not found Updated:08/04/20	of the database. Acented Oracle function unsuccessful, may This logging requidicates the status of the option, audit_option_typession list YES:.*:* ed values below: 024 at 06:01:09 PM (CALTER SYSTEM:SYSTEM)	Iditionally, the nality. Logging y provide clue rement shoul ALTER SYSTEM be, success, failure (GMT+0530) M PRIVILEGE:YI	ALTER SYSTEM and monitoring of es and forensic ev d be set as appro audit option type de re, enabled_option, ar	I privilege may be all attempts to exidences about privilege to the need fined on the databased entity_name.	pe use execute potentia eds of	d to run opera ALTER SYST al the business.			
erformance stem com atements, uspicious/ The following separated value at the separated value at the separated separ	e or no mands , wheth unauth g List Str lues of p matc .*:ALT OR, a Set Ta Last SCB_A	ormal operation of using undocume using undocume user successful or orized activities. Iring value(s) of X incolory_name, audit_colory_name, audi	of the database. Acented Oracle function unsuccessful, may This logging requidicates the status of the option, audit_option_typession list VES:.*:* ed values below: 024 at 06:01:09 PM (Iditionally, the nality. Logging y provide clue rement shoul ALTER SYSTEM pe, success, failure (GMT+0530) M PRIVILEGE:YI	ALTER SYSTEM and monitoring of es and forensic ev d be set as appro audit option type de re, enabled_option, ar	I privilege may be all attempts to exidences about privilege to the need fined on the databased entity_name.	pe use execute potentia eds of	d to run opera ALTER SYST al the business.			
erformancestem comeatements, aspicious/objective following reparated value for the following reparated value	e or no mands , wheth unauth g List Sti lues of p matc .*:ALT OR, a See Ta' Last SCB_A Evidence	ormal operation of using undocume using undocume using undocume user successful or orized activities. It is a value(s) of X incolicy_name, audit_composition and it_composition and it_composition are regular express that it is a value in the selected atting not found ble not found audit_oble not found audit_policy audit_policy audit_policy audit_option alter system	of the database. Accepted Oracle function unsuccessful, may This logging requidicates the status of the option, audit_option_typession list TES:.*:* ed values below: AUDIT_OPTION_TYPE SYSTEM PRIVILEGE	Iditionally, the nality. Logging y provide clue rement shoul ALTER SYSTEM be, success, failure (GMT+0530) M PRIVILEGE:YI	ALTER SYSTEM and monitoring of es and forensic ev d be set as appro audit option type de re, enabled_option, ar ES:YES:BY USER:ALL U FAILURE YES	I privilege may be all attempts to exidences about priate to the need fined on the databased entity_name. USERS ENABLED_OUR BY USER	pe use execute potentia eds of	d to run opera ALTER SYST al the business. butput contains c			
erformance stem come atements, uspicious/ Che following eparated value at the following eparated eparated eparated eparated eparated eparated eparated	e or no mands , wheth unauth g List Str lues of p matc .*:ALT OR, a See Tai Last SCB_A Evidence ME DDL_P-	ormal operation of using undocume using undocume using undocume user successful or orized activities. In successful or or	of the database. Accented Oracle function unsuccessful, may This logging requidicates the status of the option, audit_option_typession list TES:.*:.* ed values below: AUDIT_OPTION_TYPESYSTEM PRIVILEGE 'ALTER SYSTEM' p	Iditionally, the nality. Logging y provide clue rement shoul ALTER SYSTEM be, success, failure (GMT+0530) M PRIVILEGE:YI	ALTER SYSTEM and monitoring of es and forensic ev d be set as appro audit option type de re, enabled_option, ar ES:YES:BY USER:ALL U FAILURE YES	I privilege may be all attempts to exidences about priate to the need fined on the databased entity_name. USERS ENABLED_OUR BY USER	pe use execute potentia eds of	d to run opera ALTER SYST al the business. output contains of			
erformance stem compatements, uspicious/compatements,	e or no mands , wheth unauth g List Str lues of p matc .*:ALT OR, a See Tai Last SCB_A Evidence ME DDL_P-	ormal operation of using undocume using undocume are successful or orized activities. Iring value(s) of X incolicy_name, audit_or hes regular express SYSTEM:*:YES:Yeary of the selected ting not found ble not found Updated:08/04/20 AUDIT_DDL_POLICY CE: AUDIT_OPTION ALTER SYSTEM Us of auditing for K3CCD.hk.standa	of the database. Acented Oracle function unsuccessful, may This logging requidicates the status of the option, audit_option_typession list TES:.*:* ed values below: AUDIT_OPTION_TYPESYSTEM PRIVILEGE 'ALTER SYSTEM' pardchartered.com)	Iditionally, the nality. Logging y provide clue rement shoul ALTER SYSTEM be, success, failure (GMT+0530) M PRIVILEGE:YILLege:YILlege:YILlege:YILlege:YILlege:YILlege:YILlege:YILlege:YILlege:YILlege:YILlege:YILlege:YILlege:YILlege:YILlege:YILlege:YIllege:	ALTER SYSTEM and monitoring of es and forensic ev d be set as appro audit option type de re, enabled_option, ar ES:YES:BY USER:ALL U FAILURE YES	I privilege may be all attempts to exidences about priate to the need fined on the databased entity_name. USERS ENABLED_OUR BY USER	per use execute potential eds of see. The co	d to run opera ALTER SYST al the business. output contains c ENTITY_NAME ALL USERS			
erformance stem come at the come at the come at the come at the construction of the following eparated value of the come at the construction of the come at the come at the construction of the come at th	e or no mands , wheth unauth g List Str lues of p matc .*:ALT OR, a Set Ta Last SCB_A Evidence ME DDL_P-	ormal operation of using undocume using undocume are successful or orized activities. Iring value(s) of X incolicy_name, audit_or hes regular express SYSTEM:*:YES:Yeary of the selected ting not found ble not found Updated:08/04/20 AUDIT_DDL_POLICY CE: AUDIT_OPTION ALTER SYSTEM Us of auditing for K3CCD.hk.standa	of the database. Accented Oracle function unsuccessful, may This logging requidicates the status of the option, audit_option_typession list TES:.*:.* ed values below: AUDIT_OPTION_TYPESYSTEM PRIVILEGE 'ALTER SYSTEM' p	Iditionally, the nality. Logging y provide clue rement shoul ALTER SYSTEM be, success, failure (GMT+0530) M PRIVILEGE:YILLege:YILlege:YILlege:YILlege:YILlege:YILlege:YILlege:YILlege:YILlege:YILlege:YILlege:YILlege:YILlege:YILlege:YILlege:YILlege:YIllege:	ALTER SYSTEM and monitoring of es and forensic ev d be set as appro audit option type de re, enabled_option, ar ES:YES:BY USER:ALL U FAILURE YES	I privilege may be all attempts to exidences about priate to the need fined on the databased entity_name. USERS ENABLED_OUR BY USER	per use execute potential eds of see. The co	d to run opera ALTER SYST al the business. output contains c ENTITY_NAME ALL USERS			

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

(1.37) 14359 Status of auditing for 'ALTER SYSTEM' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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- ALTER SYSTEM SYSTEM PRIVILEGE YES YES BY USER ALL USERS

(1.37) 14359 Status of auditing for 'ALTER SYSTEM' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_type, success, failure, enabled_option, and entity_name.

separateu vait	ies of policy_name, addit_op	dion, addit_option_type, success, faild	ire, enabled_option, and	rentity_name.					
Expected	matches regular expre	ssion list							
	.*:ALTER SYSTEM:.*:YES:YES:.*:.*								
	OR, any of the selected values below:								
	Setting not found								
	Table not found								
Actual	Last Updated:08/04/20	24 at 06:01:09 PM (GMT+0530)							
	SCB_AUDIT_DDL_POLICY:	ALTER SYSTEM:SYSTEM PRIVILEGE:Y	ES:YES:BY USER:ALL US	SERS					
Extended E	Extended Evidence:								
POLICY_NAM	E AUDIT_OPTION	AUDIT_OPTION_TYPE SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME				

SCB_AUDIT_DDL_P- ALTER SYSTEM	SYSTEM PRIVILEGE	YES	YES	BY USER	ALL USERS
OLICY					

(1.37) 14359 Status of auditing for 'ALTER SYSTEM' privilege (Unified Auditing)(oracle19:1:1621: **Passed MEDIUM** POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) Actual

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 SYSTEM PRIVILEGE YES SCB_AUDIT_DDL_P- ALTER SYSTEM YES BY USER ALL USERS

(1.37) 14359 Status of auditing for 'ALTER SYSTEM' privilege (Unified Auditing)(oracle19:1:1621: **Passed MEDIUM** POHK1CAT.hk.standardchartered.com)

oracle19:1:1621:POHK1CAT.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_type, success, failure, enabled_option, and entity_name.									
Expected	matches regular expression list								
	.*:ALTER SYSTEM:.*:YES:YES:.*·.*								
	OR, any	OR, any of the selected values below:							
	Setting not found								
	Table n	ot found							
Actual	Last Upd	lated:08/04/20	24 at 06:01:09 PM ((GMT+0530)					
	SCB_AUDI	T_DDL_POLICY:	ALTER SYSTEM:STANI	OARD ACTION:YES:YE	S:BY USER:ALL USERS				
	SCB_AUDI	SCB_AUDIT_DDL_POLICY:ALTER SYSTEM:SYSTEM PRIVILEGE:YES:YES:BY USER:ALL USERS							
Extended Ex	vidence:								
POLICY_NAMI	E AUE	DIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_D OLICY	DL_P- ALT	ER SYSTEM	SYSTEM PRIVILEGE	YES	YES	BY USER	ALL USERS		
SCB_AUDIT_D	DL_P- ALT	ER SYSTEM	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.37) 14359 Status of auditing for 'ALTER SYSTEM' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) Actual 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- ALTER SYSTEM SYSTEM PRIVILEGE YES YES BY USER ALL USERS

(1.37) 14359 Status of auditing for 'ALTER SYSTEM' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 type success failure enabled option and entity name.

separated values of policy_name, addit_option_type, success, failure, enabled_option, and entity_name.								
Expected	matches regular expression list							
	.*:ALT	LTER SYSTEM:.*:YES:YES:.*:.*						
OR, any of the selected values below:								
	Set	ting not found						
	Tal	ole not found						
				(0117 0500)				
Actual	Last	t 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_NAM	Е	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_D OLICY	DL_P-	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: Passed MEDIUM POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 STANDARD ACTION YES SCB_AUDIT_DDL_P- CREATE TRIGGER YES BY USER ALL USERS

(1.38) 14360 Status of auditing for 'CREATE TRIGGER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

matches regular expression list **Expected** *: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:** AUDIT_OPTION_TYPE SUCCESS **FAILURE** ENABLED_OPTION ENTITY_NAME POLICY NAME AUDIT_OPTION SCB_AUDIT_DDL_P- CREATE TRIGGER STANDARD ACTION YES YES BY USER ALL USERS

(1.38) 14360 Status of auditing for 'CREATE TRIGGER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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- CREATE TRIGGER OLICY STANDARD ACTION YES YES BY USER ALL USERS (1.38) 14360 Status of auditing for 'CREATE TRIGGER' privilege (Unified Auditing)(oracle19:1:1621: **Passed MEDIUM** POHK4CCD.hk.standardchartered.com) oracle19:1:1621:POHK4CCD.hk.standardchartered.com Instance Previous Status 08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date** 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 Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) Actual SCB_AUDIT_DDL_POLICY:CREATE TRIGGER:STANDARD ACTION:YES:YES:BY USER:ALL USERS **Extended Evidence:** AUDIT_OPTION_TYPE SUCCESS **FAILURE** ENTITY_NAME POLICY_NAME AUDIT_OPTION ENABLED_OPTION SCB_AUDIT_DDL_P- CREATE TRIGGER OLICY STANDARD ACTION YES YES BY USER ALL USERS (1.38) 14360 Status of auditing for 'CREATE TRIGGER' privilege (Unified Auditing)(oracle19:1:1621: **MEDIUM** POHK5CCD.hk.standardchartered.com) oracle19:1:1621:POHK5CCD.hk.standardchartered.com Instance Previous Status **Evaluation Date** 08/04/2024 at 10:38:34 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								
	Tal	ole not found							
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)								
	SCB_A	.UDIT_DDL_POLICY:0	CREATE TRIGGER:STA	NDARD ACTION:YES:Y	ES:BY USER:ALL USEI	RS			
Extended Ev	videnc	e:							
POLICY_NAMI	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_DI OLICY	DL_P-	CREATE TRIGGER	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.38) 14360 Status of auditing for 'CREATE TRIGGER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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, a	OR, any of the selected values below:							
	Set	ting not found							
	Tal	ble not found							
Actual	Local Limitation (100/04/2024 at 00:04:00 DM (CMT: 0520)								
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 E	viden	· • ·							
LAteriaca L	videiid	· · · · · · · · · · · · · · · · · · ·							
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_D OLICY	DL_P-	CREATE TRIGGER	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.38) 14360 Status of auditing for 'CREATE TRIGGER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

colon separated values of policy_name, addit_option, addit_option_type, success, familie, 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			

(1.38) 14360 Status of auditing for 'CREATE TRIGGER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	matc	hes regular expre	ssion list						
	.*:CRE	EATE TRIGGER:.*:YES:	YES:.*:.*						
	OR, a	any of the selected	d values below:						
	Set	Setting not found							
	Table not found								
Actual	Loot	Undeted-09/04/201	04 at 06:04:00 DM	CMT - 0520\					
Actual	Last	Opdated:06/04/20/	24 at 06:01:09 PM ((GIVI I +0530)					
	SCB_A	AUDIT_DDL_POLICY:(CREATE TRIGGER:STAI	NDARD ACTION:YES:Y	ES:BY USER:ALL USE	RS			
Extended E	viden	ce:							
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_D	DL_P-	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: Passed MEDIUM POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

separated values of policy_name, addit_option, addit_option_type, success, failure, enabled_option, and enacy_name.								
Expected	matc	hes regular expres	ssion list					
	.*:ALTER TRIGGER:.*:YES:YES:.*:.*							
	OR, any of the selected values below:							
	Setting not found							
	Table not found							
Actual	Loot		04 at 06:04:00 DM (CMT - 0520\				
Actual	Last	Updated:08/04/202	24 at 06:01:09 PW (GIVI I +0530)				
	SCB_A	AUDIT_DDL_POLICY:A	LTER TRIGGER:STAN	DARD ACTION:YES:YE	S:BY USER:ALL USER:	S		
Extended E	Extended Evidence:							
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_D OLICY	DL_P-	ALTER TRIGGER	STANDARD ACTION	YES	YES	BY USER	ALL USERS	

(1.39) 14361 Status of auditing for 'ALTER TRIGGER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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. matches regular expression list *:ALTER TRIGGER:.*:YES:YES:.*:.* OR, any of the selected values below: Setting not found Table not found Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) Actual 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- ALTER TRIGGER STANDARD ACTION YES YES BY USER ALL USERS

(1.39) 14361 Status of auditing for 'ALTER TRIGGER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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, type success, failure, enabled, option, and entity, name.

separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.								
Expected	matc	hes regular expre	ssion list					
	.*:ALTER TRIGGER:.*:YES:YES:.*:.*							
	OR, any of the selected values below:							
	Setting not found							
	Table not found							
Actual	Last	Updated:08/04/20	24 at 06:01:09 PM ((GMT+0530)				
	SCB_A	AUDIT_DDL_POLICY:	ALTER TRIGGER:STAN	DARD ACTION:Y	ES:YES:BY USER:ALL U	SERS		
Extended E	viden	ce:						
POLICY_NAM	ΙE	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_D OLICY	DL_P-	ALTER TRIGGER	STANDARD ACTION	YES	YES	BY USER	ALL USERS	

(1.39) 14361 Status of auditing for 'ALTER TRIGGER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(1.39) 14361 Status of auditing for 'ALTER TRIGGER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK5CCD.hk.standardchartered.com)

YES

BY USER

ALL USERS

STANDARD ACTION YES

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

SCB_AUDIT_DDL_P- ALTER TRIGGER

Evaluation Date 08/04/2024 at 10:38:34 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.

matches regular expression list **Expected** *: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:** AUDIT_OPTION_TYPE SUCCESS **FAILURE** ENABLED_OPTION POLICY NAME AUDIT_OPTION ENTITY_NAME SCB_AUDIT_DDL_P- ALTER TRIGGER STANDARD ACTION YES YES BY USER ALL USERS

(1.39) 14361 Status of auditing for 'ALTER TRIGGER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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- ALTER TRIGGER OLICY STANDARD ACTION YES YES BY USER ALL USERS (1.39) 14361 Status of auditing for 'ALTER TRIGGER' privilege (Unified Auditing)(oracle19:1:1621: **MEDIUM** Passed POHK1CCD.hk.standardchartered.com) oracle19:1:1621:POHK1CCD.hk.standardchartered.com Instance Previous Status 08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date** 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 Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) Actual SCB_AUDIT_DDL_POLICY:ALTER TRIGGER:STANDARD ACTION:YES:YES:BY USER:ALL USERS **Extended Evidence:** AUDIT_OPTION_TYPE SUCCESS **FAILURE** ENTITY_NAME POLICY_NAME AUDIT_OPTION ENABLED_OPTION SCB_AUDIT_DDL_P- ALTER TRIGGER OLICY STANDARD ACTION YES YES BY USER ALL USERS (1.39) 14361 Status of auditing for 'ALTER TRIGGER' privilege (Unified Auditing)(oracle19:1:1621: **Passed MEDIUM** POHK2CCD.hk.standardchartered.com) oracle19:1:1621:POHK2CCD.hk.standardchartered.com Instance Previous Status **Evaluation Date** 08/04/2024 at 10:38:34 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:

	Tab	ole not found						
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)							
	SCB_A	.UDIT_DDL_POLICY:A	ALTER TRIGGER:STANI	DARD ACTION:YES:YE	S:BY USER:ALL USERS	5		
Extended Ev	idenc	e:						
POLICY_NAME	2	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_DI	DL_P-	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: Passed MEDIUM POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	matc	hes regular expres	ssion list						
	.*:DRC	OP TRIGGER:.*:YES:YES	5:.*:.*						
	OR, any of the selected values below:								
	Setting not found								
	Table not found								
Actual	Last	Updated:08/04/202	24 at 06:01:00 PM ((CMT+0530)					
Actual		•		OARD ACTION:YES:YES	SAZOLI IIV-AZOLI VA:S				
	JCD_F	NODII_DDL_I OLICI.L	MOI INIGGEN.SIANE	AND ACTION, TES. TEC	D.DT USEK.ALL USEKS				
Extended E	vidend	e:							
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_D OLICY	DL_P-	DROP TRIGGER	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.40) 14362 Status of auditing for 'DROP TRIGGER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

separateu vai	des of policy_name, addic_option, addic_option_type, success, famure, 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		

(1.40) 14362 Status of auditing for 'DROP TRIGGER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	matc	matches regular expression list									
	.*:DRC	OP TRIGGER:.*:YES:YE	S:.*:.*								
	OR, any of the selected values below:										
	Setting not found										
	Table not found										
Actual	Loot	Undeted-09/04/201	04 of 06:04:00 DM /	CMT - 0520\							
Actual	Last	Updated:08/04/202	24 at 06:01:09 PW (GIVI I +0530)							
	SCB_A	AUDIT_DDL_POLICY:I	ROP TRIGGER:STAND	ARD ACTION:YES:YES	S:BY USER:ALL USERS						
Extended Ex	Extended Evidence:										
POLICY_NAM	Е	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME				
SCB_AUDIT_D	DL_P-	DROP TRIGGER	STANDARD ACTION	YES	YES	BY USER	ALL USERS				

(1.40) 14362 Status of auditing for 'DROP TRIGGER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

separated value	separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.							
Expected	matc	hes regular expres	ssion list					
	.*:DRC	OP TRIGGER:.*:YES:YE	S:.*:.*					
	OR, a	any of the selected	d values below:					
	Setting not found							
	☐ Table not found							
Actual	Last	Undated:08/04/203	24 at 06:01:09 PM (GMT+0530)				
Actual		•	DROP TRIGGER:STAND	•	S-RY HSFR-ALL HSFRS			
			THOUSEN.STAINE	THE THOTY. TEO. TEC	J.D.T. COLIC. ALL COLICO			
Extended E	vidend	ce:						
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_D OLICY	DL_P-	DROP TRIGGER	STANDARD ACTION	YES	YES	BY USER	ALL USERS	

(1.40) 14362 Status of auditing for 'DROP TRIGGER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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. matches regular expression list *:DROP TRIGGER:.*:YES:YES:.*:.* OR, any of the selected values below: Setting not found Table not found Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) Actual 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- DROP TRIGGER STANDARD ACTION YES YES BY USER ALL USERS

(1.40) 14362 Status of auditing for 'DROP TRIGGER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) Actual 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- DROP TRIGGER STANDARD ACTION YES ALL USERS YES BY USER

(1.40) 14362 Status of auditing for 'DROP TRIGGER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 STANDARD ACTION YES SCB_AUDIT_DDL_P- DROP TRIGGER YES BY USER ALL USERS

(1.40) 14362 Status of auditing for 'DROP TRIGGER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

matches regular expression list **Expected** *: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:** AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME POLICY_NAME AUDIT_OPTION SCB_AUDIT_DDL_P- 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.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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. matches regular expression list **Expected** .*: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_TYPE SUCCESS AUDIT_OPTION **FAILURE** ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P- | CREATE PROCEDURE | STANDARD ACTION | YES YES BY USER ALL USERS OLICY (1.41) 14364 Status of auditing for 'CREATE PROCEDURE' statement (Unified Auditing) **MEDIUM** Passed (oracle19:1:1621:POHK3CCD.hk.standardchartered.com) oracle19:1:1621:POHK3CCD.hk.standardchartered.com Instance Previous Status 08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date** 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 Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) Actual SCB_AUDIT_DDL_POLICY:CREATE PROCEDURE:STANDARD ACTION:YES:YES:BY USER:ALL USERS **Extended Evidence:** AUDIT_OPTION_TYPE SUCCESS **FAILURE** POLICY_NAME AUDIT_OPTION ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P-OLICY CREATE STANDARD ACTION YES YES BY USER ALL USERS **PROCEDURE** (1.41) 14364 Status of auditing for 'CREATE PROCEDURE' statement (Unified Auditing) **Passed MEDIUM** (oracle19:1:1621:POHK1RCT.hk.standardchartered.com) oracle19:1:1621:POHK1RCT.hk.standardchartered.com Instance Previous Status **Evaluation Date** 08/04/2024 at 10:38:34 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. matches regular expression list **Expected** *:CREATE PROCEDURE:.*:YES:YES:.*:.* OR, any of the selected values below:

		tting not found ble not found					
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM ((GMT+0530)			
	SCB_A	AUDIT_DDL_POLICY:0	CREATE PROCEDURE:S	STANDARD ACTION:Y	ES:YES:BY USER:ALL U	JSERS	
Extended E	viden	ce:					
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_D OLICY	DL_P-	CREATE PROCEDURE	STANDARD ACTION	YES	YES	BY USER	ALL USERS
02101		THOUSE CINE					

(1.41) 14364 Status of auditing for 'CREATE PROCEDURE' statement (Unified Auditing) (oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_type, success, failure, enabled_option, and entity_name.

Expected r	natches regular expres	ssion list						
<u>.</u> :	*:CREATE PROCEDURE:.*:Y	ES:YES:.*:.*						
OR, any of the selected values below:								
	Setting not found							
	☐ Table not found							
Actual L	_ast Updated:08/04/202	24 at 06:01:09 PM ((GMT+0530)					
S	CB_AUDIT_DDL_POLICY:CREATE PROCEDURE:STANDARD ACTION:YES:YES:BY USER:ALL USERS							
Extended Evi	Extended Evidence:							
POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_DD	L_P- CREATE PROCEDURE	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.41) 14364 Status of auditing for 'CREATE PROCEDURE' statement (Unified Auditing) Passed MEDIUM (oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_type, success, failure, enabled_option, and entity_name.

•	• "	-		•		.,	
Expected	matches regular express	ion list					
	.*:CREATE PROCEDURE:.*:YES	:YES:.*:.*					
	OR, any of the selected v	alues below	v:				
	Setting not found						
	Table not found						
Actual	Last Updated:08/04/2024	at 06:01:09	PM (GMT+0530)				
	SCB_AUDIT_DDL_POLICY:CR	EATE PROCED	URE:STANDARD ACTIO	ON:YES:YES:BY USE	R: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		

(1.41) 14364 Status of auditing for 'CREATE PROCEDURE' statement (Unified Auditing) (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Passed **MEDIUM**

oracle19:1:1621:POHK1CAT.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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_type, success, failure, enabled_option, and entity_name.

Expected	matc	hes regular expres	ssion list					
	.*:CRE	ATE PROCEDURE:.*:Y	ES:YES:.*:.*					
	OR, a	any of the selected	d values below:					
Setting not found								
	Table not found							
Actual	Last Undated-09/04/2024 at 06:01:00 PM (GMT: 0520)							
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 Ev	videnc	ce:						
POLICY_NAMI	3	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_D	DL_P-	CREATE	STANDARD ACTION	YES	YES	BY USER	ALL USERS	

(1.41) 14364 Status of auditing for 'CREATE PROCEDURE' statement (Unified Auditing) (oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Passed **MEDIUM**

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 separate	ed valu	es of policy_name, au	dit_option, audit_opti	on_type, success, failu	ıre, enabled_option, ar	nd entity_name.	•
Expected	matc	hes regular expres	ssion list				
	.*:CRE	ATE PROCEDURE:.*:Y	ES:YES:.*:.*				
	OR, a	any of the selected	d values below:				
	Setting not found						
	Table not found						
Actual	Lact	IIndated:08/04/201	24 at 06:01:09 PM (CMT+0530)			
Actual		-		•	ES:YES:BY USER:ALL U	ICEDC	
			KEATE I KOCEDUKE.	TANDARD ACTION.T	ES.TES.DT USER.ALL (JOEKO	
Extended E	viden	ce:					
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_D OLICY	DL_P-	CREATE PROCEDURE	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.41) 14364 Status of auditing for 'CREATE PROCEDURE' statement (Unified Auditing) (oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

Instance oracle 19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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. matches regular expression list *:CREATE PROCEDURE:.*:YES:YES:.*:.* OR, any of the selected values below: Setting not found Table not found Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) Actual 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 BY USER SCB_AUDIT_DDL_P- CREATE STANDARD ACTION YES YES ALL USERS **PROCEDURE**

(1.42) 14365 Status of auditing for 'CREATE FUNCTION' statement (Unified Auditing) (oracle19:1:1621:POHK1API.hk.standardchartered.com)

Passed MEDIUM

Passed

MEDIUM

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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, type success failure enabled option, and entity, name

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 **FAILURE** AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P- CREATE FUNCTION STANDARD ACTION YES OLICY YES BY USER ALL USERS

(1.42) 14365 Status of auditing for 'CREATE FUNCTION' statement (Unified Auditing) (oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_P- CREATE FUNCTION STANDARD ACTION YES YES BY USER ALL USERS

(1.42) 14365 Status of auditing for 'CREATE FUNCTION' statement (Unified Auditing) (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 10:38:34 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.

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

(1.42) 14365 Status of auditing for 'CREATE FUNCTION' statement (Unified Auditing) (oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

	.*:CRE	ATE FUNCTION:.*:YES	S:YES:.*:.*				
	OR, a	any of the selected	l values below:				
	Set	ting not found					
	Table not found						
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)						
	SCB_A	AUDIT_DDL_POLICY:C	REATE FUNCTION:ST	ANDARD ACTION:YES	S:YES:BY USER:ALL US	SERS	
Extended Ev	videnc	e:					
POLICY_NAME	3	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DI OLICY	DL_P-	CREATE FUNCTION	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.42) 14365 Status of auditing for 'CREATE FUNCTION' statement (Unified Auditing) (oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Passed MEDIUM

oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Instance

Evaluation Date 08/04/2024 at 10:38:34 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	matc	hes regular expre	ssion list					
	.*:CRE	ATE FUNCTION:.*:YES	S:YES:.*:.*					
	OR, a	any of the selected	d values below:					
Setting not found Table not found								
Actual	Local Lindoted (09/04/2024 of 06:04:00 DM (CMT: 0520)							
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 E	Extended Evidence:							
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_D	DL_P-	CREATE FUNCTION	STANDARD ACTION	YES	YES	BY USER	ALL USERS	

(1.42) 14365 Status of auditing for 'CREATE FUNCTION' statement (Unified Auditing) Passed (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_P- OLICY	CREATE FUNCTION	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.42) 14365 Status of auditing for 'CREATE FUNCTION' statement (Unified Auditing) (oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_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_TYP	E SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_P- CREATE FUNCT: OLICY	ON STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.42) 14365 Status of auditing for 'CREATE FUNCTION' statement (Unified Auditing) (oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_P- OLICY	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.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) Actual 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_P- CREATE PACKAGE OLICY STANDARD ACTION YES YES BY USER ALL USERS

(1.43) 14366 Status of auditing for 'CREATE PACKAGE' statement (Unified Auditing) (oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

Passed MEDIUM

Instance oracle 19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

matches regular expression list **Expected** *: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:** AUDIT OPTION TYPE SUCCESS **FAILURE** ENABLED OPTION ENTITY NAME POLICY NAME AUDIT OPTION SCB_AUDIT_DDL_P- CREATE PACKAGE OLICY STANDARD ACTION YES YES BY USER ALL USERS

(1.43) 14366 Status of auditing for 'CREATE PACKAGE' statement (Unified Auditing) (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 10:38:34 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.

	matches regular expression list .*:CREATE PACKAGE:.*:YES:YES::*:* OR any of the selected values below:								
	OR, any of the selected values below:								
	Setting not found Table not found								
Actual	Last Updated:08/04/2	024 at 06:01:09 PM ((GMT+0530)						
	SCB_AUDIT_DDL_POLIC	Y:CREATE PACKAGE:STA	NDARD ACTION:	YES:YES:BY USER:ALL	USERS				
Extended Ev	vidence:								
POLICY_NAME	E AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCB_AUDIT_DI OLICY	DL_P- CREATE PACKAGE	STANDARD ACTION	YES	YES	BY USER	ALL USERS			
(1.43) 14366	Status of auditing for	'CREATE PACKAGI	E' statement (l	Jnified Auditing)	Passe	ed MEDIUM			
·	(oracle19:1:1621:PO			n)					
nstance Previous Status	oracie19:1:1621:P Passed	OHK4CCD.hk.standardcl	nartered.com						
Evaluation Date		:38:34 PM (GMT+0530))						
	ase packages, which								
	defined by PL/SQL o								
	create package, whet nauthorized activities								
The following colon separate	List String value(s) of X in ed values of policy_name,	dicates the status of the audit_option, audit_option	CREATE PACKA on_type, success,	GE audit option type de failure, enabled_option	fined on the database. The n, and entity_name.	e output contains			
Expected	matches regular exp	ression list							
	.*:CREATE PACKAGE:.*:YI								
	OR, any of the select	ed values below:							
	Setting not found Table not found								
	Last Updated:08/04/2	024 at 06:01:09 PM ((GMT+0530)						
Actual		V-CREATE PACKAGE-STA	NDARD ACTION:	YES:YES:BY USER:ALL	USERS				
Actual	SCB_AUDIT_DDL_POLIC	I.CKLATE I ACIGIOL.51A							
Extended Ex		I.CKLAIL I ACKAGE.SIA							
	vidence:	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
Extended Ex	vidence:			FAILURE YES	ENABLED_OPTION BY USER	ENTITY_NAME ALL USERS			
Extended ExPOLICY_NAMI	vidence: E AUDIT_OPTION DL_P- CREATE PACKAGE	AUDIT_OPTION_TYPE STANDARD ACTION	YES	YES	BY USER	ALL USERS			
Extended ExPOLICY_NAMI	vidence: E AUDIT_OPTION DL_P- CREATE PACKAGE Status of auditing for	AUDIT_OPTION_TYPE STANDARD ACTION 'CREATE PACKAGI	YES E' statement (I	YES Unified Auditing)		ALL USERS			
Extended Expolicy_NAMI SCB_AUDIT_DIOLICY (1.43) 14366	vidence: E AUDIT_OPTION DL_P- CREATE PACKAGE Status of auditing for (oracle19:1:1621:POI	AUDIT_OPTION_TYPE STANDARD ACTION 'CREATE PACKAGI	YES E' statement (ldchartered.com	YES Unified Auditing)	BY USER	ALL USERS			
Extended ExpOLICY_NAMI SCB_AUDIT_DI OLICY (1.43) 14366	vidence: E AUDIT_OPTION DL_P- CREATE PACKAGE Status of auditing for (oracle19:1:1621:POI	AUDIT_OPTION_TYPE STANDARD ACTION - 'CREATE PACKAGE HK5CCD.hk.standard	YES E' statement (ldchartered.com	YES Unified Auditing)	BY USER	ALL USERS			
Extended ExPOLICY_NAMI	vidence: E AUDIT_OPTION DL_P- CREATE PACKAGE Status of auditing for (oracle19:1:1621:PO) oracle19:1:1621:POPUS	AUDIT_OPTION_TYPE STANDARD ACTION - 'CREATE PACKAGE HK5CCD.hk.standard	YES E' statement (Idchartered.com	YES Unified Auditing)	BY USER	ALL USERS			
POLICY_NAMI SCB_AUDIT_DI OLICY (1.43) 14366 Instance Previous Status Evaluation Date Oracle datab	widence: E AUDIT_OPTION DL_P- CREATE PACKAGE Status of auditing for (oracle19:1:1621:PO) oracle19:1:1621:P Passed 08/04/2024 at 10 pase packages, which	AUDIT_OPTION_TYPE STANDARD ACTION T'CREATE PACKAGI HK5CCD.hk.standard OHK5CCD.hk.standardcl 2:38:34 PM (GMT+0530) The are stored within the	YES E' statement (Idchartered.com hartered.com	YES Unified Auditing) n) are created to perference are created to perference are created.	Passe	all users ed MEDIUM ons and access			
POLICY_NAMI SCB_AUDIT_DIOLICY (1.43) 14366 Instance Previous Status Evaluation Date Oracle datab database as	widence: E AUDIT_OPTION DL_P- CREATE PACKAGE Status of auditing for (oracle19:1:1621:PO) oracle19:1:1621:PO Passed 08/04/2024 at 10 pase packages, which defined by PL/SQL or	AUDIT_OPTION_TYPE STANDARD ACTION T'CREATE PACKAGI HK5CCD.hk.standardcl 1:38:34 PM (GMT+0530) The are stored within the ode and SQL states	YES E' statement (Idchartered.com hartered.com he database, ments contain	YES Unified Auditing) n) are created to perfeed within these ob	Passe porm business function jects. Logging and m	all users ed MEDIUM ons and access nonitoring of all			
POLICY_NAMI SCB_AUDIT_DIOLICY (1.43) 14366 Instance Previous Status Evaluation Date Oracle datab database as attempts to contact the state of the	widence: E AUDIT_OPTION DL_P- CREATE PACKAGE Status of auditing for (oracle19:1:1621:PO) oracle19:1:1621:P Passed 08/04/2024 at 10 pase packages, which	AUDIT_OPTION_TYPE STANDARD ACTION T'CREATE PACKAGI HK5CCD.hk.standard COHK5CCD.hk.standardcl 1:38:34 PM (GMT+0530) In are stored within the ode and SQL states ther successful or ur	YES E' statement (Idchartered.com hartered.com he database, ments contain	YES Unified Auditing) are created to perfed within these ob any provide clues a	Passe orm business function jects. Logging and mand forensic evidence	all users ad MEDIUM ons and access nonitoring of all es about potentia			
POLICY_NAMI SCB_AUDIT_DIOLICY (1.43) 14366 Instance Previous Status Evaluation Date Oracle datab database as attempts to consultations (in the consultation of the	widence: E AUDIT_OPTION DL_P- CREATE PACKAGE Status of auditing for (oracle19:1:1621:PO) oracle19:1:1621:PO Passed 08/04/2024 at 10 pase packages, which defined by PL/SQL or create package, whether the package is the package of the package	AUDIT_OPTION_TYPE STANDARD ACTION T'CREATE PACKAGI HK5CCD.hk.standard COHK5CCD.hk.standardcl C38:34 PM (GMT+0530) The are stored within the ode and SQL states ther successful or ur This logging requires	YES E' statement (Idchartered.com hartered.com he database, ments contain nsuccessful, r	yes Unified Auditing) are created to perfeed within these ob any provide clues at the set as appropriate the set as a set as appropriate the set as appropriat	Passe orm business function jects. Logging and mand forensic evidenciate to the needs of	all users ad MEDIUM ons and access nonitoring of all es about potentia the business.			
POLICY_NAMI SCB_AUDIT_DI OLICY (1.43) 14366 Instance Previous Status Evaluation Date Dracle datab database as attempts to couspicious/un The following incolon separate	Status of auditing for (oracle19:1:1621:PO) Passed 08/04/2024 at 10 pase packages, which defined by PL/SQL oracle package, wheth nauthorized activities	AUDIT_OPTION_TYPE STANDARD ACTION T'CREATE PACKAGI HK5CCD.hk.standardcl 2:38:34 PM (GMT+0530) The are stored within the ode and SQL states the status of the audit_option, audit_option	YES E' statement (Idchartered.com hartered.com he database, ments contain nsuccessful, r	yes Unified Auditing) are created to perfeed within these ob any provide clues at the set as appropriate the set as a set as appropriate the set as appropriat	Passe orm business function jects. Logging and mand forensic evidenciate to the needs of	all users ad MEDIUM ons and access nonitoring of all es about potentia the business.			
Extended ExpoLicy_NAMI SCB_AUDIT_DIOLICY (1.43) 14366 Instance Previous Status Evaluation Date Dracle datab database as attempts to conspicious/under the following colon separate Expected	Status of auditing for (oracle19:1:1621:PO) Passed 08/04/2024 at 10 pase packages, which defined by PL/SQL oracte package, wheth authorized activities List String value(s) of X in advalues of policy_name, whether regular explications are considered by the constant of	AUDIT_OPTION_TYPE STANDARD ACTION T'CREATE PACKAGI HK5CCD.hk.standard COHK5CCD.hk.standard C	YES E' statement (Idchartered.com hartered.com he database, ments contain nsuccessful, r	yes Unified Auditing) are created to perfeed within these ob any provide clues at the set as appropriate the set as a set as appropriate the set as appropriat	Passe orm business function jects. Logging and mand forensic evidenciate to the needs of	all users and access nonitoring of all es about potentia the business.			
Extended ExpoLicy_NAMI SCB_AUDIT_DIOLICY (1.43) 14366 Instance Previous Status Evaluation Date Oracle datab database as attempts to conspicious/under the following colon separate Expected	Status of auditing for (oracle19:1:1621:PO) oracle19:1:1621:PO) oracle	AUDIT_OPTION_TYPE STANDARD ACTION T'CREATE PACKAGI HK5CCD.hk.standard COHK5CCD.hk.standard C	YES E' statement (Idchartered.com hartered.com he database, ments contain nsuccessful, r	yes Unified Auditing) are created to perfeed within these ob any provide clues at the set as appropriate the set as a set as appropriate the set as appropriat	Passe orm business function jects. Logging and mand forensic evidenciate to the needs of	all users and access nonitoring of all es about potentia the business.			

(1.43) 14366 Status of auditing for 'CREATE PACKAGE' statement (Unified Auditing) (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) Actual SCB_AUDIT_DDL_POLICY:CREATE PACKAGE:STANDARD ACTION:YES:YES:BY USER:ALL USERS **Extended Evidence:** ENABLED_OPTION POLICY_NAME AUDIT_OPTION_TYPE SUCCESS FAILURE ENTITY_NAME AUDIT_OPTION SCB_AUDIT_DDL_P- CREATE PACKAGE ALL USERS STANDARD ACTION YES YES BY USER OLICY

(1.43) 14366 Status of auditing for 'CREATE PACKAGE' statement (Unified Auditing) Passed MEDIUM (oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.								
Expected	matc	hes regular expre	ssion list					
	.*:CRE	ATE PACKAGE:.*:YES:	YES:.*:.*					
	OR, a	any of the selected	d values below:					
	Setting not found							
	Table not found							
				(0117 0500)				
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM (GM1+0530)				
	SCB_A	AUDIT_DDL_POLICY:0	CREATE PACKAGE:STA	NDARD ACTION:YES:Y	YES:BY USER:ALL USE	RS		
Extended Ex	Extended Evidence:							
POLICY_NAM	Е	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_D OLICY	DL_P-	CREATE PACKAGE	STANDARD ACTION	YES	YES	BY USER	ALL USERS	

(1.43) 14366 Status of auditing for 'CREATE PACKAGE' statement (Unified Auditing)(oracle19:1:1621: **MEDIUM** Passed POHK2CCD.hk.standardchartered.com)

oracle19:1:1621:POHK2CCD.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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_P- CREATE PACKAGE STANDARD ACTION YES ALL USERS YES BY USER OLICY

(1.44) 14367 Status of auditing for 'CREATE PACKAGE BODY' statement (Unified Auditing) (oracle19:1:1621:POHK1API.hk.standardchartered.com)

MEDIUM Passed

oracle19:1:1621:POHK1API.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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_type, success, failure, enabled_option, and entity_name.

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

matches regular expression list

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:

Expected

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_P-	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:POHK3CCD.hk.standardchartered.com)

Passed MEDIUM

oracle19:1:1621:POHK3CCD.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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_P- 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:POHK1RCT.hk.standardchartered.com)

Passed MEDIUM

MEDIUM

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_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:** AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION POLICY_NAME AUDIT_OPTION ENTITY_NAME SCB_AUDIT_DDL_P-CREATE PACKAGE STANDARD ACTION YES YES BY USER ALL USERS

(1.44) 14367 Status of auditing for 'CREATE PACKAGE BODY' statement (Unified Auditing) Passed (oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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. matches regular expression list **Expected** .*: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_TYPE SUCCESS AUDIT_OPTION **FAILURE** ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P-CREATE PACKAGE STANDARD ACTION YES YES BY USER ALL USERS OLICY BODY (1.44) 14367 Status of auditing for 'CREATE PACKAGE BODY' statement (Unified Auditing) **MEDIUM** Passed (oracle19:1:1621:POHK5CCD.hk.standardchartered.com) oracle19:1:1621:POHK5CCD.hk.standardchartered.com Instance Previous Status 08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date** 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_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 Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) Actual SCB_AUDIT_DDL_POLICY:CREATE PACKAGE BODY:STANDARD ACTION:YES:YES:BY USER:ALL USERS **Extended Evidence:** AUDIT_OPTION_TYPE SUCCESS **FAILURE** POLICY_NAME AUDIT_OPTION ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P- CREATE PACKAGE BODY STANDARD ACTION YES YES BY USER ALL USERS (1.44) 14367 Status of auditing for 'CREATE PACKAGE BODY' statement (Unified Auditing) **Passed MEDIUM** (oracle19:1:1621:POHK1CAT.hk.standardchartered.com) oracle19:1:1621:POHK1CAT.hk.standardchartered.com Instance Previous Status 08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date** 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. matches regular expression list **Expected** *:CREATE PACKAGE BODY:.*:YES:YES:.*:.* OR, any of the selected values below:

	Setting not found Table not found									
Actual	Last	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)								
	SCB_A	AUDIT_DDL_POLICY:0	CREATE PACKAGE BOI	OY:STANDARD ACTIO	N:YES:YES:BY USER:A	LL USERS				
Extended E	viden	ce:								
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCB_AUDIT_D OLICY	DL_P-	CREATE PACKAGE BODY	STANDARD ACTION	YES	YES	BY USER	ALL USERS			

(1.44) 14367 Status of auditing for 'CREATE PACKAGE BODY' statement (Unified Auditing) Pass (oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_type, success, failure, enabled_option, and entity_name.

Expected	matches regular expression list								
	.*:CRE	ATE PACKAGE BODY:	*:YES:YES:.*:.*						
	OR, a	any of the selected	l values below:						
	Set	ting not found							
	☐ Table not found								
Actual	Loot	l Indoted (00/04/202	14 at 06:04:00 DM (CMT - 0520\					
		Updated:08/04/202		•					
	SCB_A	SCB_AUDIT_DDL_POLICY:CREATE PACKAGE BODY:STANDARD ACTION:YES:YES:BY USER:ALL USERS							
Extended Ev	idenc	e:							
POLICY_NAME	2	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_DIOLICY	DL_P-	CREATE PACKAGE BODY	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.44) 14367 Status of auditing for 'CREATE PACKAGE BODY' statement (Unified Auditing) Passed MEDIUM (oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

contains color	separated values of policy_name, addit_option_type, success, fandre, chabited_option, and chatty_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_P- CREATE PACKAGE STANDARD ACTION YES YES BY USER ALL USERS OLICY

(1.45) 14368 Status of auditing for 'ALTER PROCEDURE' statement (Unified Auditing) (oracle19:1:1621:POHK1API.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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									
	.*:ALT	.*:ALTER PROCEDURE:.*:YES:YES:.*:*								
	OR, a	any of the selected	l values below:							
	Set	tting not found								
	Table not found									
Actual	Last Undated:08/04/2024 at 06:01:00 PM /GMT:0520)									
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 E	Extended Evidence:									
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCB_AUDIT_I	DL_P-	ALTER PROCEDURE	STANDARD ACTION	YES	YES	BY USER	ALL USERS			

(1.45) 14368 Status of auditing for 'ALTER PROCEDURE' statement (Unified Auditing) (oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

colon separate	ed value	es of policy_name, aud	dit_option, audit_optic	on_type, success, failu	re, enabled_option, ar	nd entity_name.			
Expected	matc	hes regular expres	ssion list						
	.*:ALT	ER PROCEDURE:.*:YE	S:YES:.*:.*						
	OR, a	ny of the selected	I values below:						
	Setting not found								
	Table not found								
				·					
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM (GM1+0530)					
	SCB_A	.UDIT_DDL_POLICY:A	LTER PROCEDURE:ST	ANDARD ACTION:YES	S:YES:BY USER:ALL US	SERS			
Extended E	Extended Evidence:								
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_D OLICY	DL_P-	ALTER PROCEDURE	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.45) 14368 Status of auditing for 'ALTER PROCEDURE' statement (Unified Auditing) (oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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. matches regular expression list *:ALTER PROCEDURE:.*:YES:YES:.*:.* OR, any of the selected values below: Setting not found Table not found Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) Actual 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 BY USER SCB_AUDIT_DDL_P- ALTER PROCEDURE STANDARD ACTION YES YES ALL USERS

(1.45) 14368 Status of auditing for 'ALTER PROCEDURE' statement (Unified Auditing) (oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) Actual 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_P- ALTER PROCEDURE STANDARD ACTION YES ALL USERS YES BY USER

(1.45) 14368 Status of auditing for 'ALTER PROCEDURE' statement (Unified Auditing) (oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

Oracle_ATOS - 20240806 page 454

Passed MEDIUM

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_P- ALTER PROCEDURE | STANDARD ACTION | YES YES BY USER ALL USERS

(1.45) 14368 Status of auditing for 'ALTER PROCEDURE' statement (Unified Auditing) (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

matches regular expression list **Expected** *: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:** AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION POLICY NAME AUDIT_OPTION ENTITY_NAME SCB_AUDIT_DDL_P- ALTER PROCEDURE | STANDARD ACTION | YES YES BY USER ALL USERS

(1.45) 14368 Status of auditing for 'ALTER PROCEDURE' statement (Unified Auditing) (oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

	List Strir es of pol	ng value(s) of X indica icy_name, audit_opti	ites the status of the A on, audit_option_type,	LTER PROCEDURE success, failure, en	audit option type defined abled_option, and entity_	d on the database. The or _name.	utput contains colon				
xpected	match	es regular expres	sion list								
	.*:ALTE	ALTER PROCEDURE: *:YES:YES: *:.* OR, any of the selected values below: Setting not found Table not found									
	OR, aı										
	Tabl										
ctual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)										
	SCB_AU	JDIT_DDL_POLICY:AI	LTER PROCEDURE:STA	NDARD ACTION:YI	ES:YES:BY USER:ALL USE	RS					
xtended Ev	vidence	:									
OLICY_NAME		AUDIT_OPTION	AUDIT_OPTION_TYPE		FAILURE	ENABLED_OPTION	ENTITY_NAME				
CB_AUDIT_DI LICY	DL_P-	ALTER PROCEDURE	STANDARD ACTION	YES	YES	BY USER	ALL USERS				
(1.45) 14	4368 S (c	tatus of auditing f oracle19:1:1621:P	or 'ALTER PROCEI OHK2CCD.hk.stand	OURE' statemen lardchartered.co	t (Unified Auditing) om)	Passo	ed MEDIUM				
Instance			:POHK2CCD.hk.standa	rdchartered.com							
Previous S		Passed	100004 DM (OME OF	-00)							
Evaluation	1 Date	08/04/2024 at	10:38:34 PM (GMT+05	30)							
database attempts	e as de s to alte I suspid	efined by PL/SQL er procedure, whe	code and SQL statether successful or	atements contai unsuccessful,	e, are created to pe ned within these obj may provide clues a nent should be set as	ects. Logging and nand forensic evidence	nonitoring of all es about				
The follocolon sep	owing List String value(s) of X indicates the status of the ALTER PROCEDURE audit option type defined on the database. The output contains parated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.										
Expecte	ed m	atches regular ex	pression list								
	.*:	.*:ALTER PROCEDURE:.*:YES:YES:.*:.*									
	0	OR, any of the selected values below:									
		Setting not found									
		Table not found									
Actual		Table not found	/2024 at 06:01:09 P	M (GMT+0530)							
Actual	La	Table not found ast Updated:08/04	/2024 at 06:01:09 P CY:ALTER PROCEDUR		ON:YES:YES:BY USER:ALI	L USERS					
	L:	Table not found ast Updated:08/04 CB_AUDIT_DDL_POLI			ON:YES:YES:BY USER:ALI	_ USERS					
Extende	La SC ed Evid	Table not found ast Updated:08/04 CB_AUDIT_DDL_POLI lence:	CY:ALTER PROCEDUR	E:STANDARD ACTIO	ON:YES:YES:BY USER:ALI FAILURE		ENTITY NAME				
Extende POLICY_	La SC ed Evid NAME	Table not found ast Updated:08/04 CB_AUDIT_DDL_POLI lence: AUDIT_OPTION		E:STANDARD ACTION		ENABLED_OPTION BY USER	ENTITY_NAME ALL USERS				
Extended POLICY_SCB_AULOLICY (1.46) 14 Instance Previous S	Li SC ed Evid NAME DIT_DDL 4369 SP	Table not found ast Updated:08/04 CB_AUDIT_DDL_POLI lence: AUDIT_OPTION _P- ALTER PROCEDI tatus of auditing f OHK1API.hk.stand oracle19:1:1621 Passed	AUDIT_OPTION_T JRE STANDARD ACTION or 'ALTER FUNCTION dardchartered.com :POHK1API.hk.standar	E:STANDARD ACTION YPE SUCCESS ON YES ON' statement (I) dchartered.com	FAILURE	ENABLED_OPTION BY USER	ALL USERS				
Extender POLICY_SCB_AULOLICY (1.46) 14	Li SC ed Evid NAME DIT_DDL 4369 SP	Table not found ast Updated:08/04 CB_AUDIT_DDL_POLI lence: AUDIT_OPTION _P- ALTER PROCEDI tatus of auditing f OHK1API.hk.stand oracle19:1:1621 Passed	AUDIT_OPTION_T JRE STANDARD ACTION or 'ALTER FUNCTION dardchartered.com	E:STANDARD ACTION YPE SUCCESS ON YES ON' statement (I) dchartered.com	FAILURE YES	ENABLED_OPTION BY USER	ALL USERS				
POLICY_SCB_AULOLICY (1.46) 14 Instance Previous S Evaluation Oracle d database attempts suspicio	La SC ed Evid NAME DIT_DDL 4369 S P Status Date database e as des s to alte bus/una	Table not found ast Updated:08/04 CB_AUDIT_DDL_POLI lence: AUDIT_OPTION _P- ALTER PROCEDI tatus of auditing f OHK1API.hk.stand oracle19:1:1621 Passed 08/04/2024 at se function, which efined by PL/SQL er function, wheth uthorized activities	AUDIT_OPTION_T JRE STANDARD ACTIO or 'ALTER FUNCTIO dardchartered.com :POHK1API.hk.standar 10:38:34 PM (GMT+05) are stored within code and SQL states er successful or uses. This logging recommendations	ESTANDARD ACTION YPE SUCCESS ON YES ON' statement (I) Indichartered.com 530) the database, a atements contain successful, many appropriate the contain successful suc	FAILURE YES Jnified Auditing)(oracle are created to perform ned within these objusty provide clues and ld be set as appropri	ENABLED_OPTION BY USER cle19:1:1621: Passe m business function jects. Logging and not forensic evidences riate to the needs of	ALL USERS ed MEDIUM as and access monitoring of all about potential the business.				
Extended POLICY_SCB_AULOLICY (1.46) 14 Instance Previous S Evaluation Oracle of database attempts suspicion The follocolon sep	ed Evid NAME DIT_DDL 4369 S P Status n Date database e as des to alte us/una	Table not found ast Updated:08/04 CB_AUDIT_DDL_POLI lence: AUDIT_OPTION _P- ALTER PROCEDU tatus of auditing foohK1API.hk.standoracle19:1:1621 Passed 08/04/2024 at se function, which efined by PL/SQL er function, wheth uthorized activities at String value(s) of X values of policy_name	AUDIT_OPTION_T JRE STANDARD ACTION OF 'ALTER FUNCTION dardchartered.com :POHK1API.hk.standar 10:38:34 PM (GMT+05) are stored within code and SQL states er successful or unless. This logging receindicates the status of equalit_option, audit_compared.	ESTANDARD ACTION YPE SUCCESS ON YES ON' statement (I) Indichartered.com 530) the database, a atements contain successful, many appropriate the contain successful suc	FAILURE YES Jnified Auditing)(oracle are created to perform ned within these objusy provide clues and	ENABLED_OPTION BY USER cle19:1:1621: Passe m business function jects. Logging and not forensic evidences riate to the needs of	ALL USERS ed MEDIUM as and access monitoring of all about potential the business.				
POLICY_SCB_AULOLICY (1.46) 14 Instance Previous S Evaluation Oracle d database attempts suspicio	ed Evid NAME DIT_DDL 4369 S P Status n Date database e as de s to alte us/una owing Lis parated v ed m	Table not found ast Updated:08/04 CB_AUDIT_DDL_POLI lence: AUDIT_OPTION ALTER PROCEDI tatus of auditing f OHK1API.hk.stand oracle19:1:1621 Passed 08/04/2024 at se function, which efined by PL/SQL er function, wheth uthorized activitie at String value(s) of X values of policy_name latches regular ex	AUDIT_OPTION_T JRE STANDARD ACTION or 'ALTER FUNCTION dardchartered.com :POHK 1 API.hk.standar 10:38:34 PM (GMT+05) are stored within code and SQL state er successful or uses. This logging received indicates the status of exaudit_option, audit_corression list	ESTANDARD ACTION YPE SUCCESS ON YES ON' statement (I) Indichartered.com 530) the database, a atements contain successful, many appropriate the contain successful suc	FAILURE YES Jnified Auditing)(oracle are created to perform ned within these objusty provide clues and ld be set as appropri	ENABLED_OPTION BY USER cle19:1:1621: Passe m business function jects. Logging and not forensic evidences riate to the needs of	ALL USERS ed MEDIUM as and access monitoring of all about potential the business.				
Extended POLICY_SCB_AULOLICY (1.46) 14 Instance Previous S Evaluation Oracle of database attempts suspicion The follocolon sep	ed Evid NAME DIT_DDL 4369 S P Status in Date database e as de is to alte in Date database e as de is to alte database e as de is to alte database e as de is to alte database da database database database database database database database databa	Table not found ast Updated:08/04 CB_AUDIT_DDL_POLI dence: AUDIT_OPTION _P- ALTER PROCEDI tatus of auditing f OHK1API.hk.stand oracle19:1:1621 Passed 08/04/2024 at se function, which efined by PL/SQL er function, wheth uthorized activitie at String value(s) of X values of policy_name atches regular ex ALTER FUNCTION:*:	AUDIT_OPTION_T JRE STANDARD ACTIO or 'ALTER FUNCTION dardchartered.com :POHK1API.hk.standar 10:38:34 PM (GMT+05) in are stored within acode and SQL states are successful or under the status of experimental endicates the experime	E:STANDARD ACTION YPE SUCCESS ON' Statement (I) Indichartered.com Signification Significati	FAILURE YES Jnified Auditing)(oracle are created to perform ned within these objusty provide clues and ld be set as appropri	ENABLED_OPTION BY USER cle19:1:1621: Passe m business function jects. Logging and not forensic evidences riate to the needs of	ALL USERS ed MEDIUM as and access monitoring of all about potential the business.				
Extended POLICY_SCB_AULOLICY (1.46) 14 Instance Previous S Evaluation Oracle of database attempts suspicion The follocolon sep	ed Evid NAME DIT_DDL 4369 S P Status in Date database e as de is to alte in Date database e as de is to alte database e as de is to alte database e as de is to alte database da database database database database database database database databa	Table not found ast Updated:08/04 CB_AUDIT_DDL_POLI dence: AUDIT_OPTION _P- ALTER PROCEDI tatus of auditing f OHK1API.hk.stand oracle19:1:1621 Passed 08/04/2024 at se function, which efined by PL/SQL er function, wheth uthorized activitie at String value(s) of X values of policy_name atches regular ex ALTER FUNCTION:*:	AUDIT_OPTION_T JRE STANDARD ACTION or 'ALTER FUNCTION dardchartered.com :POHK 1 API.hk.standar 10:38:34 PM (GMT+05) are stored within code and SQL state er successful or uses. This logging received indicates the status of exaudit_option, audit_corression list	E:STANDARD ACTION YPE SUCCESS ON' Statement (I) Indichartered.com Signification Significati	FAILURE YES Jnified Auditing)(oracle are created to perform ned within these objusty provide clues and ld be set as appropri	ENABLED_OPTION BY USER cle19:1:1621: Passe m business function jects. Logging and not forensic evidences riate to the needs of	ALL USERS ed MEDIUM as and access monitoring of all about potential the business.				

Actual Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)										
SC	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_ OLICY	P ALTER FUNCTION	STANDARD ACTION	YES	YES	BY USER	ALL USERS				

(1.46) 14369 Status of auditing for 'ALTER FUNCTION' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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. matches regular expression list *:ALTER FUNCTION:.*:YES:YES:.*:.* OR, any of the selected values below: Setting not found Table not found Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) Actual SCB_AUDIT_DDL_POLICY:ALTER FUNCTION:STANDARD ACTION:YES:YES:BY USER:ALL USERS **Extended Evidence:** POLICY_NAME **FAILURE** AUDIT_OPTION_TYPE SUCCESS ENABLED_OPTION ENTITY_NAME AUDIT_OPTION STANDARD ACTION YES ALL USERS SCB_AUDIT_DDL_P- ALTER FUNCTION YES BY USER OLICY

(1.46) 14369 Status of auditing for 'ALTER FUNCTION' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

colon separate	colon separated values of policy_name, audit_option_type, success, failure, enabled_option, and entity_name.								
Expected	matc	hes regular expre	ssion list						
	.*:ALT	ER FUNCTION:.*:YES:	YES:.*:.*						
	OR, a	any of the selected	d values below:						
	Setting not found								
	Table not found								
A = 1	1	Lll	0.4 =1.00-04-00 DM	(OMT - 0500)					
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 E	vidend	ce:							
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_D OLICY	DL_P-	ALTER FUNCTION	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.46) 14369 Status of auditing for 'ALTER FUNCTION' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	matc	hes regular expre	ssion list						
	.*:ALTER FUNCTION:.*:YES:YES::*:								
OR, any of the selected values below:									
	Set	ting not found							
	Table not found								
A			04 - 4 00 04 00 DN	(OMT OFOO)					
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM ((GM I +0530)					
	SCB_A	AUDIT_DDL_POLICY:A	ALTER FUNCTION:STA	NDARD ACTION:YES:	YES:BY USER:ALL USE	RS			
Extended E	Extended Evidence:								
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_D OLICY	DL_P-	ALTER FUNCTION	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.46) 14369 Status of auditing for 'ALTER FUNCTION' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_type, success, failure, enabled_option, and entity_name.

colon separate	colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.								
Expected	matches regular expression list								
	.*:ALT	ER FUNCTION:.*:YES:	YES:.*:.*						
	OR, a	any of the selected	l values below:						
	Setting not found								
	Table not found								
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM ((GMT+0530)					
	SCB_A	AUDIT_DDL_POLICY:A	LTER FUNCTION:STA	NDARD ACTION:YES:	YES:BY USER:ALL USE	RS			
Extended Ex	/iden	ce:							
POLICY_NAMI	3	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_D	DL_P-	ALTER FUNCTION	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.46) 14369 Status of auditing for 'ALTER FUNCTION' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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									
	.*:ALT	.*:ALTER FUNCTION:.*:YES:YES:.*:.*								
	OR, any of the selected values below:									
Setting not found										
	Table not found									
		11. 1.4. 1.00/04/00/	04 - 4 00 04 00 DM	(OMT OFOO)						
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 E	Extended Evidence:									
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCB_AUDIT_D	DL_P-	ALTER FUNCTION	STANDARD ACTION	YES	YES	BY USER	ALL USERS			

(1.46) 14369 Status of auditing for 'ALTER FUNCTION' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_type, success, failure, enabled_option, and entity_name.

Expected	matc	hes regular expres	ssion list				
	.*:ALT	ER FUNCTION:.*:YES:	YES:.*:.*				
	OR, any of the selected values below:						
	Set	ting not found					
	Tal	ole not found					
Actual	Loot	l Indoted .00/04/201	04 at 06:04:00 DM /	CMT - 0520\			
Actual	Last	Updated:06/04/202	24 at 06:01:09 PM (GIVI I +0530)			
	SCB_A	AUDIT_DDL_POLICY:A	LTER FUNCTION:STA	NDARD ACTION:YES:	YES:BY USER:ALL USE	RS	
Extended Ex	videnc	e:					
POLICY_NAM	Е	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_D OLICY	DL_P-	ALTER FUNCTION	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.46) 14369 Status of auditing for 'ALTER FUNCTION' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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, a	DR, any of the selected values below:						
	Set	ting not found						
	Tal	ble not found						
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM ((GMT+0530)				
	SCB_A	AUDIT_DDL_POLICY: <i>A</i>	ALTER FUNCTION:STA	NDARD ACTION:YES:Y	YES:BY USER:ALL USE	RS		
Extended Ex	/iden	ce:						
POLICY_NAMI	3	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_D OLICY	DL_P-	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: Passed MEDIUM POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	matc	hes regular expres	ssion list					
	.*:ALT	ER PACKAGE:.*:YES:Y	ES:.*:.*					
	OR, a	any of the selected	I values below:					
Setting not found								
	Tal	ole not found						
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)							
Actual								
	SCB_AUDIT_DDL_POLICY:ALTER PACKAGE:STANDARD ACTION:YES:YES:BY USER:ALL USERS							
Extended Ev	/idend	e:						
POLICY_NAMI	3	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_D: OLICY	DL_P-	ALTER PACKAGE	STANDARD ACTION	YES	YES	BY USER	ALL USERS	

(1.47) 14370 Status of auditing for 'ALTER PACKAGE' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

coion separate	ed 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 E	vidence:

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

(1.47) 14370 Status of auditing for 'ALTER PACKAGE' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	matc	nes regular expres	ssion list					
	.*:ALT	ER PACKAGE:.*:YES:Y	ES:.*:.*					
	OR, a	any of the selected	d values below:					
	Set	ting not found						
	Tal	ole not found						
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM ((GMT+0530)				
	SCB_AUDIT_DDL_POLICY:ALTER PACKAGE:STANDARD ACTION:YES:YES:BY USER:ALL USERS							
Extended E	vidend	ce:						
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_D	DL_P-	ALTER PACKAGE	STANDARD ACTION	YES	YES	BY USER	ALL USERS	

(1.47) 14370 Status of auditing for 'ALTER PACKAGE' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

colon separated	values of policy_name, as	udit_option, audit_option	on_type, success, failu	ıre, enabled_option, aı	nd entity_name.	1	
Expected r	natches regular expre	ession list					
<u>.</u>	*:ALTER PACKAGE:.*:YES:	YES:.*:.*					
	OR, any of the selected values below:						
	Setting not found						
	Table not found						
Actual I	ast Updated:08/04/20	024 at 06:01:09 PM ((GMT+0530)				
S	CB_AUDIT_DDL_POLICY:	ALTER PACKAGE:STAN	DARD ACTION:YES:Y	ES:BY USER:ALL USER	S		
Extended Evi	dence:						
POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_DD OLICY	L_P- ALTER PACKAGE	STANDARD ACTION	YES	YES	BY USER	ALL USERS	

(1.47) 14370 Status of auditing for 'ALTER PACKAGE' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) Actual 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- ALTER PACKAGE STANDARD ACTION YES YES BY USER ALL USERS OLICY

(1.47) 14370 Status of auditing for 'ALTER PACKAGE' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) Actual SCB_AUDIT_DDL_POLICY:ALTER PACKAGE:STANDARD ACTION:YES:YES:BY USER:ALL USERS **Extended Evidence:** AUDIT_OPTION_TYPE SUCCESS **FAILURE** ENABLED_OPTION POLICY_NAME AUDIT_OPTION ENTITY_NAME SCB_AUDIT_DDL_P- ALTER PACKAGE STANDARD ACTION YES YES BY USER ALL USERS

OLICI						
(1 47) 14370 Stat	us of auditing for '	ALTER PACKAGE'	statement (Unified	d Auditing)(oracle1	9.1.1621 Pass	ed MEDIUM
(IITI) ITOIO OLUL	ao oi aaaitiiig ioi	~ = : = : · · · · · · · · · · · · · · · ·	otatomont (ommo	a maaitiiiggoi aolo i	0.1.10 <u>-</u> 1. 1 033	

POHK1CCD.hk.standardchartered.com)
Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

Extended Evidence: POLICY NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME SUBJECT NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME OULT NAME AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME OULT NAME AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME NAME AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME NAME AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME AUDIT_OPTION_AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME OULTED_PACKAGE STANDARD ACTION_YES YES BY USER ALL USERS Extended Evidence: POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME OULTED_PACKAGE STANDARD ACTION_YES YES BY USER ALL USERS EXECUTED. 1.48) 14371 Status of auditing for 'ALTER PACKAGE BODY' statement (Unified Auditing) Passed MEDIL (oracle19:1:1621:POHK1API.hk.standardchartered.com) Passed MEDIL (Unified Auditing) Passed MEDIL (Oracle19:1:1621:POHK1API.hk.standardchartered.com)		matches regular expression list									
Actual Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) SCB_AUDTT_DDL_POLICY_ALTER PACKACE_STANDARD ACTION_YES_YES_BY_USER_ALL_USERS Extended Evidence: POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE_SUCCESS FAILURE ENABLED_OPTION ENTITY_NAMS. SCB_AUDTT_DDL_P— ALTER PACKACE STANDARD ACTION_YES YES BY_USER ALL_USERS BY USER ALL_USERS OULCY 1.477 14370 Status of auditing for "ALTER PACKAGE" statement (Unified Auditing)(oracle19:1:1621: Passed MEDIL POHKZCCD.hk.standardchartered.com POHKZCCD.hk.standardchartered.com Passed OR_04/2024 at 10:38:34 PM (GMT+0530) Oracle database packages, which are stored within the database, are created to perform business functions and accelatabase as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring of attempts to alter package, whether successful or unsuccessful, may provide clues and forensic evidences about poter tumps to alter package, whether successful or unsuccessful, may provide clues and forensic evidences about poter user of the provide clues and forensic evidences about poter user of the provide clues and forensic evidences about poter user of the provide clues and forensic evidences about poter user of the provide clues and forensic evidences about poter user of the provide clues and forensic evidences about poter user of the provide clues and forensic evidences about poter user of the provide clues and forensic evidences about poter user of the provide clues and forensic evidences about poter user of the provide clues and forensic evidences about poter user of the provide clues and forensic evidences about poter user of the provide clues and forensic evidences about poter user of the provide clues of the business functions are stored values of policy name, audic, option, audit, option, type, success, failure, enabled, option, and entity, name. Expected **ALTER PACKAGE.**YESYES.**** OR, any of the selected values below: Setting not found Table not found Table not found **ALTER PACKAGE.**YESYES.**** OR, any o		.*:ALTER PACKAGE:.*:YES	S:YES:.*:.*								
Table not found Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)		OR, any of the selected values below:									
Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) SCB_AUDIT_DDL_POLICY:ALTER PACKACE-STANDARD ACTION:YES:YES:BY USERALL USERS Extended Evidence: POLICY:NAME AUDIT_OPTION AUDIT_OPTION.TYPE:SUCCESS FAILURE ENABLED_OPTION ENTITY:NAME SCB_AUDIT_DDL_P- ALTER PACKACE 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- ALTER PACKAGE STANDARD ACTION YES YES BY USER ALL USERS 1.47) 14370 Status of auditing for 'ALTER PACKAGE' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIL POHK2CD.hk.standardchartered.com) POHK2CCD.hk.standardchartered.com PoHK2CD.hk.standardchartered.com		☐ Table not found									
Extended Evidence: POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME OULCY 1.47) 14370 Status of auditing for 'ALTER PACKAGE' STANDARD ACTION YES YES BY USER ALL USERS MEDIT_OPTION_ENTITY_NAME OULCY 1.47) 14370 Status of auditing for 'ALTER PACKAGE' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIT OPTION_ENTITY_NAME OULCY) 1.47) 14370 Status of auditing for 'ALTER PACKAGE' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIT OPTION_ENTITY_NAME OULCY) 1.47) 14370 Status of auditing for 'ALTER PACKAGE' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIT OPTION_ENTITY_NAME OULCY) 1.47) 14370 Status of auditing for 'ALTER PACKAGE BODY' statement (Unified Auditing) Passed MEDIT OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_PALTER PACKAGE STANDARD ACTION YES YES BY USER ALL USERS Extended Evidence: Extended Evidence:	Actual	Last Updated:08/04/2	2024 at 06:01:09 PM	(GMT+0530)							
POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P—ALTER PACKAGE STANDARD ACTION YES YES BY USER ALL USERS MEDIL OF THE PACKAGE STANDARD ACTION YES YES BY USER ALL USERS MEDIL OF THE PACKAGE STANDARD ACTION YES YES BY USER ALL USERS MEDIL OF THE PACKAGE STANDARD ACTION YES YES BY USER ALL USERS MEDIL OF THE PACKAGE STANDARD ACTION YES YES BY USER ALL USERS MEDIL OF THE 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—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—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—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—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—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—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—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—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 AUDIT_OPTION_TYPE SUCCESS FAI		SCB_AUDIT_DDL_POLIC	Y:ALTER PACKAGE:STAN	NDARD ACTION:	YES:YES:BY USER:ALL	USERS					
ALL USERS OLLCY 1.4.7) 14370 Status of auditing for 'ALTER PACKAGE' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIL POHK2CCD.hk.standardchartered.com) POHK2CCD.hk.standardchartered.com POHK2CCD.hk.standardchartered.com Passed O8/04/2024 at 10:38:34 PM (GMT+0530) O7acle database packages, which are stored within the database, are created to perform business functions and acceleatabase as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring of a titempts to alter package, whether successful or unsuccessful, may provide clues and forensic evidences about poter uspicious/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: **YESYPES:**** 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 USERALL USERS Extended Evidence: POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAMI SCB_AUDIT_DDL_P- ALTER PACKAGE STANDARD ACTION YES YES BY USER ALL USERS Extended Evidence: POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAMI SCB_AUDIT_DDL_P- ALTER PACKAGE STANDARD ACTION YES YES BY USER ALL USERS Extended Evidence: POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAMI SCB_AUDIT_DDL_P- ALTER PACKAGE STANDARD ACTION YES YES BY USER ALL USERS ### ALTER PACKAGE STANDARD ACTION YES YES BY USER ALL USERS ### ALTER PACKAGE STANDARD ACTION YES YES BY USER ALL USERS ### ALTER PACKAGE STANDARD ACTION YES YES BY USER ALL USERS ### ALTER PACKAGE STANDARD	Extended E	Evidence:									
1.47) 14370 Status of auditing for 'ALTER PACKAGE' statement (Unified Auditing)(oracle19:1:1621: Passed POHK2CCD.hk.standardchartered.com) 1.55 passed oracle19:1:1621:POHK2CCD.hk.standardchartered.com 1.56 passed oracle19:1:1621:POHK2CD.hk.standardchartered.com 1.57 passed oracle19:1:1621:POHK2CD.hk.standardchartered.com 1.58 passed oracle19:1:1621:POHK2CD.hk.standardchartered.com 1.58 passed oracle19:1:1621:POHK2CD.hk.standardchartered.com 1.58 passed oracle19:1:1621:POHK2CD.hk.standardchartered.com 1.58 passed oracle19:1:1621:POHK12CD.hk.standardchartered.com 1.58 passed oracle19:1:1621:POHK12CD.hk.standardchartered.com 1.59 passed oracle19:1:1621:POHK1AP.hk.standardchartered.com 1.50 passed oracle19:1:1621:POHK1AP.hk.stan	POLICY_NAM	ME AUDIT_OPTION	AUDIT_OPTION_TYPI	E SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME				
POHK2CCD.hk.standardchartered.com revious Status valuation Date oracle19:1:1621:POHK2CCD.hk.standardchartered.com Passed 08/04/2024 at 10:38:34 PM (GMT+0530) Oracle database packages, which are stored within the database, are created to perform business functions and accellatabase as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring of attempts to alter package, whether successful or unsuccessful, may provide clues and forensic evidences about poter uspicious/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_type, success, failure, enabled_option, and entity_name. Expected matches regular expression list "*ALTER PACKAGE.**YESYES.**.** OR, any of the selected values below: Setting not found Actual Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) SCB_AUDIT_DDL_POLICY:ALTER PACKAGE.STANDARD ACTION:YESYES:BY USERALL USERS Extended Evidence: POLICY_NAME AUDIT_OPTION AUDIT_OPTION AUDIT_OPTION TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAMI SCB_AUDIT_DDL_P- ALTER PACKAGE STANDARD ACTION YES YES BY USER ALL USERS MEDIL (oracle19:1:1621:POHK1APLhk.standardchartered.com Passed O8/04/2024 at 10:38:34 PM (GMT+0530) Oracle database package bodies, which are stored within the database, are created to perform business functions and cocess database as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitorir	SCB_AUDIT_I OLICY	DDL_P- ALTER PACKAGE	STANDARD ACTION	YES	YES	BY USER	ALL USERS				
oracle 19:1:1621:POHK2CCD.hk.standardchartered.com Passed valuation Date 08/04/2024 at 10:38:34 PM (GMT+0530) Oracle database packages, which are stored within the database, are created to perform business functions and acce latabase as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring of a latabase as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring of a latabase as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring of a latabase as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring of a latabase as defined by PL/SQL code and SQL statements contained on the database. Logging and monitoring of a latabase as defined by PL/SQL code and SQL statements (Unified Auditing) Oracle database package bodies, which are stored within the database, are created to perform business functions and cocess database as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring oracle database as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring and acce latabase are created to perform business functions and cocess database as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring are created to perform business functions and cocess database as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring are created to perform business functions and cocess database as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring latabase created to perform business functions and cocess database as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring latabase created to perform business functions and cocess database as defined by PL/SQL code and SQL statements contained within these objects.	1.47) 14370	Status of auditing fo POHK2CCD.hk.stand	r 'ALTER PACKAGE' dardchartered.com)	statement (U	nified Auditing)(ora	acle19:1:1621: Passe	ed MEDIUN				
Oracle database packages, which are stored within the database, are created to perform business functions and acce database as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring of attempts to alter package, whether successful or unsuccessful, may provide clues and forensic evidences about poter uspicious/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, uppe, success, failure, enabled_option, and entity_name. Expected matches regular expression list	nstance		•	hartered.com							
Pracele database packages, which are stored within the database, are created to perform business functions and accelatabase as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring of attempts to alter package, whether successful or unsuccessful, may provide clues and forensic evidences about poter uspicious/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_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 Actual Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) SCB_AUDIT_DDL_POLICY:ALTER PACKAGE:STANDARD ACTION:YES:YES:BY USERALL USERS Extended Evidence: POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAMI SCB_AUDIT_DDL_P- ALTER PACKAGE STANDARD ACTION YES YES BY USER ALL USERS OLICY 1.48) 14371 Status of auditing for 'ALTER PACKAGE BODY' statement (Unified Auditing) Passed MEDIU (oracle19:1:1621:POHK1API.hk.standardchartered.com) Passed O8/04/2024 at 10:38:34 PM (GMT+0530) Oracle database package bodies, which are stored within the database, are created to perform business functions and cocess database as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitorir	revious Status	s Passed									
atabase as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring of a ttempts to alter package, whether successful or unsuccessful, may provide clues and forensic evidences about poter uspicious/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_type, success, failure, enabled_option, and entity_name. Expected matches regular expression list "ALTER PACKAGE."YESYES.".** 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 SCB_AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAMI SCB_AUDIT_DDL_P- ALTER PACKAGE STANDARD ACTION YES YES BY USER ALL USERS 1.48) 14371 Status of auditing for 'ALTER PACKAGE BODY' statement (Unified Auditing) Passed MEDIT_OPTION_STATE Passed O8/04/2024 at 10:38:34 PM (GMT+0530) Oracle 19:1:1621:POHK1APLhk.standardchartered.com Passed O8/04/2024 at 10:38:34 PM (GMT+0530) Oracle database package bodies, which are stored within the database, are created to perform business functions and cocess database as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring contained within these objects.	valuation Dat	e 08/04/2024 at 10	0:38:34 PM (GMT+0530)							
atabase as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring of a ttempts to alter package, whether successful or unsuccessful, may provide clues and forensic evidences about poter uspicious/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_type, success, failure, enabled_option, and entity_name. Expected matches regular expression list "ALTER PACKAGE."YESYES.".** 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 SCB_AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAMI SCB_AUDIT_DDL_P- ALTER PACKAGE STANDARD ACTION YES YES BY USER ALL USERS 1.48) 14371 Status of auditing for 'ALTER PACKAGE BODY' statement (Unified Auditing) Passed MEDIT_OPTION_STATE Passed O8/04/2024 at 10:38:34 PM (GMT+0530) Oracle 19:1:1621:POHK1APLhk.standardchartered.com Passed O8/04/2024 at 10:38:34 PM (GMT+0530) Oracle database package bodies, which are stored within the database, are created to perform business functions and cocess database as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring contained within these objects.											
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_NAMI SCB_AUDIT_DDL_P- ALTER PACKAGE STANDARD ACTION YES YES BY USER ALL USERS OLICY 1.48) 14371 Status of auditing for 'ALTER PACKAGE BODY' statement (Unified Auditing) (oracle19:1:1621:POHK1API.hk.standardchartered.com) Instance oracle 19:1:1621:POHK1API.hk.standardchartered.com Passed oracle 19:1:1621:POHK1API.hk.standardchartered.com	ttempts to uspicious/u	alter package, whethe unauthorized activities	er successful or uns s. This logging requi	successful, ma rement shoul	ay provide clues a d be set as approp	nd forensic evidences oriate to the needs of	s about potentia the business.				
*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_NAMI SCB_AUDIT_DDL_P- ALTER PACKAGE STANDARD ACTION YES YES BY USER ALL USERS MEDIL Oracle19:1:1621:POHK1API.hk.standardchartered.com revious Status valuation Date O8/04/2024 at 10:38:34 PM (GMT+0530) Oracle database package bodies, which are stored within the database, are created to perform business functions and cocess database as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring and cocess database as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring and cocess database.	The following colon separat	g List String value(s) of X ir ted values of policy_name,	ndicates the status of the audit_option, audit_opti	e ALTER PACKAC on_type, success	E audit option type de s, failure, enabled_option	fined on the database. The on, and entity_name.	e output contains				
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	Expected										
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	=	* AT MED DACKAGE * MEG	P.V.P.C. *. *								
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	-										
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	-										
Extended Evidence: POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P- 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.hk.standardchartered.com) Instance oracle19:1:1621:POHK1API.hk.standardchartered.com Passed O8/04/2024 at 10:38:34 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		OR, any of the select									
POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P—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.hk.standardchartered.com) Instance oracle19:1:1621:POHK1API.hk.standardchartered.com Passed	·	OR, any of the select									
POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P- 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.hk.standardchartered.com) Instance oracle19:1:1621:POHK1API.hk.standardchartered.com Passed oracle19:1:1621:POHK1API.hk.standardchartered.com Passed oracle19:1:1621:POHK1API.hk.standardchartered.com Passed oracle19:1:1621:POHK1API.hk.standardchartered.com Passed 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	Actual	OR, any of the select Setting not found Table not found	ted values below:	(GMT+0530)							
POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P- 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.hk.standardchartered.com) Instance oracle19:1:1621:POHK1API.hk.standardchartered.com Passed oracle19:1:1621:POHK1API.hk.standardchartered.com Passed oracle19:1:1621:POHK1API.hk.standardchartered.com Passed oracle19:1:1621:POHK1API.hk.standardchartered.com Passed 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	Actual	OR, any of the select Setting not found Table not found Last Updated:08/04/2	ted values below: 2024 at 06:01:09 PM		YES:YES:BY USER:ALL V	USERS					
SCB_AUDIT_DDL_P- 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.hk.standardchartered.com) Instance oracle19:1:1621:POHK1API.hk.standardchartered.com Passed valuation Date 08/04/2024 at 10:38:34 PM (GMT+0530) Dracle 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		OR, any of the select Setting not found Table not found Last Updated:08/04/2 SCB_AUDIT_DDL_POLICE	ted values below: 2024 at 06:01:09 PM		YES:YES:BY USER:ALL I	USERS					
1.48) 14371 Status of auditing for 'ALTER PACKAGE BODY' statement (Unified Auditing) (oracle19:1:1621:POHK1API.hk.standardchartered.com) Instance oracle19:1:1621:POHK1API.hk.standardchartered.com Passed valuation Date 08/04/2024 at 10:38:34 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	Extended E	OR, any of the select Setting not found Table not found Last Updated:08/04/2 SCB_AUDIT_DDL_POLICE Evidence:	ted values below: 2024 at 06:01:09 PM Y:ALTER PACKAGE:STAN	NDARD ACTION:			ENTITY NAME				
(oracle19:1:1621:POHK1API.hk.standardchartered.com) Instance oracle19:1:1621:POHK1API.hk.standardchartered.com Instance revious Status Passed Invaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530) Instance oracle19:1:1621:POHK1API.hk.standardchartered.com Instance oracle19:1:1621:1621:POHK1API.hk.standardchartered.com Instance oracle19:1:1621:1621:1621:1621:1621:1621:1621:	Extended E	OR, any of the select Setting not found Table not found Last Updated:08/04/2 SCB_AUDIT_DDL_POLICE Evidence: ME AUDIT_OPTION	ted values below: 2024 at 06:01:09 PM Y:ALTER PACKAGE:STAN AUDIT_OPTION_TYPE	NDARD ACTION:	FAILURE	ENABLED_OPTION					
revious Status Passed valuation Date 08/04/2024 at 10:38:34 PM (GMT+0530) Pracle database package bodies, which are stored within the database, are created to perform business functions and cocess database as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring	POLICY_NAM	OR, any of the select Setting not found Table not found Last Updated:08/04/2 SCB_AUDIT_DDL_POLICE Evidence: ME AUDIT_OPTION	ted values below: 2024 at 06:01:09 PM Y:ALTER PACKAGE:STAN AUDIT_OPTION_TYPE	NDARD ACTION:	FAILURE	ENABLED_OPTION					
valuation Date 08/04/2024 at 10:38:34 PM (GMT+0530) Dracle database package bodies, which are stored within the database, are created to perform business functions and codes database as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring	Extended E POLICY_NAM SCB_AUDIT_I OLICY	OR, any of the select Setting not found Table not found Last Updated:08/04/2 SCB_AUDIT_DDL_POLIC Evidence: ME AUDIT_OPTION DDL_P- ALTER PACKAGE	2024 at 06:01:09 PM Y:ALTER PACKAGE:STAN AUDIT_OPTION_TYPE STANDARD ACTION	E SUCCESS YES BODY' statem	FAILURE YES	ENABLED_OPTION BY USER	ALL USERS				
Dracle database package bodies, which are stored within the database, are created to perform business functions and comments are defined by PL/SQL code and SQL statements contained within these objects. Logging and monitoring	Extended E POLICY_NAM SCB_AUDIT_I OLICY	OR, any of the select Setting not found Table not found Last Updated:08/04/2 SCB_AUDIT_DDL_POLIC Evidence: ME AUDIT_OPTION DDL_P- ALTER PACKAGE 1 Status of auditing fo (oracle19:1:1621:PO	AUDIT_OPTION_TYPE STANDARD ACTION r 'ALTER PACKAGE HK1API.hk.standard	E SUCCESS YES BODY' statem chartered.cor	FAILURE YES	ENABLED_OPTION BY USER	ALL USERS				
ccess database as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitorir	Extended E POLICY_NAM SCB_AUDIT_I OLICY 1.48) 14371 astance	OR, any of the select Setting not found Table not found Last Updated:08/04/2 SCB_AUDIT_DDL_POLIC Evidence: ME AUDIT_OPTION DDL_P- ALTER PACKAGE 1 Status of auditing for (oracle19:1:1621:PO oracle19:1:1621:PO	AUDIT_OPTION_TYPE STANDARD ACTION r 'ALTER PACKAGE HK1API.hk.standard	E SUCCESS YES BODY' statem chartered.cor	FAILURE YES	ENABLED_OPTION BY USER	ALL USERS				
ccess database as defined by PL/SQL code and SQL statements contained within these objects. Logging and monitorir	Extended E POLICY_NAM SCB_AUDIT_I OLICY 1.48) 14371 Instance Previous Status	OR, any of the select Setting not found Table not found Last Updated:08/04/2 SCB_AUDIT_DDL_POLIC Evidence: ME AUDIT_OPTION DDL_P- ALTER PACKAGE 1 Status of auditing for (oracle19:1:1621:PO oracle19:1:1621:Fo Passed	AUDIT_OPTION_TYPE STANDARD ACTION r 'ALTER PACKAGE HK1API.hk.standardch	E SUCCESS YES BODY' statem chartered.com	FAILURE YES	ENABLED_OPTION BY USER	ALL USERS				
	Extended E POLICY_NAM SCB_AUDIT_I OLICY 1.48) 14371 Instance Previous Status valuation Dat	OR, any of the select Setting not found Table not found Last Updated:08/04/2 SCB_AUDIT_DDL_POLIC Evidence: ME AUDIT_OPTION DDL_P- ALTER PACKAGE 1 Status of auditing fo (oracle19:1:1621:PO	AUDIT_OPTION_TYPE STANDARD ACTION r 'ALTER PACKAGE HK1API.hk.standard POHK1API.hk.standardch D:38:34 PM (GMT+0530	E SUCCESS YES BODY' statem chartered.com	FAILURE YES nent (Unified Auditi	ENABLED_OPTION BY USER ng) Passe	ALL USERS ed MEDIUN				
	Extended E POLICY_NAM SCB_AUDIT_I OLICY 1.48) 14371 Instance Previous Status valuation Dat Dracle data	OR, any of the select Setting not found Table not found Last Updated:08/04/2 SCB_AUDIT_DDL_POLIC Evidence: ME AUDIT_OPTION DDL_P- ALTER PACKAGE 1 Status of auditing for (oracle19:1:1621:PO oracle19:1:1621:PO oracle19:10:1621:PO	AUDIT_OPTION_TYPE STANDARD ACTION r 'ALTER PACKAGE HK1API.hk.standard POHK1API.hk.standardch D:38:34 PM (GMT+0530) , which are stored v	E SUCCESS YES BODY' statem chartered.com nartered.com	FAILURE YES nent (Unified Auditin)	eNABLED_OPTION BY USER ng) Passe to perform business	ALL USERS ed MEDIUM functions and				
otential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the	Extended E POLICY_NAM SCB_AUDIT_I OLICY 1.48) 14371 Instance revious Status valuation Dat Oracle data ccess data II attempts	OR, any of the select Setting not found Table not found Last Updated:08/04/2 SCB_AUDIT_DDL_POLIC Evidence: ME AUDIT_OPTION DDL_P- ALTER PACKAGE 1 Status of auditing for (oracle19:1:1621:Po	AUDIT_OPTION_TYPE STANDARD ACTION T'ALTER PACKAGE HK1API.hk.standardch D:38:34 PM (GMT+0530) which are stored v L/SQL code and SQ y, whether successf	E SUCCESS YES BODY' statem chartered.com artered.com within the data L statements ul or unsucce	FAILURE YES nent (Unified Auditin) abase, are created contained within the ssful, may provide	enabled_option By user ng) Passe to perform business ese objects. Logging clues and forensic e	ALL USERS ed MEDIU functions and and monitorin vidences abo				

page 463

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.

matches regular expression list

Setting not found
Table not found

.*:ALTER PACKAGE BODY:.*:YES:YES:.*:*
OR, any of the selected values below:

Expected

Oracle_ATOS - 20240806

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_P- ALTER PACKAGE STANDARD ACTION YES BY USER ALL USERS YES OLICY **BODY**

(1.48) 14371 Status of auditing for 'ALTER PACKAGE BODY' statement (Unified Auditing) (oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_TYPE SUCCESS AUDIT_OPTION **FAILURE** ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P- ALTER PACKAGE STANDARD ACTION YES YES BY USER ALL USERS

(1.48) 14371 Status of auditing for 'ALTER PACKAGE BODY' statement (Unified Auditing) Passed MEDIUM (oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

contains color	separ	ated values of policy_	name, audit_option, a	udit_option_type, succ	cess, failure, enabled_	option, and entity_nar	ne.
Expected	matc	hes regular expre	ssion list				
	.*:ALT	ER PACKAGE BODY:.*	:YES:YES:.*:.*				
	OR, a	any of the selected	d values below:				
	Setting not found						
	Ta	ble not found					
Actual	Lact		24 at 06:01:09 PM (CMT - 0530\			
Actual		-		•			
	SCB_A	AUDIT_DDL_POLICY: <i>P</i>	ALTER PACKAGE BODY	Y:STANDARD ACTION:	:YES:YES:BY USER:ALI	L USERS	
Extended E	viden	ce:					
POLICY_NAM	Е	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_D	DL_P-	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:POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 selecte	d values below:					
	Setting not found						
	Table not found						
A	1 1 1 - 1 1 - 0 - 10 - 10 -	04 . (00 04 00 DM	(OMT 0500)				
Actual	Last Updated:08/04/20	024 at 06:01:09 PM	(GMT+0530)				
	SCB_AUDIT_DDL_POLICY	ALTER PACKAGE BOD	Y:STANDARD ACTIO	N:YES:YES:BY USER	ALL USERS		
Extended E	vidence:						
POLICY_NAM	E AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_D OLICY	DL_P- ALTER PACKAGE BODY	STANDARD ACTION	YES	YES	BY USER	ALL USERS	

(1.48) 14371 Status of auditing for 'ALTER PACKAGE BODY' statement (Unified Auditing) (oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Passed MEDIUM

Passed

MEDIUM

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

contains colo	n separa	ated values of policy_	name, audit_option, au	udit_option_type, suc	cess, failure, enabled_	option, and entity_nar	ne.		
Expected	matc	hes regular expre	ssion list						
	.*:ALT	*:ALTER PACKAGE BODY:.*:YES:YES:.*:.*							
	OR, a	any of the selected	d values below:						
	Set	Setting not found							
	Tal	ble not found							
Actual		•	24 at 06:01:09 PM (•	·VEC·VEC·RA I ICED·VI I	IISEDS			
Cytonded C			LIER I NORNOL DOD	1.51711VD/IIIVD NC1101V	TES.TES.DT CSER.MET	COLICO			
Extended E									
POLICY_NAN	1E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_I	DDL_P-	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:POHK1CAT.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_P- 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:POHK1CCD.hk.standardchartered.com)

Passed MEDIUM

Instance oracle 19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_P- ALTER PACKAGE STANDARD ACTION YES YES BY USER ALL USERS
OLICY

(1.48) 14371 Status of auditing for 'ALTER PACKAGE BODY' statement (Unified Auditing) (oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

*• ^	matches regular expression list							
· .A.	LTER PACKAGE BODY:.*:Y	ES:YES:.*:.*						
OR	, any of the selected v	alues below:						
	Setting not found							
	Table not found							
ual Las	t Updated:08/04/2024	at 06:01:09 PM (G	MT+0530)					
SCB	_AUDIT_DDL_POLICY:AL	TER PACKAGE BODY:	STANDARD ACTIO	N:YES:YES:BY USER:ALL I	USERS			
ended Evider	nce:							
ICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPI	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
_AUDIT_DDL_P `Y	- ALTER PACKAGE BODY	STANDARD ACTION	YES	YES	BY USER	ALL USERS		
(1.49) 14372	Status of auditing fo	or 'DROP PROCED HK1API.hk.standa	URE' statement	(Unified Auditing) m)	Passe	ed MEDIU		
Instance	oracle19:1:1621:1	POHK1API.hk.standar	dchartered.com	•				
Previous Status	Passed							
Evaluation Date	e 08/04/2024 at 1	0:38:34 PM (GMT+05	530)					
suspicious/t	nauthorized activities	s. This logging re	quirernent snot					
The following colon separat	List String value(s) of X i ed values of policy name,	ndicates the status of audit option, audit o	the DROP PROCEI	OURE audit option type d ss, failure, enabled option	efined on the database. T n, and entity name.	The output contain		
	List String value(s) of X i ed values of policy_name, matches regular exp		the DROP PROCEI option_type, succes	OURE audit option type d ss, failure, enabled_option	efined on the database. T n, and entity_name.	The output contain		
The following colon separat	List String value(s) of X i ed values of policy_name, matches regular exp .*:DROP PROCEDURE:*:	ression list	the DROP PROCEI pption_type, succes	DURE audit option type d ss, failure, enabled_option	efined on the database. 'I n, and entity_name.	he output contain		
	matches regular exp	ression list YES:YES:.*:.*		DURE audit option type d is, failure, enabled_option	efined on the database. 'I n, and entity_name.	he output contai		
	matches regular exp.*:DROP PROCEDURE.:*:	ression list YES:YES:.*:.*		DURE audit option type d is, failure, enabled_option	efined on the database. 'I n, and entity_name.	he output contai		
	matches regular exp. *:DROP PROCEDURE:.*: OR, any of the select Setting not found	oression list YES:YES:.*:.* ted values below:		DURE audit option type d ss, failure, enabled_option	efined on the database. 'I n, and entity_name.	he output contai		
Expected	matches regular exp. *:DROP PROCEDURE.:*: OR, any of the selectory Setting not found Table not found Last Updated:08/04/	oression list YES:YES:.*:.* ted values below: 2024 at 06:01:09 P	M (GMT+0530)	DURE audit option type d is, failure, enabled_option DN:YES:YES:BY USER:ALL		he output contai		
Expected	matches regular exp. *:DROP PROCEDURE:.*: OR, any of the select Setting not found Table not found Last Updated:08/04/ SCB_AUDIT_DDL_POLICE	oression list YES:YES:.*:.* ted values below: 2024 at 06:01:09 P	M (GMT+0530)			he output contain		
Expected Actual	matches regular exp. *:DROP PROCEDURE:.*: OR, any of the selectory Setting not found Table not found Last Updated:08/04/ SCB_AUDIT_DDL_POLICY vidence:	oression list YES:YES:.*:.* ted values below: 2024 at 06:01:09 P	M (GMT+0530) ::STANDARD ACTIO					
Actual Extended E POLICY_NAM	matches regular exp. *:DROP PROCEDURE:.*: OR, any of the select Setting not found Table not found Last Updated:08/04/ SCB_AUDIT_DDL_POLICY vidence:	vession list YES:YES:.*:.* ted values below: 2024 at 06:01:09 P CY:DROP PROCEDURE AUDIT_OPTION_T	M (GMT+0530) ESTANDARD ACTION	DN:YES:YES:BY USER:ALL	USERS			
Actual Extended E POLICY_NAM SCB_AUDIT_I OLICY	matches regular exp. *:DROP PROCEDURE:.*: OR, any of the select Setting not found Table not found Last Updated:08/04/ SCB_AUDIT_DDL_POLICY vidence: E AUDIT_OPTION	pression list YES:YES:.*:.* ted values below: 2024 at 06:01:09 P CY:DROP PROCEDURE AUDIT_OPTION_T RE STANDARD ACTION OF 'DROP PROCED	M (GMT+0530) ESTANDARD ACTION YPE SUCCESS ON YES URE' statement	DN:YES:YES:BY USER:ALL FAILURE YES (Unified Auditing)	USERS ENABLED_OPTION	ENTITY_NAME ALL USERS		
Actual Extended E POLICY_NAM SCB_AUDIT_I OLICY	matches regular exp*:DROP PROCEDURE*: OR, any of the select Setting not found Table not found Last Updated:08/04/ SCB_AUDIT_DDL_POLICY VIDENTIAL OPTION DDL_P-DROP PROCEDURE Status of auditing for (oracle19:1:1621:PO	pression list YES:YES:.*:.* ted values below: 2024 at 06:01:09 P CY:DROP PROCEDURE AUDIT_OPTION_T RE STANDARD ACTION OF 'DROP PROCED	M (GMT+0530) AMESTANDARD ACTION APPE SUCCESS ON YES URE' statement lardchartered.com	DN:YES:YES:BY USER:ALL FAILURE YES (Unified Auditing)	USERS ENABLED_OPTION BY USER	ENTITY_NAME ALL USERS		
Actual Extended E POLICY_NAM SCB_AUDIT_I OLICY (1.49) 14372	matches regular exp. *:DROP PROCEDURE:.*: OR, any of the select Setting not found Table not found Last Updated:08/04/ SCB_AUDIT_DDL_POLICY vidence: E AUDIT_OPTION DDL_P- DROP PROCEDURE Status of auditing for (oracle19:1:1621:190) oracle19:1:1621:190 Passed	pression list YES:YES:.*:.* ted values below: 2024 at 06:01:09 P CY:DROP PROCEDURE AUDIT_OPTION_T RE STANDARD ACTION OF 'DROP PROCED OHK3CCD.hk.stand	CM (GMT+0530) C:STANDARD ACTION TYPE SUCCESS ON YES URE' statement dardchartered.com	DN:YES:YES:BY USER:ALL FAILURE YES (Unified Auditing)	USERS ENABLED_OPTION BY USER	ENTITY_NAME ALL USERS		

(1.49) 14372 Status of auditing for 'DROP PROCEDURE' statement (Unified Auditing) (oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

•	1 3- 1 -1 -31							
Expected	matc	hes regular expres	ssion list					
	.*:DRC	OP PROCEDURE:.*:YES	:YES:.*:.*					
	OR, a	any of the selected	I values below:					
	Set	ting not found						
	Ta	ble not found						
Actual	Lact	Undated:09/04/201	04 at 06:01:00 DM (CMT - 0530\				
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)							
	SCB_A	AUDIT_DDL_POLICY:E	ROP PROCEDURE:ST.	ANDARD ACTION:YES	:YES:BY USER:ALL US	RS		
Extended E	viden	ce:						
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_D OLICY	DL_P-	DROP PROCEDURE	STANDARD ACTION	YES	YES	BY USER	ALL USERS	

(1.49) 14372 Status of auditing for 'DROP PROCEDURE' statement (Unified Auditing) (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 10:38:34 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.

coloii separate	eu vaiu	es of policy_name, au	uit_option, audit_option	on_type, success, rand	ire, enabieu_option, ai	iu entity_name.	
Expected	matc	hes regular expre	ssion list				
	.*:DROP PROCEDURE:.*:YES:YES:.*:.*						
	OR, any of the selected values below:						
	Set	ting not found					
	Tal	ole not found					
				(0117 0500)			
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM (GM1+0530)			
	SCB_A	AUDIT_DDL_POLICY:I	DROP PROCEDURE:ST.	ANDARD ACTION:YES	:YES:BY USER:ALL US	ERS	
Extended E	Extended Evidence:						
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_D OLICY	DL_P-	DROP PROCEDURE	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.49) 14372 Status of auditing for 'DROP PROCEDURE' statement (Unified Auditing)(oracle19:1:1621: **MEDIUM** Passed POHK4CCD.hk.standardchartered.com)

oracle19:1:1621:POHK4CCD.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 expr	ession list					
	.*:DROP PROCEDURE:.*:YI	.*:DROP PROCEDURE*:YES:YES:.*:.*					
	OR, any of the selected values below:						
	Setting not found						
	Table not found						
Actual	Last Updated:08/04/20	124 at 06:01:00 PM	(GMT±0530)				
Actual	SCB_AUDIT_DDL_POLICY		•	C-VEC-RV HSER-ALL HS	FDS		
	3CD_AODI1_DDL_1 OLIC1	DROI TROCEDORE.31	ANDARD ACTION.TEC	J. IEJ.DI UJEK.ALL UJ	EKO		
Extended E	vidence:						
POLICY_NAM	E AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_D OLICY	DDL_P- DROP PROCEDURE	STANDARD ACTION	YES	YES	BY USER	ALL USERS	

(1.49) 14372 Status of auditing for 'DROP PROCEDURE' statement (Unified Auditing) (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

STANDARD ACTION YES

(oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Passed MEDIUM

oracle19:1:1621:POHK1CAT.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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: FAILURE** POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS ENABLED_OPTION ENTITY_NAME

(1.49) 14372 Status of auditing for 'DROP PROCEDURE' statement (Unified Auditing) **Passed**

YES

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

OLICY

SCB_AUDIT_DDL_P- DROP PROCEDURE

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

Oracle database procedures, which are stored within the database, are created to perform business functions and access

Oracle_ATOS - 20240806 page 469

MEDIUM

ALL USERS

BY USER

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							
	.*:DRC	OP PROCEDURE:.*:YES	:YES:.*:.*					
	OR, a	any of the selected	l values below:					
	Set	ting not found						
	Tal	ole not found						
Actual	1	l la data d.00/04/00	04 -4 0C-04-00 DM /	OMT - 0520\				
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM (GIVI I +0530)				
	SCB_A	SCB_AUDIT_DDL_POLICY:DROP PROCEDURE:STANDARD ACTION:YES:YES:BY USER:ALL USERS						
Extended E	idone	201						
Extended	videnc	e.						
POLICY_NAM	Е	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_D	DL_P-	DROP PROCEDURE	STANDARD ACTION	YES	YES	BY USER	ALL USERS	

(1.49) 14372 Status of auditing for 'DROP PROCEDURE' statement (Unified Auditing) (oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

colon separated values of policy_name, audit_option_type, success, failure, enabled_option, and entity_name.							
Expected	matches regular expression list						
	.*:DR0	OP PROCEDURE:.*:YES	S:YES:.*:.*				
	OR, a	any of the selected	d values below:				
	Setting not found						
	Ta	ble not found					
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM (GMT+0530)			
	SCB_A	AUDIT_DDL_POLICY:I	DROP PROCEDURE:ST.	ANDARD ACTION:YE	S:YES:BY USER:ALL US	SERS	
Extended E	Eviden	ce:					
POLICY_NAM	1E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_I OLICY	DDL_P-	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: Passed MEDIUM POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

colon separati	ed values of policy_name, addit_option, addit_option_type, success, famare, enabled_option, and enaty_name.
Expected	matches regular expression list
	.*:DROP FUNCTION:.*:YES:YES:.*:.*

	OR, any of the selected values below:						
	Setting not found						
	Tal	ble not found					
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)						
	SCB_A	AUDIT_DDL_POLICY:I	ROP FUNCTION:STAN	NDARD ACTION:YES:Y	ES:BY USER:ALL USE	RS	
Extended Ex	/iden	ce:					
POLICY_NAMI	3	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_D OLICY	DL_P-	DROP FUNCTION	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.50) 14373 Status of auditing for 'DROP FUNCTION' statement (Unified Auditing)(oracle19:1:1621: **MEDIUM Passed** POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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

coloii separate	cu vaiu	es of policy_name, au	dit_option, addit_option	on_type, success, rand	ire, enabieu_option, ai	iu entity_name.	
Expected	matc	hes regular expre	ssion list				
	.*:DROP FUNCTION:.*:YES:YES:.*:*						
	OR, any of the selected values below:						
	Set	ting not found					
	Tal	ole not found					
				(0117 0500)			
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM (GM I +0530)			
	SCB_A	AUDIT_DDL_POLICY:I	DROP FUNCTION:STAN	NDARD ACTION:YES:Y	ES:BY USER:ALL USE	RS	
Extended E	vidend	e:					
POLICY_NAM	Е	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_D OLICY	DL_P-	DROP FUNCTION	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.50) 14373 Status of auditing for 'DROP FUNCTION' statement (Unified Auditing)(oracle19:1:1621: Passed **MEDIUM** POHK5CCD.hk.standardchartered.com)

oracle19:1:1621:POHK5CCD.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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 separat	ed 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 E	vidence:

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

(1.50) 14373 Status of auditing for 'DROP FUNCTION' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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							
	.*:DRC	OP FUNCTION:.*:YES:Y	'ES:.*:.*					
	OR, a	any of the selected	d values below:					
	Set	ting not found						
	Tal	ble not found						
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM (GMT+0530)				
	SCB_A	AUDIT_DDL_POLICY:I	DROP FUNCTION:STAN	NDARD ACTION:YES:Y	ES:BY USER:ALL USEF	RS		
Extended E	Extended Evidence:							
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_D	DL_P-	DROP FUNCTION	STANDARD ACTION	YES	YES	BY USER	ALL USERS	

(1.50) 14373 Status of auditing for 'DROP FUNCTION' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

colon separate	ed values of policy_name, a	udit_option, audit_optic	on_type, success, rai	iure, enabled_optio	n, and entity_name.			
Expected	matches regular expre	ession list						
	.*:DROP FUNCTION:.*:YES	YES:.*:.*						
	OR, any of the selecte	d values below:						
	Setting not found							
	Table not found							
Actual	Last Updated:08/04/20							
	SCB_AUDIT_DDL_POLICY	DROP FUNCTION:STAN	NDARD ACTION:YES	YES:BY USER:ALL U	JSERS			
Extended E	Extended Evidence:							
POLICY_NAM	E AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB AUDIT D	DL P- DROP FUNCTION	STANDARD ACTION	YFS	YFS	BY LISER	ALL HSFRS		

(1.50) 14373 Status of auditing for 'DROP FUNCTION' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

OLICY

Evaluation Date 08/04/2024 at 10:38:34 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 Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) Actual 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_P- DROP FUNCTION STANDARD ACTION YES YES BY USER **ALL USERS**

(1.50) 14373 Status of auditing for 'DROP FUNCTION' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

OLICY

Evaluation Date 08/04/2024 at 10:38:34 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:** AUDIT_OPTION_TYPE SUCCESS ENABLED_OPTION ENTITY_NAME POLICY_NAME AUDIT_OPTION **FAILURE** STANDARD ACTION YES ALL USERS SCB_AUDIT_DDL_P- DROP FUNCTION YES BY USER

(1.50) 14373 Status of auditing for 'DROP FUNCTION' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

Actual Last SCB Extended Eviden POLICY_NAME SCB_AUDIT_DDL_P-OLICY 1.51) 14374 State POH Instance Previous Status Evaluation Date Dracle database Estatabase as definattempts to drop is suspicious/unautl The following List S separated values of Expected mate Expected mate Scalar Scala	AUDIT_DDL_POLICY nce: AUDIT_OPTION - DROP FUNCTION tus of auditing for HK1API.hk.standar oracle19:1:1621:PC Passed 08/04/2024 at 10: packages, which ned by PL/SQL copackage, whether horized activities. String value(s) of X incorpolicy_name, audit_ocches regular expressions.	AUDIT_OPTION_TYPE STANDARD ACTION "DROP PACKAGE" STANDARD ACTION "DROP PACKAGE" OHK1API.hk.standardch Sas:34 PM (GMT+0530) are stored within the ode and SQL states of successful or unsubstitution. This logging required icates the status of the option, audit_option_typession list YES.*:.*	SUCCESS YES statement (U artered.com ne database ments contai uccessful, m rement shou	FAILURE YES nified Auditing)(oral , are created to period within these contay provide clues and all the set as approximately approximately approximately approximately and the set as approximately a	ENABLED_OPTION BY USER	ALL USERS sed MEDIUM tions and access monitoring of all es about potential of the business.						
Actual Last SCB_ Extended Evident POLICY_NAME SCB_AUDIT_DDL_P- OLICY 1.51) 14374 State POH Instance Previous Status Evaluation Date Dracle database Elatabase as definattempts to drop guspicious/unautl The following List Separated values of Expected mate *:DR OR, SG TA Actual Last SCB_	etting not found fable not found t Updated:08/04/20 AUDIT_DDL_POLICY nce: AUDIT_OPTION - DROP FUNCTION tus of auditing for HK1API.hk.standal oracle19:1:1621:PO Passed 08/04/2024 at 10: packages, which ned by PL/SQL co package, whethe horized activities. String value(s) of X inc policy_name, audit_outches regular expressions. Compackage: *YES:Yese any of the selected.	AUDIT_OPTION_TYPE STANDARD ACTION 'DROP PACKAGE': rdchartered.com) DHK1API.hk.standardch are stored within the de and SQL statel or successful or unsertion. This logging requi- dicates the status of the option, audit_option_type ession list YES.*:.*	SUCCESS YES statement (U artered.com ne database ments contai uccessful, m rement shou	FAILURE YES nified Auditing)(oral , are created to period within these contay provide clues and all the set as approximately approximately approximately approximately and the set as approximately a	erform business functobjects. Logging and and forensic evidence opriate to the needs of	ALL USERS sed MEDIUM tions and access monitoring of all es about potential of the business.						
Actual Lasi SCB Extended Eviden POLICY_NAME SCB_AUDIT_DDL_P-OLICY 1.51) 14374 State POH Instance Previous Status Ivaluation Date Dracle database Idatabase as define Interpret to drop Isuspicious/unautl The following List S Isseparated values of Expected Mateurical Corp. In Scalar	t Updated:08/04/20 _AUDIT_DDL_POLICY nce: AUDIT_OPTION - DROP FUNCTION tus of auditing for HK1API.hk.standa oracle19:1:1621:PO Passed 08/04/2024 at 10: packages, which ned by PL/SQL co package, whethe horized activities. String value(s) of X inc policy_name, audit_o ches regular expression any of the selected	AUDIT_OPTION_TYPE STANDARD ACTION 'DROP PACKAGE' rdchartered.com) OHK1API.hk.standardch are stored within the ode and SQL state of successful or unsubstantial to the status of the option, audit_option_type ession list YES.*:.*	SUCCESS YES statement (U artered.com ne database ments contai uccessful, m rement shou	FAILURE YES nified Auditing)(oral , are created to period within these contay provide clues and all the set as approximately approximately approximately approximately and the set as approximately a	erform business functobjects. Logging and and forensic evidence opriate to the needs of	ALL USERS sed MEDIUM tions and access monitoring of all es about potential of the business.						
Extended Eviden POLICY_NAME SCB_AUDIT_DDL_P- OLICY 1.51) 14374 State POH Instance Previous Status Evaluation Date Dracle database database as define attempts to drop suspicious/unautl The following List S separated values of Expected mate -*:DR OR, Sc OR, SCB_ CCB_ CCB_CCC CCC CCC CCC CCC	AUDIT_DDL_POLICY nce: AUDIT_OPTION DROP FUNCTION tus of auditing for HK1API.hk.standa oracle19:1:1621:PC Passed 08/04/2024 at 10: packages, which ned by PL/SQL copackage, whether horized activities. String value(s) of X incopolicy_name, audit_oracle. Compackage: Compack	AUDIT_OPTION_TYPE STANDARD ACTION 'DROP PACKAGE' rdchartered.com) OHK1API.hk.standardch are stored within the ode and SQL state of successful or unsubstantial to the status of the option, audit_option_type ession list YES.*:.*	SUCCESS YES statement (U artered.com ne database ments contai uccessful, m rement shou	FAILURE YES nified Auditing)(oral , are created to period within these contay provide clues and all the set as approximately approximately approximately approximately and the set as approximately a	erform business functobjects. Logging and and forensic evidence opriate to the needs of	ALL USERS sed MEDIUM tions and access monitoring of all es about potential of the business.						
Extended Evident POLICY_NAME SCB_AUDIT_DDL_POLICY 1.51) 14374 State POHOLICY 1.51) 14374 States Poholicy Status Evaluation Date Dracle database as define attempts to drop suspicious/unaution Separated values of Expected Materials Policy	AUDIT_OPTION DROP FUNCTION tus of auditing for HK1API.hk.standar oracle19:1:1621:PC Passed 08/04/2024 at 10: packages, which ned by PL/SQL corpackage, whether horized activities. String value(s) of X incorpolicy_name, audit_oracles. Ches regular expression of the selected activities.	AUDIT_OPTION_TYPE STANDARD ACTION 'DROP PACKAGE': rdchartered.com) DHK1API.hk.standardch as 38:34 PM (GMT+0530) are stored within the ode and SQL states of successful or unser successf	success YES statement (U artered.com ne database ments contai uccessful, m rement shou	FAILURE YES nified Auditing)(oral , are created to period within these contay provide clues and all the set as approximately approximately approximately approximately and the set as approximately a	erform business functobjects. Logging and and forensic evidence opriate to the needs of	ALL USERS sed MEDIUM tions and access monitoring of all es about potential of the business.						
POLICY_NAME SCB_AUDIT_DDL_P-OLICY 1.51) 14374 State POHENISTANCE Previous Status valuation Date Dracle database latabase as definatempts to drop grace suspicious/unautly The following List Separated values of Expected mate *:DR OR, ScB_ SCB_ SCB_ SCB_ SCB_ SCB_ SCB_ SCB_ SC	AUDIT_OPTION DROP FUNCTION tus of auditing for HK1API.hk.standar oracle19:1:1621:PC Passed 08/04/2024 at 10: packages, which ned by PL/SQL corpackage, whether horized activities. String value(s) of X incorpolicy_name, audit_oracles. Ches regular expression of the selected and possible to the selected	"DROP PACKAGE's rdchartered.com" DHK1API.hk.standardch 38:34 PM (GMT+0530) are stored within the ode and SQL state or successful or unsignature of the option, audit_option_typession list YES:.*:.*	statement (U artered.com ne database nents contai uccessful, m	nified Auditing)(oral, are created to perined within these chay provide clues and the set as approximately approximately and the set as approximately a	BY USER acle19:1:1621: Pass erform business funct objects. Logging and and forensic evidence opriate to the needs of	ALL USERS sed MEDIUM tions and access monitoring of all es about potential of the business.						
SCB_AUDIT_DDL_POLICY 1.51) 14374 State POP Instance Previous Status Invaluation Date Dracle database Itatabase as definite mpts to drop Itatabase as definite mpts to drop Itatabase Ita	tus of auditing for HK1API.hk.standar oracle19:1:1621:PC Passed 08/04/2024 at 10: packages, which ned by PL/SQL copackage, whether horized activities. String value(s) of X incopolicy_name, audit_ocches regular expressor	"DROP PACKAGE's rdchartered.com" DHK1API.hk.standardch 38:34 PM (GMT+0530) are stored within the ode and SQL state or successful or unsignature of the option, audit_option_typession list YES:.*:.*	statement (U artered.com ne database nents contai uccessful, m	nified Auditing)(oral, are created to perined within these chay provide clues and the set as approximately approximately and the set as approximately a	BY USER acle19:1:1621: Pass erform business funct objects. Logging and and forensic evidence opriate to the needs of	ALL USERS sed MEDIUM tions and access monitoring of all es about potential of the business.						
OLICY 1.51) 14374 State POP Instance Previous Status valuation Date Oracle database latabase as definitempts to drop suspicious/unauti The following List S separated values of Expected Expected OR, SG TA Actual Last SCB	tus of auditing for HK1API.hk.standal oracle19:1:1621:PC Passed 08/04/2024 at 10: packages, which ned by PL/SQL copackage, whethe horized activities. String value(s) of X incopolicy_name, audit_ocches regular expressor	'DROP PACKAGE' a rdchartered.com) OHK1API.hk.standardch 38:34 PM (GMT+0530) are stored within the ode and SQL states of successful or unstances. This logging requidicates the status of the option, audit_option_typession list YES:*:*	artered.com ne database ments contai uccessful, m	nified Auditing)(ora , are created to pe ined within these c nay provide clues a ald be set as appro	erform business funct objects. Logging and and forensic evidence opriate to the needs of	sed MEDIUM tions and access monitoring of all es about potential of the business.						
pol- nstance revious Status valuation Date Dracle database latabase as defir ttempts to drop juspicious/unautl The following List S separated values of Expected mat *:DR OR, Se Ta Actual Last SCB_	Passed 08/04/2024 at 10: packages, which ned by PL/SQL co package, whethe horized activities. String value(s) of X inc policy_name, audit_o ches regular expressory any of the selected	rdchartered.com) DHK1API.hk.standardch 38:34 PM (GMT+0530) are stored within the ode and SQL states of successful or unstantion. This logging requidicates the status of the option, audit_option_typession list YES.*:.*	artered.com ne database ments contai uccessful, m rement shou	, are created to pe ined within these c nay provide clues a ıld be set as appro	erform business funct objects. Logging and and forensic evidence opriate to the needs o	tions and access monitoring of all es about potential of the business.						
Previous Status Evaluation Date Dracle database as definatempts to drop suspicious/unautly The following List Separated values of the tempts to drop suspicious and the tempts	Passed 08/04/2024 at 10: packages, which ned by PL/SQL co package, whethe horized activities. String value(s) of X inc policy_name, audit_o ches regular expri- ROP PACKAGE::*:YES:Y	are stored within the code and SQL states or successful or unstantial This logging requidicates the status of the option, audit_option_typession list	ne database ments contai uccessful, m rement shou	ined within these on ay provide clues a Ild be set as appro	objects. Logging and and forensic evidence options to the needs of the	monitoring of all es about potential of the business.						
Dracle database latabase as definitempts to drop suspicious/unaut. The following List S separated values of Expected mate.*:DR OR, Separated Last Actual Last SCB_	packages, which ned by PL/SQL copackage, whethe horized activities. String value(s) of X incopolicy_name, audit_outches regular expressor PACKAGE:.*:YES:Yeany of the selected.	are stored within the ode and SQL states of successful or unstantial This logging requidicates the status of the option, audit_option_typession list	ne database ments contai uccessful, m rement shou	ined within these on ay provide clues a Ild be set as appro	objects. Logging and and forensic evidence options to the needs of the	monitoring of all es about potential of the business.						
Dracle database latabase as definitempts to drop suspicious/unaution. The following List S separated values of Expected mateurical	packages, which ned by PL/SQL copackage, whethe horized activities. String value(s) of X incopolicy_name, audit_ocches regular expressor PACKAGE:.*:YES:Yeany of the selecter.	are stored within the ode and SQL states of successful or unstantial This logging requidicates the status of the option, audit_option_typession list	ne database ments contai uccessful, m rement shou	ined within these on ay provide clues a Ild be set as appro	objects. Logging and and forensic evidence options to the needs of the	monitoring of all es about potential of the business.						
database as definatempts to drop guspicious/unautl The following List S separated values of Expected mate .*:DR OR, Separated Last SCB_	ned by PL/SQL copackage, whethe horized activities. String value(s) of X incopolicy_name, audit_ocches regular expressor PACKAGE: *: YES: Yearn of the selected.	ode and SQL stated or successful or unsolution. This logging requi- dicates the status of the option, audit_option_typession list YES:.*:.*	ments contai uccessful, m rement shou	ined within these on ay provide clues a Ild be set as appro	objects. Logging and and forensic evidence options to the needs of the	monitoring of all es about potential of the business.						
.*:DR OR, SG Ta Actual Last SCB_	ROP PACKAGE:.*:YES:Y any of the selecte	YES:.*:.*										
OR, Se Ta Actual Last SCB_	any of the selecte			*DPOP PACKACE * YES YES * * *								
Actual Last	•	ed values below.	.*:DROP PACKAGE:.*:YES:YES:*:.* OR any of the selected values below:									
Actual Last SCB_	ctting not round	OR, any of the selected values below: Setting not found										
SCB_	Table not found											
	t Updated:08/04/20	024 at 06:01:09 PM (GMT+0530)									
Extended Eviden	_AUDIT_DDL_POLICY	:DROP PACKAGE:STAN	DARD ACTION:	YES:YES:BY USER:ALL	USERS							
	nce:											
POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	N ENTITY_NAME						
SCB_AUDIT_DDL_P- OLICY	– DROP PACKAGE	STANDARD ACTION	YES	YES	BY USER	ALL USERS						
1.51) 14374 Stat POI	tus of auditing for HK3CCD.hk.standa	'DROP PACKAGE' : ardchartered.com)	statement (U	nified Auditing)(ora	acle19:1:1621: Pass	sed MEDIUM						
nstance		OHK3CCD.hk.standardc	nartered.com									
revious Status	Passed	-20-24 DM (CMT, 0520)										
valuation Date	U8/U4/ZUZ4 at 10:	:38:34 PM (GMT+0530)	1									
					erform business funct objects. Logging and							

Oracle_ATOS - 20240806 page 474

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.

matches regular expression list

OR, any of the selected values below:

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

Setting not found
Table not found

Expected

Actual	Last Opualed.00/04/2024 at 00.01.03 F W (GW1+0330)									
	SCB_AUDIT_DDL_POLICY:DROP PACKAGE:STANDARD ACTION:YES:YES:BY USER:ALL USERS									
Extended Ev	Extended Evidence:									
POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME				
SCB_AUDIT_DI	DL_P- DROP PACKAGE	STANDARD ACTION	YES	YES	BY USER	ALL USERS				

(1.51) 14374 Status of auditing for 'DROP PACKAGE' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Loct Undeted-09/04/2024 at 06:04:00 PM (CMT: 0520)

Previous Status Passed

A atual

Evaluation Date 08/04/2024 at 10:38:34 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, a	any of the selected	I values below:						
	Set	ting not found							
	Table not found								
A . 4 1				OMT OFOO					
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM (GM I +0530)					
	SCB_A	AUDIT_DDL_POLICY:D	ROP PACKAGE:STANI	DARD ACTION:YES:YE	S:BY USER:ALL USERS)			
Extended E	vidon	201							
Extended	viden	.e.							
POLICY_NAM	ΙE	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_I OLICY	DL_P-	DROP PACKAGE	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.51) 14374 Status of auditing for 'DROP PACKAGE' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

separated valu	es of p	oolicy_name, audit_o _l	ption, audit_option_typ	e, success, fail	ure, enabled_option, and e	ntity_name.		
Expected	matc	hes regular expre	ession list					
	.*:DRC	OP PACKAGE:.*:YES:Y	ES:.*:.*					
	OR, a	any of the selecte	d values below:					
	Setting not found							
	Tal	ble not found						
A . 4 1		11. 1.4. 1.00/04/00	04 - 1 00 04 00 DH	(OMT 0500)				
Actual	Last	Updated:08/04/20	24 at 06:01:09 PM ((GIVI I +0530)				
	SCB_A	AUDIT_DDL_POLICY:	DROP PACKAGE:STANI	DARD ACTION:	YES:YES:BY USER:ALL USE	RS		
Extended Evidence:								
POLICY_NAMI	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_D OLICY	DL_P-	DROP PACKAGE	STANDARD ACTION	YES	YES	BY USER	ALL USERS	

(1.51) 14374 Status of auditing for 'DROP PACKAGE' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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									
		Tal	ole not found								
	A = 41	1	l ll - (l. 00/04/00/	0.4 =4.00-04-00 DM	(OMT - 0500)						
4	Actual	Last	Updated:08/04/202	24 at 06:01:09 PM (GW1+0530)						
		SCB_A	AUDIT_DDL_POLICY:I	DROP PACKAGE:STANI	DARD ACTION:YES:YE	S:BY USER:ALL USERS)				
	Extended Evidence:										
	POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
	SCB_AUDIT_D OLICY	DL_P-	DROP PACKAGE	STANDARD ACTION	YES	YES	BY USER	ALL USERS			

(1.51) 14374 Status of auditing for 'DROP PACKAGE' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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: FAILURE** POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS ENTITY_NAME ENABLED_OPTION

(1.51) 14374 Status of auditing for 'DROP PACKAGE' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CCD.hk.standardchartered.com)

YES

BY USER

ALL USERS

STANDARD ACTION YES

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

OLICY

SCB_AUDIT_DDL_P- DROP PACKAGE

Evaluation Date 08/04/2024 at 10:38:34 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										
	.*:DRC	.*:DROP PACKAGE:.*:YES:YES:.*:.*									
	OR, a	any of the selected	d values below:								
	Setting not found										
	Table not found										
				(OLIT OFOS)							
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM ((GMT+0530)							
	SCB_A	AUDIT_DDL_POLICY:I	DROP PACKAGE:STANI	DARD ACTION:YES:YE	S:BY USER:ALL USERS)					
Extended E	Extended Evidence:										
POLICY_NAM	ΙE	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME				
SCB_AUDIT_I	DDL_P-	DROP PACKAGE	STANDARD ACTION	YES	YES	BY USER	ALL USERS				

(1.51) 14374 Status of auditing for 'DROP PACKAGE' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 n	ot found							
	Table not found								
Δctual	Last Unda	ted:08/04/20	024 at 06:01:09 PM ((GMT±0530)					
Actual			024 at 06:01:09 PM (':DROP PACKAGE:STANI		ES:YES:BY USER:ALL I	USERS			
	SCB_AUDIT_		024 at 06:01:09 PM (CDROP PACKAGE:STAN)		ES:YES:BY USER:ALL U	USERS			
Actual Extended E	SCB_AUDIT_ Evidence:	_DDL_POLICY	:DROP PACKAGE:STANI	DARD ACTION:Y			ENITITY NAME		
Extended E	SCB_AUDIT_ Evidence:	_DDL_POLICY T_OPTION		DARD ACTION:Y	ES:YES:BY USER:ALL U FAILURE YES	USERS ENABLED_OPTION BY USER	ENTITY_NAME ALL USERS		

(1.52) 14375 Status of auditing for 'DROP PACKAGE BODY' statement (Unified Auditing) Passed MEDIUM (oracle19:1:1621:POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	d values below:				
	Setting not found					
	Table not found					
Actual	Last Updated:08/04/20	24 at 06:01:09 PM (GMT+0530)			
	SCB_AUDIT_DDL_POLICY:	DROP PACKAGE BODY:	:STANDARD ACTION:	YES:YES:BY USER:ALL	USERS	
Extended E	vidence:					
POLICY_NAM	E AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
	DL_P- DROP PACKAGE BODY	STANDARD ACTION	YES	YES	BY USER	ALL USERS
(1.52) 14375	Status of auditing for ' (oracle19:1:1621:POHI	DROP PACKAGE B K4CCD.hk.standard	BODY' statement (I Ichartered.com)	Unified Auditing)	Passe	ed MEDIUM
Instance	oracle19:1:1621:PO	HK4CCD.hk.standardch	nartered.com			
Previous Status	Passed					
Evaluation Date	e 08/04/2024 at 10:3	38:34 PM (GMT+0530)				
access datal	pase package bodies, voase as defined by PL/sto drop package body, spicious/unauthorized a	SQL code and SQL whether successfu	statements conta ul or unsuccessfu	ained within these I, may provide clu	objects. Logging a es and forensic e	and monitoring of vidences about

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									
Astual	1+	l los al a tra al 200/04/200	14 -4 0C-04-00 DM (OMT - 0520\						
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 Ev	Extended Evidence:									
POLICY_NAME	3	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCB_AUDIT_DIOLICY		DROP PACKAGE BODY	STANDARD ACTION	YES	YES	BY USER	ALL USERS			

(1.52) 14375 Status of auditing for 'DROP PACKAGE BODY' statement (Unified Auditing) Passed MEDIUM (oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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, type, success, failure, enabled_option, and entity_name.

colon separate	varies of policy_name, addit_option_type, success, failure, chabled_option, and chitty_name.							
Expected	matches regular expression list							
	.*DROP PACKAGE BODY:.*:YES:YES:.*:*							
	OR, any of the selected values below:							
	Setting not found							
	Table not found							

Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) Actual SCB AUDIT DDL POLICY:DROP PACKAGE BODY:STANDARD ACTION:YES:YES:BY USER:ALL USERS **Extended Evidence:** POLICY_NAME AUDIT_OPTION_TYPE SUCCESS AUDIT_OPTION **FAILURE** ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P- DROP PACKAGE STANDARD ACTION YES BY USER YES ALL USERS OLICY **BODY**

(1.52) 14375 Status of auditing for 'DROP PACKAGE BODY' statement (Unified Auditing) (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 10:38:34 PM (GMT+0530)

Expected matches regular expression list

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.

	.*DROP PACKAGE BODY:.*:	YES:YES:.*:.*						
	OR, any of the selected	d values below:						
	Setting not found							
	Table not found							
Actual	Last Updated:08/04/202	24 at 06:01:09 PM /	(CMT+0530)					
			•					
	SCB_AUDIT_DDL_POLICY:I	DROP PACKAGE BODY	:STANDARD ACTION:	YES:YES:BY USER:ALL	USERS			
Extended Ev	idence:							
POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_DE	DL_P- DROP PACKAGE BODY	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.52) 14375 Status of auditing for 'DROP PACKAGE BODY' statement (Unified Auditing) Passed MEDIUM (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	mato	hes regular expre	ssion list						
	.*DRC	P PACKAGE BODY:.*:	/ES:YES:.*:.*						
	OR, any of the selected values below:								
	Setting not found								
	Ta	ble not found							
A = 1=1	1		04 -4 00-04-00 DM	(OMT : 0500)					
Actual	Last	Updated:08/04/202	24 at 06:01:09 PW ((GIVI I +0530)					
	SCB_A	AUDIT_DDL_POLICY:I	ROP PACKAGE BODY	:STANDARD ACTION:	YES:YES:BY USER:ALL	USERS			
Extended E	vidon	20.							
Extended E	videii	Je.							
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_D OLICY	DL_P-	DROP PACKAGE BODY	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.52) 14375 Status of auditing for 'DROP PACKAGE BODY' statement (Unified Auditing) (oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	matc	hes regular expres	ssion list					
	.*DRO	P PACKAGE BODY:.*:Y	/ES:YES:.*:.*					
	OR, any of the selected values below:							
Setting not found								
	Tal	ole not found						
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM (GMT+0530)				
	SCB_AUDIT_DDL_POLICY:DROP PACKAGE BODY:STANDARD ACTION:YES:YES:BY USER:ALL USERS							
Extended Ev	/idenc	e:						
POLICY_NAMI	3	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_D: OLICY		DROP PACKAGE BODY	STANDARD ACTION	YES	YES	BY USER	ALL USERS	

(1.52) 14375 Status of auditing for 'DROP PACKAGE BODY' statement (Unified Auditing) (oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

Passed MEDIUM

Passed

MEDIUM

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

colon separated values of policy_name, addit_option, addit_option_type, success, failure, enabled_option, and enuty_name.									
Expected	matc	hes regular expre	ssion list						
	.*DRO	P PACKAGE BODY:.*:	YES:YES:.*:.*						
	OR, a	any of the selected	d values below:						
	Set	Setting not found							
	Table not found								
Astual	1	Un dete de00/04/20	04 -4 0C-04-00 DM /	CMT - 0520)					
Actual	Last	Updated:08/04/20/	24 at 06:01:09 PM (GIVI I +0530)					
	SCB_A	AUDIT_DDL_POLICY:I	OROP PACKAGE BODY	STANDARD ACTION:	YES:YES:BY USER:ALL	USERS			
Extended E	videnc	ce:							
POLICY_NAM	ſΕ	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_I	DDL_P-	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:POHK3CCD.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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							
	.*DRC	P PACKAGE BODY:.*:	YES:YES:.*:.*					
	OR, any of the selected values below:							
	Setting not found							
	Ta	ble not found						
A - 1 I	1 1	I I	04 -4 00-04-00 DM	OMT (0500)				
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM (GM I +0530)				
	SCB_A	AUDIT_DDL_POLICY:I	OROP PACKAGE BODY	:STANDARD ACTION:	YES:YES:BY USER:ALL	USERS		
Extended E	viden	ce:						
POLICY_NAM	ΙE	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_I	DDL_P-	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.hk. Passed MEDIUM standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

xpected	matches regular expression list									
	.*:LOGON:.*:.*:YES:.*:.*									
	OR, any of the selected values below:									
	Setting not found									
	Table not found									
	Table not found									
Actual	☐ Table not found Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)									
Actual										
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)									

3CD_1	SCB_LOGON_LOGOFF_FRIVOSER.LOGON.STANDARD ACTION.TES.TES.BI OSER.ALL OSERS									
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				

(1.53) 14376 Status of auditing for 'LOGON' action (Unified Auditing)(oracle19:1:1621:POHK4CCD. Passed MEDIUM hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

					type defined on the da abled_option, and enti		ontains colon		
Expected	matc	hes regular expres	ssion list						
	.*:LOC	GON:.*:.*:YES:.*:.*							
	OR, any of the selected values below:								
	Set	Setting not found							
	Tal	ble not found							
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM (GMT+0530)					
	SCB_I	.OGON_ALL_FAILURE	S:LOGON:STANDARD	ACTION:NO:YES:BY U	SER:ALL USERS				
	SCB_L	.OGON_LOGOFF_PRI\	/USER:LOGON:STAND	ARD ACTION:YES:YES	:BY USER:ALL USERS				
Extended Ex	vidend	ce:							
POLICY_NAMI	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_LOGON_I FF_PRIVUSER		LOGON	STANDARD ACTION	YES	YES	BY USER	ALL USERS		
SCB_LOGON_AFAILURES	ALL	LOGON	STANDARD ACTION	NO	YES	BY USER	ALL USERS		

(1.53) 14376 Status of auditing for 'LOGON' action (Unified Auditing)(oracle19:1:1621:POHK5CCD. Passed MEDIUM hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

Exteriaca Eviacin	Exteriora 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				

(1.53) 14376 Status of auditing for 'LOGON' action (Unified Auditing)(oracle19:1:1621:POHK1RCT.hk. Passed MEDIUM standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	matc	hes regular expres	ssion list						
	.*:LO0	GON:.*:.*:YES:.*:.*							
	OR, any of the selected values below:								
	Setting not found								
	Ta	ble not found							
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM ((GMT+0530)					
		_	S:LOGON:STANDARD	,	SER:ALL USERS				
	SCB_I	LOGON_LOGOFF_PRIV	/USER:LOGON:STAND	ARD ACTION:YES:YES	:BY USER:ALL USERS				
Extended E	viden	ce:							
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_LOGON_IFF_PRIVUSER		LOGON	STANDARD ACTION	YES	YES	BY USER	ALL USERS		
SCB_LOGON_AFAILURES	ALL	LOGON	STANDARD ACTION	NO	YES	BY USER	ALL USERS		

(1.53) 14376 Status of auditing for 'LOGON' action (Unified Auditing)(oracle19:1:1621:POHK1CAT.hk. Passed MEDIUM standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_AUDIT_DDL_POLICY:LOGON:STANDARD ACTION:YES:YES:BY USER:ALL USERS 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_AUDIT_DDL_P- OLICY	LOGON	STANDARD ACTION	YES	YES	BY USER	ALL USERS
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

(1.53) 14376 Status of auditing for 'LOGON' action (Unified Auditing)(oracle19:1:1621:POHK1CCD. Passed MEDIUM hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_LOGOF- LOGON ALL USERS STANDARD ACTION YES BY USER

(1.53) 14376 Status of auditing for 'LOGON' action (Unified Auditing)(oracle19:1:1621:POHK2CCD. Passed MEDIUM hk.standardchartered.com)

YES

BY USER

ALL USERS

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

STANDARD ACTION NO

Previous Status Passed

SCB_LOGON_ALL_F- LOGON

F_PRIVUSER

AILŪRES

Evaluation Date 08/04/2024 at 10:38:34 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:

Externaca Evident	ZATORIGOU EVIGORIOO.								
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			

(1.53) 14376 Status of auditing for 'LOGON' action (Unified Auditing)(oracle19:1:1621:POHK3CCD. Passed MEDIUM hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	matc	hes regular expr	ession list							
-	.*:LOGON:.*:.*:YES:.*:.*									
	OR, any of the selected values below:									
	Setting not found									
	Tal	ble not found								
Actual	Last	Updated:08/04/2	024 at 06:01:09 PM ((GMT+0530)						
	SCB_LOGON_ALL_FAILURES:LOGON:STANDARD ACTION:NO:YES:BY USER:ALL USERS									
	SCB_I	.OGON_LOGOFF_PR	IVUSER:LOGON:STAND	ARD ACTION:Y	ES:YES:BY USER:ALL U	SERS				
Extended E	viden	ce:								
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCB_LOGON_I FF_PRIVUSER	LOGO-	LOGON	STANDARD ACTION	YES	YES	BY USER	ALL USERS			
SCB_LOGON_AFAILURES	ALL	LOGON	STANDARD ACTION	NO	YES	BY USER	ALL USERS			
(1.54) 14377		is of auditing for andardchartered	'LOGOFF' action (U l.com)	Inified Auditi	ng)(oracle19:1:162 ⁻	1:POHK1API. Passe	ed MEDIUM			
Instance		oracle19:1:1621:P0	OHK1API.hk.standardch	artered.com						

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

	p,/, p-	,	,,,			
Expected	matches regular expression list					
	.*:LOGOFF:.*:YES:YES:.*:.*					
	OR, any of the selected values below:					
	Setting not found					
	Table not found					
	1 1 1 1 1 1	-				
Actual	Last Updated:08/04/202	24 at 06:01:09 PM (GMT+0530)				
	SCB_LOGON_LOGOFF_PRIVUSER:LOGOFF:STANDARD ACTION:YES:YES:BY USER:ALL USERS					
	• • • • • • • • • • • • • • • • • • • •					
Extended E	vidence:					
POLICY_NAM	E AUDIT_OPTION	AUDIT_OPTION_TYPE SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	

SCB_LOGON_LOGO- FF_PRIVUSER	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.54) 14377 Status of auditing for 'LOGOFF' action (Unified Auditing)(oracle19:1:1621:POHK4CCD. Passed MEDIUM hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

separateu vaiu	ies 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 L	_ast Updated:08/04/2024 at 06:01:09 PM (GMT+0530)						
S	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_LO	GO- LOGOFF	STANDARD ACTION	YES	YES	BY USER	ALL USERS	

(1.54) 14377 Status of auditing for 'LOGOFF' action (Unified Auditing)(oracle19:1:1621:POHK5CCD. Passed MEDIUM hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 m	matches regular expression list								
.	.:LOGOFF:.*:YES:YES:.**								
0	R, any of the selected	d values below:							
	Setting not found								
	Table not found								
Actual La	st Updated:08/04/20	24 at 06:01:09 PM ((GMT+0530)						
SC	B_LOGON_LOGOFF_PRI	VUSER:LOGOFF:STANI	DARD ACTION:YES:YE	S:BY USER:ALL USERS					
Extended Evid	ence:								
POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCB_LOGON_LOG FF_PRIVUSER	O- LOGOFF	STANDARD ACTION	YES	YES	BY USER	ALL USERS			

(1.54) 14377 Status of auditing for 'LOGOFF' action (Unified Auditing)(oracle19:1:1621:POHK1RCT. Passed MEDIUM hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

separated value	ies of p	olicy_name, audit_op	tion, audit_option_typ	e, success, failure, en	abled_option, and ent	ity_name.	
Expected	matc	hes regular expres	ssion list				
	.*:LOC	OFF:.*:YES:YES:.*:.*					
	OR, a	any of the selected	l values below:				
	Set	ting not found					
	Tal	ole not found					
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM (GMT+0530)			
	SCB_I	OGON_LOGOFF_PRI\	/USER:LOGOFF:STANI	OARD ACTION:YES:YE	S:BY USER:ALL USERS	S	
Extended Evidence:							
POLICY_NAM	NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME						
SCB_LOGON_IFF_PRIVUSER		LOGOFF	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.54) 14377 Status of auditing for 'LOGOFF' action (Unified Auditing)(oracle19:1:1621:POHK1CAT. Passed MEDIUM hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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								
	.*:LOC	GOFF:.*:YES:YES:.*:.*							
	OR, a	any of the selected	l values below:						
	Set	tting not found							
	Tal	ble not found							
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM (GMT+0530)					
	SCB_AUDIT_DDL_POLICY:LOGOFF:STANDARD ACTION:YES:YES:BY USER:ALL USERS								
	SCB_I	LOGON_LOGOFF_PRIV	/USER:LOGOFF:STANI	DARD ACTION:YES:YE	S:BY USER:ALL USERS				
Extended Ev	vidend	ce:							
POLICY_NAMI	Е	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_D OLICY	DL_P-	LOGOFF	STANDARD ACTION	YES	YES	BY USER	ALL USERS		
SCB_LOGON_I	LOGO-	LOGOFF	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.54) 14377 Status of auditing for 'LOGOFF' action (Unified Auditing)(oracle19:1:1621:POHK1CCD. Passed MEDIUM hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 and entity name

separated valu	ies of p	oolicy_name, audit_op	tion, audit_option_typ	e, success, failure, er	nabled_option, and ent	ity_name.	ontains colon
Expected	matches regular expression list						
	.*:LOC	OFF:.*:YES:YES:.*:.*					
	OR, a	any of the selected	d values below:				
	Set	ting not found					
	Tal	ble not found					
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM ((GMT+0530)			
	SCB_I	OGON_LOGOFF_PRIV	/USER:LOGOFF:STANI	DARD ACTION:YES:YI	ES:BY USER:ALL USERS)	
Extended E	Extended Evidence:						
POLICY_NAM	NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME						
SCB_LOGON_I FF_PRIVUSER		LOGOFF	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.54) 14377 Status of auditing for 'LOGOFF' action (Unified Auditing)(oracle19:1:1621:POHK2CCD. Passed MEDIUM hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	matc	matches regular expression list							
	.*:LO0	GOFF:.*:YES:YES:.*:.*							
	OR, a	any of the selected	d values below:						
	Set	tting not found							
	Ta	ble not found							
Actual	Last	Un dete de00/04/20	04 at 00:04:00 DM (CMT - 0520\					
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM (GIVI I +0530)					
	SCB_I	LOGON_LOGOFF_PRIV	/USER:LOGOFF:STANI	DARD ACTION:YES:YE	S:BY USER:ALL USERS				
Extended E	viden	ce:							
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_LOGON_ FF_PRIVUSER		LOGOFF	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.54) 14377 Status of auditing for 'LOGOFF' action (Unified Auditing)(oracle19:1:1621:POHK3CCD. Passed MEDIUM hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

	г		,	-,	abrea_operors, arra erre		
Expected	matc	hes regular expre	ssion list				
	.*:LOG	OFF:.*:YES:YES:.*:.*					
	OR, a	any of the selected	l values below:				
	Set	ting not found					
	Tal	ole not found					
A = (=1	1	l ll- (l-00/04/00/	04 -4 00-04-00 DM	OMT (0500)			
Actual	Last	Updated:08/04/20/	24 at 06:01:09 PM (GIVI I +0530)			
	SCB_L	OGON_LOGOFF_PRIV	/USER:LOGOFF:STANI	OARD ACTION:YES:YE	S:BY USER:ALL USERS		
Extended Ex	tended Evidence:						
POLICY_NAM	AME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME						
SCB_LOGON_I FF_PRIVUSER		LOGOFF	STANDARD ACTION	YES	YES	BY USER	ALL USERS

(1.55) 24264 Status of ENCRYPTION_SERVER and AUTHENTICATION_SERVICES(oracle19:1:1621: Failed MEDIUM POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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 value	es below:	
	Setting not found		
	File not found		
Actual	Last Updated:08/04/2024 at 0	6:01:09 PM (GMT+0530)	
	File not found	, ,	
Extended E	Evidence:		
File name		Setting	Value
	id/product/12cR2/network/admin/		
sqlnet.ora			
OR			
The following	g List String value(s) of X indicates th	ne status of the SQLNET.authentication_services se	etting defined within the sqlnet.ora file.
Expected	contains regular expression	list	
	tcps		
	OR, any of the selected value	es below:	
	Setting not found		
	File not found		
Actual	Last Updated:08/04/2024 at 0	6:01:09 PM (GMT+0530)	
	File not found	·	
Extended E	Evidence:		
File name		Setting	Value
/u01/app/gri	id/product/12cR2/network/admin/		
sqlnet.ora			
Instance Previous Status Evaluation Dat			
Lvaldation Dat	00/04/2024 at 10.30.34 11	vi (Givii 10000)	
tracing featu Security opt enabled on t has been in	ures, prioritizing naming meth tions. The 'ENCRYPTION_SE he database server. 'AUTHEN'	ication method can be none, all, beq, Ke	c processes, and Oracle Advanced etermines whether or not encryption is re authentication services. If authentication
This String va	alue X indicates the current value se	for the SQLNET.ENCRYPTION_SERVER paramete	r in the sqlnet.ora file.
Expected	regular expression match		
	REQUESTED		
	OR, any of the selected value	es below:	
	Setting not found		
	File not found		
Actual	Last Updated:08/04/2024 at 0	6:01:09 PM (GMT+0530)	
	File not found	· · · · · ·	
Extended E	vidence:		
File name		Setting	Value
	id/product/12cR2/network/admin/		
OR			
The following	z List String value(s) of X indicates th	ne status of the SQLNET.authentication_services se	etting defined within the solnet ora file
Expected	contains regular expression		a zamez man die ognicanta me.
Lyberien	tcps	iiot .	
	OR any of the selected value	os holow:	

	Setting not found File not found		
Actual	Last Updated:08/04/2024 at 0	6:01:09 PM (GMT+0530)	
	File not found		
Extended Ev	vidence:		
File name		Setting	Value
/u01/app/grid sqlnet.ora	/product/12cR2/network/admin/	sqlnet.authentication_services	

(1.55) 24264 Status of ENCRYPTION_SERVER and AUTHENTICATION_SERVICES(oracle19:1:1621: Failed MEDIUM POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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 va	lue X indicates the current value set	for the SQLNET.ENCRYPTION_SERVER parameter	in the sqlnet.ora file.
Expected	Expected regular expression match		
	REQUESTED		
	OR, any of the selected value	es below:	
	Setting not found		
	File not found		
Actual	Last Updated:08/04/2024 at 0	6:01:09 PM (GMT+0530)	
	File not found		
Extended E	vidence:		
File name		Setting	Value
/u01/app/grisqlnet.ora	d/product/12cR2/network/admin/	sqlnet.encryption_server	
OR			
The following	List String value(s) of X indicates th	ne status of the SQLNET.authentication_services se	tting defined within the sqlnet.ora file.
Expected	contains regular expression	list	
	tcps		
	OR, any of the selected value	es below:	
	Setting not found		
	File not found		
Actual	Last Updated:08/04/2024 at 0	6:01:09 PM (GMT+0530)	
	File not found		
Extended E	vidence:		
File name		Setting	Value
/u01/app/grid sqlnet.ora	d/product/12cR2/network/admin/	sqlnet.authentication_services	

(1.55) 24264 Status of ENCRYPTION_SERVER and AUTHENTICATION_SERVICES(oracle19:1:1621: Failed MEDIUM POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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 value	es below:	
	Setting not found		
	File not found		
Actual	Last Updated:08/04/2024 at 0	6:01:09 PM (GMT+0530)	
	File not found		
Extended E	vidence:		
File name		Setting	Value
/u01/app/grid sqlnet.ora	d/product/12cR2/network/admin/	sqlnet.encryption_server	
OR			
The following	List String value(s) of X indicates th	e status of the SQLNET.authentication_services set	tting defined within the sqlnet.ora file.
Expected	contains regular expression list		
	tcps		
	OR, any of the selected value	es below:	
	Setting not found		
	File not found		
Actual	Last Updated:08/04/2024 at 0	6:01:09 PM (GMT+0530)	
	File not found		
Extended E	vidence:		
File name		Setting	Value
/u01/app/grid sqlnet.ora	d/product/12cR2/network/admin/	sqlnet.authentication_services	

(1.55) 24264 Status of ENCRYPTION_SERVER and AUTHENTICATION_SERVICES(oracle19:1:1621: Passed MEDIUM POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 val	ue 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:08/04/2024 at 06:01:09 PM (GMT+0530)
	REQUESTED
Extended Ex	vidence:

File name		Setting	Value
/u01/app/ora ora	cle/local/network/admin/sqlnet.	sqlnet.encryption_server	REQUESTED
OR			
The following	List String value(s) of X indicates the	ne status of the SQLNET.authentication_services set	ting defined within the sqlnet.ora file.
Expected	contains regular expression	list	
	tcps		
	OR, any of the selected value	es below:	
	Setting not found File not found		
Actual	Last Updated:08/04/2024 at 0	06:01:09 PM (GMT+0530)	
	Setting not found		
Extended E	d Evidence:		
File name		Setting	Value
/u01/app/ora	cle/local/network/admin/sqlnet.	sqlnet.authentication_services	

(1.55) 24264 Status of ENCRYPTION_SERVER and AUTHENTICATION_SERVICES(oracle19:1:1621: Failed MEDIUM POHK1CCD.hk.standardchartered.com)

 $In stance \qquad \qquad oracle 19:1:1621: POHK1CCD. hk. standard chartered. com$

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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.

alue X indicates the current value set	for the SQLNET.ENCRYPTION_SERVER parameter	ter in the sqlnet.ora file.
Expected regular expression match		
REQUESTED		
OR, any of the selected value	es below:	
Setting not found		
File not found		
Last Updated:08/04/2024 at 0	6:01:09 PM (GMT+0530)	
File not found		
Evidence:		
	Setting	Value
id/product/12cR2/network/admin/	sqlnet.encryption_server	
g List String value(s) of X indicates th	e status of the SQLNET.authentication_services	setting defined within the sqlnet.ora file.
contains regular expression	list	
tcps		
OR, any of the selected value	es below:	
Setting not found		
File not found		
Last Updated:08/04/2024 at 0	6:01:09 PM (GMT+0530)	
File not found		
Evidence:		
		Value
	regular expression match REQUESTED OR, any of the selected value Setting not found File not found Last Updated:08/04/2024 at 0 File not found Evidence: id/product/12cR2/network/admin/ g List String value(s) of X indicates the contains regular expression tcps OR, any of the selected value Setting not found File not found Last Updated:08/04/2024 at 0 File not found	REQUESTED OR, any of the selected values below: Setting not found File not found Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) File not found Evidence: Setting id/product/12cR2/network/admin/ sqlnet.encryption_server g List String value(s) of X indicates the status of the SQLNET.authentication_services contains regular expression list tcps OR, any of the selected values below: Setting not found File not found Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) File not found

/u01/app/grid/product/12cR2/network/adminsqlnet.ora	sqlnet.authentication_services	
---	--------------------------------	--

(1.55) 24264 Status of ENCRYPTION_SERVER and AUTHENTICATION_SERVICES(oracle19:1:1621: Failed MEDIUM POHK2CCD.hk.standardchartered.com)

Instance oracle 19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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 va	alue 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 value	es below:	
	Setting not found		
	File not found		
Actual	Last Updated:08/04/2024 at 0	6:01:09 PM (GMT+0530)	
	File not found		
Extended E	vidence:		
File name		Setting	Value
/u01/app/gri sqlnet.ora	id/product/12cR2/network/admin/	sqlnet.encryption_server	
OR			
The following	g List String value(s) of X indicates th	ne status of the SQLNET.authentication_services set	tting defined within the sqlnet.ora file.
Expected	contains regular expression	list	
	tcps		
	OR, any of the selected value	es below:	
	Setting not found		
	File not found		
Actual	Last Updated:08/04/2024 at 0	6:01:09 PM (GMT+0530)	
	File not found		
Extended E	vidence:		
File name		Setting	Value
/u01/app/gri sqlnet.ora	id/product/12cR2/network/admin/	sqlnet.authentication_services	

(1.55) 24264 Status of ENCRYPTION_SERVER and AUTHENTICATION_SERVICES(oracle19:1:1621: Failed MEDIUM POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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			
A 1		0.04.00 PM (ONT. 0500)		
Actual	Last Updated:08/04/2024 at 0 File not found	6:01:09 PM (GMT+0530)		
Extended E	ividence:	1_	I	
File name	1/ 1 //10 DO/ / 1/ 1 : /	Setting	Value	
/u01/app/gri sqlnet.ora	id/product/12cR2/network/admin/	sqinet.encryption_server		
OR				
The following	g List String value(s) of X indicates th	ne status of the SQLNET.authentication_services se	tting defined within the sqlnet.ora file.	
Expected	contains regular expression	list		
	tcps			
	OR, any of the selected value	es below:		
	Setting not found File not found			
Actual	Last Updated:08/04/2024 at 0	6:01:09 PM (GMT+0530)		
	File not found			
Extended E	vidence:			
File name		Setting	Value	
/u01/app/gri sqlnet.ora	id/product/12cR2/network/admin/	sqlnet.authentication_services		
(1.56) 10062	28 Disallow Factory or Vendor	Default accounts in Production(oracle19:1	:1621: Passed HIGH	
Ŧ	POHK3CCD.hk.standardcha	•		
Instance Previous Status	oracle19:1:1621:POHK3CCl s Passed	J.hk.standardchartered.com		
Evaluation Date		M (GMT+0530)		
Disallow Fa	ctory or Vendor Default accou	unts in Production		
Disallow Fact	ory or Vendor Default accounts in P	roduction		
Scan Paran	neters:			
DBQUERY:	select username from dba_users			
Expected	does not contain regular exp	ression list		
	DB Column Name: USERNAME			
	^SH\$			
	^SCOTT\$			
	^PM\$			
	^OE\$			
	^IX\$			
	^HR\$			
	^BI\$	as balawi		
	OR, any of the selected value Set status to PASS if no data for			
A - 1 - 1				
Actual	Last Updated:08/04/2024 at 0	6:01:09 PM (GMT+0530)		

ISERNAME
YS
YSTEM
IS\$NULL
DJVMSYS
BACSYS
DACSIS
YS\$UMF
DBSNMP
PPQOSSYS
DESFWUSER
CGSYS
NONYMOUS
TXSYS
VSYS
VF
SMADMIN_INTERNAL
MDSYS
DLAPSYS
IDB
VMSYS
SMCATUSER
CS_SCAN
MDDATA
YSBACKUP
EMOTE_SCHEDULER_AGENT
DRARO
CB_LINK
SMUSER
YSRAC
SMROOTUSER
DRAMED2
I_INFORMTN_SCHEMA
BARO
UDSYS
OIP
DRDPLUGINS
BADDM
YSKM
DRDDATA
OGEMS
DRACLE_OCM
DEMUSER NAME OF THE PROPERTY O
YSDG
PRDSYS
PRAMED1
ECADMIN
C_ITRS
GADMIN
CB_ADMIN

Extended Evidence:

Statistics:

Query returned 49 rows

(1.56) 100628 Disallow Factory or Vendor Default accounts in Production(oracle19:1:1621: Passed HIGH POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

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
DBSNMP
APPQOSSYS
DBSFWUSER
GGSYS
ANONYMOUS
CTXSYS
DVSYS
DVF
GSMADMIN_INTERNAL
MDSYS
OLAPSYS
XDB
WMSYS
GSMCATUSER
MDDATA
SYSBACKUP
REMOTE_SCHEDULER_AGENT
GSMUSER
SYSRAC
GSMROOTUSER
SI_INFORMTN_SCHEMA
AUDSYS
DIP
ORDPLUGINS
SYSKM
ORDDATA
ORACLE_OCM
SYSDG
ORDSYS
ORARO CARO
PUPPETAM
ORAMED1
CCS_SCAN CS_SCAN
SCB_LINK DRADO
DBARO DPADDM
DBADDM DBADO2
DBARO2
AOGEMS
SCB_REMOTE_CLONE
OEMUSER
SECADMIN
SCB_ADMIN

Extended Evidence:

Statistics:

Query returned 49 rows

(1.56) 100628 Disallow Factory or Vendor Default accounts in Production(oracle19:1:1621: Passed HIGH POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

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
DBSNMP
APPQOSSYS
DBSFWUSER
GGSYS
ANONYMOUS
CTXSYS
DVSYS
DVF
GSMADMIN_INTERNAL
MDSYS
OLAPSYS
XDB
WMSYS
GSMCATUSER
CCS_SCAN
MDDATA
SYSBACKUP
REMOTE_SCHEDULER_AGENT
ORARO
SCB_LINK
GSMUSER
SYSRAC
GSMROOTUSER
ORAMED2
SI_INFORMTN_SCHEMA
DBARO
AUDSYS
DIP
ORDPLUGINS
DBADDM SYSKM
ORDDATA LOGDING
AOGEMS
ORACLE_OCM
OEMUSER
SYSDG
ORDSYS
ORAMED1
SECADMIN
DAY DAY DAY OF THE STATE OF THE
PUPPETAM
PUPPETAM CC_ITRS GGADMIN

Extended Evidence:

Statistics:

Query returned 49 rows

(1.56) 100628 Disallow Factory or Vendor Default accounts in Production(oracle19:1:1621: Passed HIGH POHK1RCT.hk.standardchartered.com)

 $In stance \qquad \qquad or a cle 19:1:1621: POHK1RCT. hk. standard chartered. com$

Previous Status Passed

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
DBSNMP
APPQOSSYS
DBSFWUSER
GGSYS
ANONYMOUS
CTXSYS
DVSYS
DVF
GSMADMIN_INTERNAL
MDSYS
OLAPSYS
XDB
WMSYS
GSMCATUSER
CCS_SCAN
MDDATA
SYSBACKUP
REMOTE_SCHEDULER_AGENT
ORARO
SCB_LINK
GSMUSER
SYSRAC
GSMROOTUSER
ORAMED2
SI_INFORMTN_SCHEMA
DBARO
AUDSYS
DIP
ORDPLUGINS
DBADDM
SYSKM
ORDDATA
AOGEMS
ORACLE_OCM
OEMUSER OEMUSER
SYSDG
ORDSYS
ORAMED1
PUPPETAM
CC_ITRS
SECADMIN SCR ADMIN
SCB_ADMIN

Extended Evidence:

Statistics:

Query returned 49 rows

(1.56) 100628 Disallow Factory or Vendor Default accounts in Production(oracle19:1:1621: Passed HIGH POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

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)

ISERNAME
YS
YSTEM
IS\$NULL
DJVMSYS
BACSYS
DACSIS
YS\$UMF
DBSNMP
PPQOSSYS
DESFWUSER
CGSYS
NONYMOUS
TXSYS
VSYS
VF
SMADMIN_INTERNAL
MDSYS
DLAPSYS
IDB
VMSYS
SMCATUSER
CS_SCAN
MDDATA
YSBACKUP
EMOTE_SCHEDULER_AGENT
DRARO
CB_LINK
SMUSER
YSRAC
SMROOTUSER
DRAMED2
I_INFORMTN_SCHEMA
BARO
UDSYS
OIP
DRDPLUGINS
BADDM
YSKM
DRDDATA
OGEMS
DRACLE_OCM
DEMUSER NAME OF THE PROPERTY O
YSDG
PRDSYS
PRAMED1
ECADMIN
C_ITRS
GADMIN
CB_ADMIN

Statistics:

Query returned 49 rows

(1.56) 100628 Disallow Factory or Vendor Default accounts in Production(oracle19:1:1621: Passed HIGH POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

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	

Statistics:

Query returned 47 rows

(1.56) 100628 Disallow Factory or Vendor Default accounts in Production(oracle19:1:1621: Passed HIGH POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

Disallow Factory or Vendor Default accounts in Production

Disallow Factor	Disallow Factory or Vendor Default accounts in Production					
Scan Paran	Scan Parameters:					
DBQUERY:	select username from dba_users					
Expected	does not contain regular expression list					
	DB Column Name: USERNAME					
	^SH\$					
	^SCOTT\$					
	^PM\$					
	^OE\$					
	^JX\$					
	^HR\$					

OR, any of the selected values below:

Set status to PASS if no data found

^BI\$

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

ISERNAME
YS
YSTEM
IS\$NULL
DJVMSYS
BACSYS
DACSIS
YS\$UMF
DBSNMP
PPQOSSYS
DESFWUSER
CGSYS
NONYMOUS
TXSYS
VSYS
VF
SMADMIN_INTERNAL
MDSYS
DLAPSYS
IDB
VMSYS
SMCATUSER
CS_SCAN
MDDATA
YSBACKUP
EMOTE_SCHEDULER_AGENT
DRARO
CB_LINK
SMUSER
YSRAC
SMROOTUSER
DRAMED2
I_INFORMTN_SCHEMA
BARO
UDSYS
OIP
DRDPLUGINS
BADDM
YSKM
DRDDATA
OGEMS
DRACLE_OCM
DEMUSER NAME OF THE PROPERTY O
YSDG
PRDSYS
PRAMED1
ECADMIN
C_ITRS
GADMIN
CB_ADMIN

Statistics:

Query returned 49 rows

(1.56) 100628 Disallow Factory or Vendor Default accounts in Production(oracle19:1:1621: Passed HIGH POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

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)

ISERNAME
YS
YSTEM
IS\$NULL
DJVMSYS
BACSYS
DACSIS
YS\$UMF
DBSNMP
PPQOSSYS
DESFWUSER
CGSYS
NONYMOUS
TXSYS
VSYS
VF
SMADMIN_INTERNAL
MDSYS
DLAPSYS
IDB
VMSYS
SMCATUSER
CS_SCAN
MDDATA
YSBACKUP
EMOTE_SCHEDULER_AGENT
DRARO
CB_LINK
SMUSER
YSRAC
SMROOTUSER
DRAMED2
I_INFORMTN_SCHEMA
BARO
UDSYS
OIP
DRDPLUGINS
BADDM
YSKM
DRDDATA
OGEMS
DRACLE_OCM
DEMUSER NAME OF THE PROPERTY O
YSDG
PRDSYS
PRAMED1
ECADMIN
C_ITRS
GADMIN
CB_ADMIN

Statistics:

Query returned 49 rows

(1.57) 101067 Status of auditing on the unified audit table(CIS-100)(oracle19:1:1621:POHK3CCD.hk. Passed HIGH standardchartered.com)

 $In stance \qquad \qquad oracle 19:1:1621: POHK3CCD. hk. standard chartered. com$

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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)

matches regular expression list **Expected**

DB Column Name: OBJECT_NAME

AUD\\$UNIFIED

OR, any of the selected values below:

Set status to PASS if no data found

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

> OBJECT_NAME AUD\$UNIFIED

Extended Evidence:

Statistics:

Query returned 1 rows

(1.57) 101067 Status of auditing on the unified audit table(CIS-100)(oracle19:1:1621:POHK1CAT.hk. HIGH **Passed** standardchartered.com)

oracle19:1:1621:POHK1CAT.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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

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

OBJECT_NAME

AUD\$UNIFIED

Extended Evidence:

Statistics:

Query returned 1 rows

(1.57) 101067 Status of auditing on the unified audit table(CIS-100)(oracle19:1:1621:POHK5CCD.hk. HIGH **Passed** standardchartered.com)

oracle19:1:1621:POHK5CCD.hk.standardchartered.com Instance

Previous Status

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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

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

Scan Parameters:

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) DBQUERY:

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

(1.57) 101067 Status of auditing on the unified audit table(CIS-100)(oracle19:1:1621:POHK1RCT.hk. **Passed HIGH** standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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:

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

matches regular expression list **Expected**

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

(1.57) 101067 Status of auditing on the unified audit table(CIS-100)(oracle19:1:1621:POHK4CCD.hk. **Passed** HIGH standardchartered.com)

oracle19:1:1621:POHK4CCD.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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:

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) DBQUERY:

matches regular expression list **Expected**

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:

(1.57) 101067 Status of auditing on the unified audit table(CIS-100)(oracle19:1:1621:POHK1CCD.hk. **Passed** HIGH standardchartered.com)

oracle19:1:1621:POHK1CCD.hk.standardchartered.com Instance

Previous Status Passed

Query returned 1 rows

Evaluation Date 08/04/2024 at 10:38:34 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:

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) DBQUERY:

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

(1.57) 101067 Status of auditing on the unified audit table(CIS-100)(oracle19:1:1621:POHK1API.hk. **Passed HIGH** standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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:

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) DBQUERY:

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

(1.57) 101067 Status of auditing on the unified audit table(CIS-100)(oracle19:1:1621:POHK2CCD.hk. HIGH **Passed** standardchartered.com)

oracle19:1:1621:POHK2CCD.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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:

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) DBOUERY:

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:POHK1RCT. Passed HIGH hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

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

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

Scan Parameters:

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

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

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

(1.58) 101068 Status of Vendor Default accounts in Production(IAM-120)(oracle19:1:1621: **Passed** POHK3CCD.hk.standardchartered.com)

HIGH

oracle19:1:1621:POHK3CCD.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.58) 101068 Status of Vendor Default accounts in Production(IAM-120)(oracle19:1:1621:POHK1CAT. Passed **HIGH** hk.standardchartered.com)

oracle19:1:1621:POHK1CAT.hk.standardchartered.com Instance

Passed Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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

(1.58) 101068 Status of Vendor Default accounts in Production(IAM-120)(oracle19:1:1621: **Passed HIGH** POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(1.58) 101068 Status of Vendor Default accounts in Production(IAM-120)(oracle19:1:1621: HIGH **Passed** POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

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

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

Scan Parameters:

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

Expected any of the selected values below:

Set status to PASS if no data found

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.58) 101068 Status of Vendor Default accounts in Production(IAM-120)(oracle19:1:1621: **Passed** HIGH POHK1CCD.hk.standardchartered.com)

oracle19:1:1621:POHK1CCD.hk.standardchartered.com Instance

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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

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

Scan Parameters:

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

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

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

(1.58) 101068 Status of Vendor Default accounts in Production(IAM-120)(oracle19:1:1621:POHK1API. Passed HIGH hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

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

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

Scan Parameters:

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

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

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

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

Passed

HIGH

POHK2CCD.hk.standardchartered.com) Instance oracle 19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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:POHK1RCT.hk.standardchartered.com)

Passed HIGH

oracle19:1:1621:POHK1RCT.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	DEFAULT	SCB_19C_PWD_VERIFY_FUNCTION	NO NO
1	ORA_STIG_PROFILE	SCB_19C_PWD_VERIFY_FUNCTION	NO NO
1	SCB_STATIC_APP	SCB_19C_PWD_VERIFY_FUNCTION	N YES
3	SCB_SUPP	SCB_19C_PWD_VERIFY_FUNCTION	NO NO
3	DEFAULT	SCB_19C_PWD_VERIFY_FUNCTION	NO NO
3	ORA_STIG_PROFILE	SCB_19C_PWD_VERIFY_FUNCTION	NO NO

Extended Evidence:

Statistics:

Query returned 6 rows

(1.59) 101070 Status of Database user password complexity('PASSWORD_VERIFY_FUNCTION') (IAM-400,CIS-26,CIS-9)(oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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
5	DEFAULT	SCB_19C_PWD_VERIFY_FUNCTION	NO
4	SCB_SUPP	SCB_19C_PWD_VERIFY_FUNCTION	NO
4	DEFAULT	SCB_19C_PWD_VERIFY_FUNCTION	NO
4	SCB_STATIC_APP_TNG	SCB_19C_PWD_VERIFY_FUNCTION	NO
3	SCB_SUPP	SCB_19C_PWD_VERIFY_FUNCTION	NO
5	ORA_STIG_PROFILE	SCB_19C_PWD_VERIFY_FUNCTION	NO
3	SCB_STATIC_APP_PSS	SCB_19C_PWD_VERIFY_FUNCTION	NO
3	SCB_STATIC_APP_TDC	SCB_19C_PWD_VERIFY_FUNCTION	NO
5	SCB_SUPP	SCB_19C_PWD_VERIFY_FUNCTION	NO
1	ORA_STIG_PROFILE	SCB_19C_PWD_VERIFY_FUNCTION	NO
3	ORA_STIG_PROFILE	SCB_19C_PWD_VERIFY_FUNCTION	NO
4	ORA_STIG_PROFILE	SCB_19C_PWD_VERIFY_FUNCTION	NO
4	SCB_STATIC_APP_PSS	SCB_19C_PWD_VERIFY_FUNCTION	NO
5	SCB_STATIC_APP_PSS	SCB_19C_PWD_VERIFY_FUNCTION	NO
1	DEFAULT	SCB_19C_PWD_VERIFY_FUNCTION	NO
1	SCB_STATIC_APP	SCB_19C_PWD_VERIFY_FUNCTION	YES
5	SCB_STATIC_APP_QLDSADMIN	SCB_19C_PWD_VERIFY_FUNCTION	NO
3	DEFAULT	SCB_19C_PWD_VERIFY_FUNCTION	NO
3	SCB_STATIC_APP_DS	SCB_19C_PWD_VERIFY_FUNCTION	NO

Extended Evidence:

Statistics:

Query returned 19 rows

(1.59) 101070 Status of Database user password complexity('PASSWORD_VERIFY_FUNCTION') (IAM-400,CIS-26,CIS-9)(oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Passed HIGH

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

Oracle_ATOS - 20240806 page 517

Passed HIGH

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
4	SCB_STATIC_APP_ATX	SCB_19C_PWD_VERIFY_FUNCTION	NO
5	DEFAULT	SCB_19C_PWD_VERIFY_FUNCTION	NO
5	SCB_STATIC_APP	SCB_19C_PWD_VERIFY_FUNCTION	NO
1	SCB_INFRA_APP	SCB_19C_PWD_VERIFY_FUNCTION	YES
4	SCB_SUPP	SCB_19C_PWD_VERIFY_FUNCTION	NO
5	SCB_SUPP	SCB_19C_PWD_VERIFY_FUNCTION	NO
4	ORA_STIG_PROFILE	SCB_19C_PWD_VERIFY_FUNCTION	NO
4	DEFAULT	SCB_19C_PWD_VERIFY_FUNCTION	NO
5	SCB_STATIC_APP_ATX_IDLE30	SCB_19C_PWD_VERIFY_FUNCTION	NO
4	SCB_STATIC_APP	SCB_19C_PWD_VERIFY_FUNCTION	NO
1	DEFAULT	SCB_19C_PWD_VERIFY_FUNCTION	NO
1	SCB_INFRA_SUPP	SCB_19C_PWD_VERIFY_FUNCTION	YES
5	SCB_STATIC_APP_ATX	SCB_19C_PWD_VERIFY_FUNCTION	NO
5	SCB_STATIC_APP_CCS	SCB_19C_PWD_VERIFY_FUNCTION	NO
1	ORA_STIG_PROFILE	SCB_19C_PWD_VERIFY_FUNCTION	NO
5	ORA_STIG_PROFILE	SCB_19C_PWD_VERIFY_FUNCTION	NO

Extended Evidence:

Statistics:

Query returned 16 rows

(1.59) 101070 Status of Database user password complexity('PASSWORD_VERIFY_FUNCTION') (IAM-400,CIS-26,CIS-9)(oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Passed HIGH

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

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

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
3	SCB_STATIC_APP_PSS	SCB_19C_PWD_VERIFY_FUNCTION	NO
3	SCB_STATIC_APP_NGW	SCB_19C_PWD_VERIFY_FUNCTION	NO
3	SCB_STATIC_APP_INF	SCB_19C_PWD_VERIFY_FUNCTION	NO
1	SCB_INFRA_APP	SCB_19C_PWD_VERIFY_FUNCTION	YES
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	DEFAULT	SCB_19C_PWD_VERIFY_FUNCTION	NO
3	ORA_STIG_PROFILE	SCB_19C_PWD_VERIFY_FUNCTION	NO

Extended Evidence:

Statistics:

Query returned 10 rows

(1.59) 101070 Status of Database user password complexity('PASSWORD_VERIFY_FUNCTION') **Passed** (IAM-400,CIS-26,CIS-9)(oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

HIGH

oracle19:1:1621:POHK4CCD.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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:

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

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
3	ORA_STIG_PROFILE	SCB_19C_PWD_VERIFY_FUNCTION	NO
4	SCB_STATIC_APP_CAD	SCB_19C_PWD_VERIFY_FUNCTION	NO
3	DEFAULT	SCB_19C_PWD_VERIFY_FUNCTION	NO
3	SCB_STATIC_APP_PSS	SCB_19C_PWD_VERIFY_FUNCTION	NO
1	SCB_INFRA_APP	SCB_19C_PWD_VERIFY_FUNCTION	YES
5	SCB_SUPP	SCB_19C_PWD_VERIFY_FUNCTION	NO
1	ORA_STIG_PROFILE	SCB_19C_PWD_VERIFY_FUNCTION	NO
5	DEFAULT	SCB_19C_PWD_VERIFY_FUNCTION	NO
4	SCB_SUPP	SCB_19C_PWD_VERIFY_FUNCTION	NO
4	DEFAULT	SCB_19C_PWD_VERIFY_FUNCTION	NO
3	SCB_SUPP	SCB_19C_PWD_VERIFY_FUNCTION	NO
5	ORA_STIG_PROFILE	SCB_19C_PWD_VERIFY_FUNCTION	NO
4	ORA_STIG_PROFILE	SCB_19C_PWD_VERIFY_FUNCTION	NO
4	SCB_STATIC_APP_PSS	SCB_19C_PWD_VERIFY_FUNCTION	NO
5	SCB_STATIC_APP_PSS	SCB_19C_PWD_VERIFY_FUNCTION	NO
1	DEFAULT	SCB_19C_PWD_VERIFY_FUNCTION	NO
1	SCB_STATIC_APP	SCB 19C PWD VERIFY FUNCTION	YES

Extended Evidence:

Statistics:

Query returned 17 rows

(1.59) 101070 Status of Database user password complexity('PASSWORD_VERIFY_FUNCTION') (IAM-400,CIS-26,CIS-9)(oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Passed

HIGH

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Passed Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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:

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

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
7	DEFAULT	SCB_19C_PWD_VERIFY_FUNCTION	NO
4	SCB_SUPP	SCB_19C_PWD_VERIFY_FUNCTION	NO
4	ORA_STIG_PROFILE	SCB_19C_PWD_VERIFY_FUNCTION	NO
1	DEFAULT	SCB_19C_PWD_VERIFY_FUNCTION	NO
5	SCB_STATIC_APP_CCS	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
7	SCB_STATIC_APP_PSS	SCB_19C_PWD_VERIFY_FUNCTION	NO
5	SCB_SUPP	SCB_19C_PWD_VERIFY_FUNCTION	NO
5	SCB_STATIC_APP_ATX_IDLE30	SCB_19C_PWD_VERIFY_FUNCTION	NO
5	SCB_STATIC_APP_PSS	SCB_19C_PWD_VERIFY_FUNCTION	NO
4	SCB_STATIC_APP_PSS	SCB_19C_PWD_VERIFY_FUNCTION	NO
4	DEFAULT	SCB_19C_PWD_VERIFY_FUNCTION	NO
4	SCB_STATIC_APP_PAY	SCB_19C_PWD_VERIFY_FUNCTION	NO
3	ORA_STIG_PROFILE	SCB_19C_PWD_VERIFY_FUNCTION	NO
3	SCB_STATIC_APP_PSS	SCB_19C_PWD_VERIFY_FUNCTION	NO
5	SCB_STATIC_APP_ATX	SCB_19C_PWD_VERIFY_FUNCTION	NO
5	ORA_STIG_PROFILE	SCB_19C_PWD_VERIFY_FUNCTION	NO
5	DEFAULT	SCB_19C_PWD_VERIFY_FUNCTION	NO
5	SCB_APP_CCS	SCB_19C_PWD_VERIFY_FUNCTION	NO
3	SCB_SUPP	SCB_19C_PWD_VERIFY_FUNCTION	NO
7	ORA_STIG_PROFILE	SCB_19C_PWD_VERIFY_FUNCTION	
7	SCB_SUPP	SCB_19C_PWD_VERIFY_FUNCTION	
3	DEFAULT	SCB_19C_PWD_VERIFY_FUNCTION	

Extended Evidence:

Statistics:

Query returned 24 rows

(1.59) 101070 Status of Database user password complexity('PASSWORD_VERIFY_FUNCTION') (IAM-400,CIS-26,CIS-9)(oracle19:1:1621:POHK1API.hk.standardchartered.com)

HIGH **Passed**

oracle19:1:1621:POHK1API.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

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

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_SUPP	SCB_19C_PWD_VERIFY_FUNCTION	YES
3	ORA_STIG_PROFILE	SCB_19C_PWD_VERIFY_FUNCTION	NO
3	SCB_STATIC_APP_PSS	SCB_19C_PWD_VERIFY_FUNCTION	NO
3	SCB_STATIC_APP_ATX	SCB_19C_PWD_VERIFY_FUNCTION	NO
4	SCB_SUPP	SCB_19C_PWD_VERIFY_FUNCTION	NO
3	DEFAULT	SCB_19C_PWD_VERIFY_FUNCTION	NO
1	ORA_STIG_PROFILE	SCB_19C_PWD_VERIFY_FUNCTION	NO
1	SCB_INFRA_APP	SCB_19C_PWD_VERIFY_FUNCTION	YES
4	DEFAULT	SCB_19C_PWD_VERIFY_FUNCTION	NO
4	SCB_STATIC_APP_PSS	SCB_19C_PWD_VERIFY_FUNCTION	NO
3	SCB_SUPP	SCB_19C_PWD_VERIFY_FUNCTION	NO
4	ORA_STIG_PROFILE	SCB_19C_PWD_VERIFY_FUNCTION	NO
1	DEFAULT	SCB_19C_PWD_VERIFY_FUNCTION	NO
1	SCB_STATIC_APP	SCB_19C_PWD_VERIFY_FUNCTION	YES

HIGH

Extended Evidence:

Statistics:

Query returned 14 rows

(1.59) 101070 Status of Database user password complexity('PASSWORD_VERIFY_FUNCTION') (IAM-400,CIS-26,CIS-9)(oracle19:1:1621:POHK2CCD.hk.standardchartered.com) **Passed**

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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:

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

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
4	SCB_SUPP	SCB_19C_PWD_VERIFY_FUNCTION	NO
4	DEFAULT	SCB_19C_PWD_VERIFY_FUNCTION	NO
3	SCB_SUPP	SCB_19C_PWD_VERIFY_FUNCTION	NO
3	SCB_STATIC_APP_PSS	SCB_19C_PWD_VERIFY_FUNCTION	NO
6	ORA_STIG_PROFILE	SCB_19C_PWD_VERIFY_FUNCTION	NO
6	DEFAULT	SCB_19C_PWD_VERIFY_FUNCTION	NO
1	ORA_STIG_PROFILE	SCB_19C_PWD_VERIFY_FUNCTION	NO
4	SCB_STATIC_APP_WEB	SCB_19C_PWD_VERIFY_FUNCTION	NO
3	ORA_STIG_PROFILE	SCB_19C_PWD_VERIFY_FUNCTION	NO
4	SCB_STATIC_APP_NGO	SCB_19C_PWD_VERIFY_FUNCTION	NO
4	ORA_STIG_PROFILE	SCB_19C_PWD_VERIFY_FUNCTION	NO
4	SCB_STATIC_APP_NGO_1000	SCB_19C_PWD_VERIFY_FUNCTION	NO
4	SCB_STATIC_APP_PSS	SCB_19C_PWD_VERIFY_FUNCTION	NO
6	SCB_STATIC_APP_PSS	SCB_19C_PWD_VERIFY_FUNCTION	NO
1	DEFAULT	SCB_19C_PWD_VERIFY_FUNCTION	NO
1	SCB_STATIC_APP	SCB_19C_PWD_VERIFY_FUNCTION	YES
6	SCB_SUPP	SCB_19C_PWD_VERIFY_FUNCTION	NO
3	DEFAULT	SCB 19C PWD VERIFY FUNCTION	NO

Statistics:

Query returned 18 rows

(1.60) 101075 Status of the IDLE-TIME resource parameter set for Oracle profiles (IAM-450) (oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

Failed

MEDIUM

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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:

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

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	DEFAULT

Extended Evidence:

Statistics:

Query returned 1 rows

Cause of Failure:

Un	expected
val	ues

Additional values found in failed controls:

DEFAULT

(1.60) 101075 Status of the IDLE-TIME resource parameter set for Oracle profiles (IAM-450) (oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

Failed

MEDIUM

oracle19:1:1621:POHK3CCD.hk.standardchartered.com Instance

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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:

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

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	DEFAULT

Statistics:

Query returned 1 rows

Cause of Failure:

Unexpected values

Additional values found in failed controls:

DEFAULT

(1.60) 101075 Status of the IDLE-TIME resource parameter set for Oracle profiles (IAM-450) (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_INFRA_SUPP	15
SCB_SUPP	15

Extended Evidence:

Statistics:

Instance

Query returned 2 rows

(1.60) 101075 Status of the IDLE-TIME resource parameter set for Oracle profiles (IAM-450) (oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Failed MEDIUM

oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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:

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

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	DEFAULT

Statistics:

Query returned 1 rows

Cause of Failure:

Unexpected values

Additional values found in failed controls:

DEFAULT

(1.60) 101075 Status of the IDLE-TIME resource parameter set for Oracle profiles (IAM-450) (oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

Failed

MEDIUM

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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	DEFAULT
SCB_SUPP	15

Extended Evidence:

Statistics:

Query returned 2 rows

Cause of Failure:

Un	expected
val	ues

Additional values found in failed controls:

DEFAULT

(oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Failed

MEDIUM

oracle19:1:1621:POHK1CCD.hk.standardchartered.com Instance

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

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

(1.60) 101075 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:

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

Expected match all equal to

DB Column Name: LIMIT

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
SCB_SUPP
DEFAULT

Extended Evidence:

Statistics:

Query returned 1 rows

Cause of Failure:

Unexpected values

Instance

Additional values found in failed controls:

DEFAULT

(1.60) 101075 Status of the IDLE-TIME resource parameter set for Oracle profiles (IAM-450)

Passed MEDIUM

(oracle19:1:1621:POHK1API.hk.standardchartered.com) oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_INFRA_SUPP	15
SCB_SUPP	15

Extended Evidence:

Statistics:

Instance

Query returned 2 rows

(1.60) 101075 Status of the IDLE-TIME resource parameter set for Oracle profiles (IAM-450)

Passed MEDIUM

(oracle19:1:1621:POHK2CCD.hk.standardchartered.com) oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

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

> **PROFILE** LIMIT SCB_SUPP 15

Extended Evidence:

Statistics:

Query returned 1 rows

(1.61) 101101 Ensure 'EXECUTE_CATALOG_ROLE' Is Revoked from Unauthorized 'GRANTEE' (CIS-62)(oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

Passed HIGH

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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 ('SOLTXPLAIN')

Expected any of the selected values below:

Set status to PASS if no data found

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1,61) 101101 Ensure 'EXECUTE CATALOG ROLE' Is Revoked from Unauthorized 'GRANTEE' **Passed HIGH** (CIS-62)(oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

oracle19:1:1621:POHK3CCD.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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:

(1.61) 101101 Ensure 'EXECUTE CATALOG ROLE' Is Revoked from Unauthorized 'GRANTEE' **Passed HIGH** (CIS-62)(oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(1.61) 101101 Ensure 'EXECUTE_CATALOG_ROLE' Is Revoked from Unauthorized 'GRANTEE' **Passed HIGH** (CIS-62)(oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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

(1.61) 101101 Ensure 'EXECUTE_CATALOG_ROLE' Is Revoked from Unauthorized 'GRANTEE' **Passed HIGH**

(CIS-62)(oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

oracle19:1:1621:POHK4CCD.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.61) 101101 Ensure 'EXECUTE_CATALOG_ROLE' Is Revoked from Unauthorized 'GRANTEE' (CIS-62)(oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Passed HIGH

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(1.61) 101101 Ensure 'EXECUTE_CATALOG_ROLE' Is Revoked from Unauthorized 'GRANTEE' **Passed** HIGH (CIS-62)(oracle19:1:1621:POHK1API.hk.standardchartered.com)

oracle19:1:1621:POHK1API.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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:

DBOUERY:

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

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.61) 101101 Ensure 'EXECUTE_CATALOG_ROLE' Is Revoked from Unauthorized 'GRANTEE' HIGH **Passed**

(CIS-62)(oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

oracle19:1:1621:POHK2CCD.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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:

DBOUERY: 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

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.62) 101103 Ensure 'SELECT_CATALOG_ROLE' Is Revoked from Unauthorized 'GRANTEE'(CIS-61) Passed **MEDIUM** (oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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', 'GCB_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

(1.62) 101103 Ensure 'SELECT_CATALOG_ROLE' Is Revoked from Unauthorized 'GRANTEE'(CIS-61) Passed **MEDIUM** (oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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:

Ouery returned 0 rows

(1.62) 101103 Ensure 'SELECT_CATALOG_ROLE' Is Revoked from Unauthorized 'GRANTEE'(CIS-61) Passed **MEDIUM** (oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

oracle19:1:1621:POHK4CCD.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(1.62) 101103 Ensure 'SELECT_CATALOG_ROLE' Is Revoked from Unauthorized 'GRANTEE'(CIS-61) Passed **MEDIUM** (oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

Ensure 'SELECT CATALOG ROLE' Is Revoked from Unauthorized 'GRANTEE' (CIS-61)

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

Scan Parameters:

DBOUERY: SELECT GRANTEE, GRANTED_ROLE FROM DBA_ROLE_PRIVS

WHERE GRANTEE, GRANTEE, TO BE 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

(1.62) 101103 Ensure 'SELECT_CATALOG_ROLE' Is Revoked from Unauthorized 'GRANTEE'(CIS-61) Passed MEDIUM (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Instance oracle 19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 'FATROL%'

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

Set status to PASS if no data found

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.62) 101103 Ensure 'SELECT_CATALOG_ROLE' Is Revoked from Unauthorized 'GRANTEE'(CIS-61) Passed **MEDIUM** (oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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

(1.62) 101103 Ensure 'SELECT_CATALOG_ROLE' Is Revoked from Unauthorized 'GRANTEE'(CIS-61) Passed **MEDIUM** (oracle19:1:1621:POHK1API.hk.standardchartered.com)

oracle19:1:1621:POHK1API.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(1.62) 101103 Ensure 'SELECT_CATALOG_ROLE' Is Revoked from Unauthorized 'GRANTEE'(CIS-61) Passed **MEDIUM** (oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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) **Passed** HIGH (oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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')

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

Set status to PASS if no data found

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

No data found

Extended Evidence:

Statistics:

Instance

Query returned 0 rows

(1.63) 101107 Ensure 'CREATE LIBRARY' Is Revoked from Unauthorized 'GRANTEE'(CIS-57)

Passed HIGH

(oracle19:1:1621:POHK3CCD.hk.standardchartered.com) oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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:

DBOUERY: SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS

WHERE PRIVILEGE FROM DBA_STS_TRYS
WHERE PRIVILEGE='CREAT'E 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

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.63) 101107 Ensure 'CREATE LIBRARY' Is Revoked from Unauthorized 'GRANTEE'(CIS-57) **HIGH Passed**

(oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

oracle19:1:1621:POHK4CCD.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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')

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

Set status to PASS if no data found

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.63) 101107 Ensure 'CREATE LIBRARY' Is Revoked from Unauthorized 'GRANTEE'(CIS-57)

Passed HIGH

(oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

oracle19:1:1621:POHK5CCD.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

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

No data found

Extended Evidence:

Statistics:

Instance

Query returned 0 rows

(1.63) 101107 Ensure 'CREATE LIBRARY' Is Revoked from Unauthorized 'GRANTEE'(CIS-57)

Passed HIGH

(oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

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

oracle19:1:1621:POHK1CAT.hk.standardchartered.com

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

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

No data found

Extended Evidence:

Statistics:

Instance

Query returned 0 rows

(1.63) 101107 Ensure 'CREATE LIBRARY' Is Revoked from Unauthorized 'GRANTEE'(CIS-57)

Passed HIGH

(oracle19:1:1621:POHK1CCD.hk.standardchartered.com) oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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')

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

Set status to PASS if no data found

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

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.hk.standardchartered.com)

Passed HIGH

HIGH

oracle19:1:1621:POHK1API.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

DBOUERY: SELECT GRANTEE, PRIVILEGE FROM DBA SYS PRIVS

WHERE PRIVILEGE FROM DBA_SIS_INVS
WHERE PRIVILEGE='CREAT'E 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

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.63) 101107 Ensure 'CREATE LIBRARY' Is Revoked from Unauthorized 'GRANTEE'(CIS-57) **Passed**

(oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

oracle19:1:1621:POHK2CCD.hk.standardchartered.com Instance Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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) **HIGH Passed** (oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(1.64) 101108 Ensure 'CREATE ANY LIBRARY' Is Revoked from Unauthorized 'GRANTEE'(CIS-56) **Passed HIGH** (oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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');

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

Set status to PASS if no data found

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.64) 101108 Ensure 'CREATE ANY LIBRARY' Is Revoked from Unauthorized 'GRANTEE'(CIS-56) **Passed** HIGH (oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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:

Instance

(1.64) 101108 Ensure 'CREATE ANY LIBRARY' Is Revoked from Unauthorized 'GRANTEE'(CIS-56) (oracle19:1:1621:POHK5CCD.hk.standardchartered.com) **Passed HIGH**

oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

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

No data found

Extended Evidence:

Statistics:

Instance

Query returned 0 rows

(1.64) 101108 Ensure 'CREATE ANY LIBRARY' Is Revoked from Unauthorized 'GRANTEE'(CIS-56) **Passed** HIGH

(oracle19:1:1621:POHK1CAT.hk.standardchartered.com) oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.64) 101108 Ensure 'CREATE ANY LIBRARY' Is Revoked from Unauthorized 'GRANTEE'(CIS-56) Passed HIGH

(oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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');

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

Set status to PASS if no data found

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

No data found

Extended Evidence:

Statistics:

Instance

Query returned 0 rows

(1.64) 101108 Ensure 'CREATE ANY LIBRARY' Is Revoked from Unauthorized 'GRANTEE'(CIS-56) **Passed HIGH**

(oracle19:1:1621:POHK1API.hk.standardchartered.com) oracle 19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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

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

Scan Parameters:

DBOUERY:

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

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.64) 101108 Ensure 'CREATE ANY LIBRARY' Is Revoked from Unauthorized 'GRANTEE'(CIS-56) **Passed HIGH** (oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

oracle19:1:1621:POHK2CCD.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:POHK4CCD.hk.standardchartered.com)

Passed HIGH

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

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

(1.65) 101109 Ensure 'ALTER SYSTEM' Is Revoked from Unauthorized 'GRANTEE'(CIS-55) (oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Passed

HIGH

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

ORACLE_MAINTAINED='Y') AND GRANTEE NOT IN (SELECT ROLE FROM CDB_ROLES WHERE ORACLE_MAINTAINED='Y')

and grantee not in ('GGADMIN')

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

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:POHK1RCT.hk.standardchartered.com)

Passed

HIGH

oracle19:1:1621:POHK1RCT.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

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:

Instance

Query returned 0 rows

(1.65) 101109 Ensure 'ALTER SYSTEM' Is Revoked from Unauthorized 'GRANTEE'(CIS-55)

Passed HIGH

(oracle19:1:1621:POHK3CCD.hk.standardchartered.com) oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

VHERE

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:

Instance

Query returned 0 rows

(1.65) 101109 Ensure 'ALTER SYSTEM' Is Revoked from Unauthorized 'GRANTEE'(CIS-55)

Passed HIGH

(oracle19:1:1621:POHK5CCD.hk.standardchartered.com) oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

VHERE

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

(1.65) 101109 Ensure 'ALTER SYSTEM' Is Revoked from Unauthorized 'GRANTEE'(CIS-55)

Passed HIGH

(oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

ORACLE_MAINTAINED='Y') AND GRANTEE NOT IN (SELECT ROLE FROM CDB_ROLES WHERE ORACLE_MAINTAINED='Y') and grantee not in ('GGADMIN')

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

Set status to PASS if no data found

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

No data found

Extended Evidence:

Statistics:

Instance

Query returned 0 rows

(1.65) 101109 Ensure 'ALTER SYSTEM' Is Revoked from Unauthorized 'GRANTEE'(CIS-55)

Passed HIGH

(oracle19:1:1621:POHK1API.hk.standardchartered.com)

oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

ORACLE_MAINTAINED='Y') AND GRANTEE NOT IN (SELECT ROLE FROM CDB_ROLES WHERE ORACLE_MAINTAINED='Y')

and grantee not in ('GGADMIN')

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

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:POHK2CCD.hk.standardchartered.com)

HIGH **Passed**

oracle19:1:1621:POHK2CCD.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

Instance

Query returned 0 rows

(1.66) 101110 Ensure 'BECOME USER' Is Revoked from Unauthorized 'GRANTEE'(CIS-53)

HIGH **Passed**

(oracle19:1:1621:POHK4CCD.hk.standardchartered.com) oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

Instance

Query returned 0 rows

(1.66) 101110 Ensure 'BECOME USER' Is Revoked from Unauthorized 'GRANTEE'(CIS-53)

Passed HIGH

(oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(1.66) 101110 Ensure 'BECOME USER' Is Revoked from Unauthorized 'GRANTEE'(CIS-53)

HIGH Passed

(oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

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

No data found

Extended Evidence:

Statistics:

Instance

Query returned 0 rows

(1.66) 101110 Ensure 'BECOME USER' Is Revoked from Unauthorized 'GRANTEE' (CIS-53)

oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Passed HIGH

(oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

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

No data found

Extended Evidence:

Statistics:

Instance

Query returned 0 rows

(1.66) 101110 Ensure 'BECOME USER' Is Revoked from Unauthorized 'GRANTEE' (CIS-53)

Passed HIGH

(oracle19:1:1621:POHK5CCD.hk.standardchartered.com) oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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')

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

Set status to PASS if no data found

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

No data found

Extended Evidence:

Statistics:

Instance

Query returned 0 rows

(1.66) 101110 Ensure 'BECOME USER' Is Revoked from Unauthorized 'GRANTEE'(CIS-53) (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

HIGH **Passed**

oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

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

No data found

Extended Evidence:

Statistics:

Instance

Query returned 0 rows

(1.66) 101110 Ensure 'BECOME USER' Is Revoked from Unauthorized 'GRANTEE' (CIS-53)

Passed HIGH

(oracle19:1:1621:POHK1API.hk.standardchartered.com) oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

SELECT GRANTEE, PRIVILEGE, CON_ID DBQUERY:

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:

Instance

Query returned 0 rows

(1.66) 101110 Ensure 'BECOME USER' Is Revoked from Unauthorized 'GRANTEE'(CIS-53)

HIGH **Passed**

(oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

Instance

Ouery returned 0 rows

(1.67) 101112 Ensure 'AUDIT SYSTEM' Is Revoked from Unauthorized 'GRANTEE'(CIS-51)

oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Passed HIGH

(oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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

(1.67) 101112 Ensure 'AUDIT SYSTEM' Is Revoked from Unauthorized 'GRANTEE'(CIS-51) (oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Passed HIGH

oracle19:1:1621:POHK1CCD.hk.standardchartered.com Instance

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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

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

Scan Parameters:

DBOUERY: 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

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

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:POHK1RCT.hk.standardchartered.com)

HIGH Passed

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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

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

No data found

Extended Evidence:

Statistics:

Instance

Query returned 0 rows

(1.67) 101112 Ensure 'AUDIT SYSTEM' Is Revoked from Unauthorized 'GRANTEE'(CIS-51)

HIGH Passed

(oracle19:1:1621:POHK3CCD.hk.standardchartered.com) oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

DBOUERY: 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');

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

Set status to PASS if no data found

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

No data found

Extended Evidence:

Statistics:

Instance

Query returned 0 rows

(1.67) 101112 Ensure 'AUDIT SYSTEM' Is Revoked from Unauthorized 'GRANTEE'(CIS-51)

Passed HIGH

(oracle19:1:1621:POHK5CCD.hk.standardchartered.com) oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

SELECT GRANTEE, FAINTEEGE, COIN_ID
FROM COB_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');

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

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)

Passed HIGH

(oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

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

No data found

Extended Evidence:

Statistics:

Instance

Query returned 0 rows

(1.67) 101112 Ensure 'AUDIT SYSTEM' Is Revoked from Unauthorized 'GRANTEE'(CIS-51)

Passed HIGH

(oracle19:1:1621:POHK1API.hk.standardchartered.com) oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

Instance

Query returned 0 rows

(1.67) 101112 Ensure 'AUDIT SYSTEM' Is Revoked from Unauthorized 'GRANTEE'(CIS-51)

HIGH **Passed**

(oracle19:1:1621:POHK2CCD.hk.standardchartered.com) oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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) **MEDIUM** (oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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 'GGADM%' and GRANTEE not like 'APEX%' and GRANTEE not like 'GGMON%' and GRANTEE not

'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)

No data found

Extended Evidence:

Statistics:

Ouery returned 0 rows

(1.68) 101113 Ensure 'SELECT ANY DICTIONARY' Is Revoked from Unauthorized 'GRANTEE'(cis-49) **MEDIUM** (oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

oracle19:1:1621:POHK1CCD.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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

'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

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.68) 101113 Ensure 'SELECT ANY DICTIONARY' Is Revoked from Unauthorized 'GRANTEE'(cis-49) Passed **MEDIUM** (oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

oracle19:1:1621:POHK1RCT.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

DBOUERY: 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

'PERF_MON%' and GRANTEE not like 'SCB_PERFSTAT%' and GRANTEE not like 'SPLEX%' and GRANTEE not like 'SQLT%'

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

Set status to PASS if no data found

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.68) 101113 Ensure 'SELECT ANY DICTIONARY' Is Revoked from Unauthorized 'GRANTEE'(cis-49) Passed **MEDIUM** (oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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', 'DBARO', 'DBARO', '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 'PERF_MON%' and GRANTEE not like 'SCB_PERFSTAT%' and GRANTEE not like 'SPLEX%' and GRANTEE not like 'SQLT%'

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

Set status to PASS if no data found

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.68) 101113 Ensure 'SELECT ANY DICTIONARY' Is Revoked from Unauthorized 'GRANTEE'(cis-49) Passed **MEDIUM** (oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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

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

Scan Parameters:

DBOUERY:

SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS WHERE PRIVILEGE='SELECT ANY DICTIONARY' AND GRANTEE NOT IN (SELECT USERNAME FROM DBA_USERS WHERE 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 'GCDC's and GRANTEE not like 'GGADM's and GRANTEE not like 'GGMON's and GRANTEE not like 'GGMON's and GRANTEE not like 'APEX's and GRANTEE not like 'GGMON's and GRANTEE not like 'GMON's and GRANTEE not like 'GMON's and GRANTEE not like 'GMON's and GRANTEE NOT AN

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)

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.68) 101113 Ensure 'SELECT ANY DICTIONARY' Is Revoked from Unauthorized 'GRANTEE'(cis-49) Passed **MEDIUM** (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

DBOUERY:

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 'WCDCK' and GRANTEE not
like 'GGADM%' and GRANTEE not like 'PATROLK' and GRANTEE not like 'APEX%' and GRANTEE not like 'GGMON%' and GRANTEE not

'PERF_MON%' and GRANTEE not like 'SCB_PERFSTAT%' and GRANTEE not like 'SPLEX%' and GRANTEE not like 'SQLT%'

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

Set status to PASS if no data found

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.68) 101113 Ensure 'SELECT ANY DICTIONARY' Is Revoked from Unauthorized 'GRANTEE'(cis-49) **MEDIUM Failed** (oracle19:1:1621:POHK1API.hk.standardchartered.com)

oracle19:1:1621:POHK1API.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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:

DBOUERY:

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 COSENIAMIE FROM DBA_COSENS 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 'GGADM' and GRANTEE not like 'GDADM' and GD

'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

(1.68) 101113 Ensure 'SELECT ANY DICTIONARY' Is Revoked from Unauthorized 'GRANTEE'(cis-49) Passed **MEDIUM** (oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

oracle19:1:1621:POHK2CCD.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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 'GGADM' and GRANTEE not like 'PATROL', 'and GRANTEE not like 'APEX' and GRANTEE not like 'GGMON' and GRANTEE not

'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)

No data found

Extended Evidence:

Statistics:

Instance

Query returned 0 rows

(1.69) 101115 Ensure 'ALL' Is Revoked from Unauthorized 'GRANTEE' on 'AUD\$'(CIS-42)

Passed HIGH

(oracle19:1:1621:POHK4CCD.hk.standardchartered.com) oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

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

No data found

Extended Evidence:

Statistics:

Instance

Query returned 0 rows

(1.69) 101115 Ensure 'ALL' Is Revoked from Unauthorized 'GRANTEE' on 'AUD\$'(CIS-42)

HIGH **Passed**

(oracle19:1:1621:POHK1CCD.hk.standardchartered.com) oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

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

No data found

Extended Evidence:

Statistics:

Instance

Query returned 0 rows

(1.69) 101115 Ensure 'ALL' Is Revoked from Unauthorized 'GRANTEE' on 'AUD\$'(CIS-42) (oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Passed HIGH

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

SELECT GRANTEE, PRIVILEGE, CON_ID DBQUERY:

FROM CDB_TAB_PRIVS A WHERE TABLE_NAME='AUD\$' AND OWNER = 'SYS' and grantee not in('DELETE_CATALOG_ROLE', 'SECURITY_ADMIN');

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

Set status to PASS if no data found

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

Instance

(1.69) 101115 Ensure 'ALL' Is Revoked from Unauthorized 'GRANTEE' on 'AUD\$'(CIS-42)

Passed HIGH

(oracle19:1:1621:POHK1CAT.hk.standardchartered.com) oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

Instance

Query returned 0 rows

(1.69) 101115 Ensure 'ALL' Is Revoked from Unauthorized 'GRANTEE' on 'AUD\$'(CIS-42)

oracle19:1:1621:POHK1API.hk.standardchartered.com

Passed HIGH

(oracle19:1:1621:POHK1API.hk.standardchartered.com)

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

Instance

Query returned 0 rows

(1.69) 101115 Ensure 'ALL' Is Revoked from Unauthorized 'GRANTEE' on 'AUD\$'(CIS-42) (oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

oracle19:1:1621:POHK5CCD.hk.standardchartered.com

HIGH Passed

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

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

No data found

Extended Evidence:

Statistics:

Instance

Query returned 0 rows

(1.69) 101115 Ensure 'ALL' Is Revoked from Unauthorized 'GRANTEE' on 'AUD\$'(CIS-42)

HIGH Passed

(oracle19:1:1621:POHK2CCD.hk.standardchartered.com) oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

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

No data found

Extended Evidence:

Statistics:

Instance

Query returned 0 rows

(1.69) 101115 Ensure 'ALL' Is Revoked from Unauthorized 'GRANTEE' on 'AUD\$'(CIS-42)

Passed HIGH

(oracle19:1:1621:POHK1RCT.hk.standardchartered.com) oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

HIGH (1.70) 101140 Status of the 'REMOTE_LISTENER' setting via SQL query (CIS-8)(oracle19:1:1621: **Passed** POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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: $select 'N' from \ v\$system_parameter \ sp \ , v\$system_parameter \ cd \ where \ upper(sp.name) = 'REMOTE_LISTENER' \ and \ lower(cd.name) = 'cluster_database' \ and \ cd.value = 'TRUE' \ and \ sp.value \ is \ null$

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

(1.70) 101140 Status of the 'REMOTE_LISTENER' setting via SQL query (CIS-8)(oracle19:1:1621: **HIGH** Passed POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

 $select 'N' from \ v system_parameter \ sp \ , \ v system_parameter \ cd \ where \ upper (sp.name) = 'REMOTE_LISTENER' \ and \ lower (cd.name) = 'cluster_database' \ and \ cd.value = 'TRUE' \ and \ sp.value \ is \ null$ DBQUERY:

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

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

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: **Passed HIGH** POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

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

select. N Trom v\$system_parameter sp , v\$system_parameter cd where upper (sp.name)= 'REMOTE_LISTENER' and lower (cd.name)= 'cluster_database' and cd.value= 'ROE and sp.value is numerically 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

Oracle ATOS - 20240806 page 555

DBOUERY:

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

Set status to PASS if no data found

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

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: HIGH **Passed** POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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

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

Scan Parameters:

 $select 'N' from \ v \\ system_parameter \ sp \ , \ v \\ system_parameter \ cd \ where \ upper (sp.name) \\ = 'REMOTE_LISTENER' \ and \ lower (cd.name) \\ = 'cluster_database' \ and \ cd.value \\ = 'TRUE' \ and \ sp.value \ is \ null$ DBOUERY:

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

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

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: **Passed** HIGH POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

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

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

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

HIGH (1.70) 101140 Status of the 'REMOTE_LISTENER' setting via SQL query (CIS-8)(oracle19:1:1621: **Passed** POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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: $select 'N' from \ v\$system_parameter \ sp \ , v\$system_parameter \ cd \ where \ upper(sp.name) = 'REMOTE_LISTENER' \ and \ lower(cd.name) = 'cluster_database' \ and \ cd.value = 'TRUE' \ and \ sp.value \ is \ null$

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

(1.70) 101140 Status of the 'REMOTE_LISTENER' setting via SQL query (CIS-8)(oracle19:1:1621: **HIGH** Passed POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

 $select 'N' from \ v system_parameter \ sp \ , \ v system_parameter \ cd \ where \ upper (sp.name) = 'REMOTE_LISTENER' \ and \ lower (cd.name) = 'cluster_database' \ and \ cd.value = 'TRUE' \ and \ sp.value \ is \ null$ DBQUERY:

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

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

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: **Passed HIGH** POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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:

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 DBOUERY:

select. N Trom v\$system_parameter sp , v\$system_parameter cd where upper (sp.name)= 'REMOTE_LISTENER' and lower (cd.name)= 'cluster_database' and cd.value= 'ROE and sp.value is numerically 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:POHK4CCD. Passed HIGH hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(1.71) 101149 Status of the existence of the sys.user\$mig table(CIS-33)(oracle19:1:1621:POHK1CCD. Passed HIGH hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(1.71) 101149 Status of the existence of the sys.user\$mig table(CIS-33)(oracle19:1:1621:POHK3CCD. Passed HIGH hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(1.71) 101149 Status of the existence of the sys.user\$mig table(CIS-33)(oracle19:1:1621:POHK1CAT. Passed HIGH hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(1.71) 101149 Status of the existence of the sys.user\$mig table(CIS-33)(oracle19:1:1621:POHK1API. Passed HIGH hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(1.71) 101149 Status of the existence of the sys.user\$mig table(CIS-33)(oracle19:1:1621:POHK5CCD. Passed HIGH hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(1.71) 101149 Status of the existence of the sys.user\$mig table(CIS-33)(oracle19:1:1621:POHK2CCD. Passed HIGH hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(1.71) 101149 Status of the existence of the sys.user\$mig table(CIS-33)(oracle19:1:1621:POHK1RCT. Passed HIGH hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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: Passed MEDIUM

POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

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

POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

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

POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

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

POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

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

POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

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

POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(1.72) 101150 List of public database links present in the database(CIS-34)(oracle19:1:1621: Failed MEDIUM POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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'

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

Expected any of the selected values below:

Set status to PASS if no data found

Actual

Lust Opunicu. 30/04/2024 at 30:31:33 f iii (Siii 1 + 3330)		
DB_LINK	ноѕт	CON_ID
NG_OLAP.HK.STANDARDCHARTERED.COM	(DESCRIPTION_LIST=(LOAD_BALANCE=off) (FAILOVER=on) (DESCRIPTION=(ADDRESS_LIST=(ADDRESS_	

NO_OLA I III. SI NIVINI DOI I III. LEKLI. CON	(FAILOVER=on) (DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP) (HOST=HKLPDPS2B1A-SCAN.HK.STANDARDCHARTERED.COM) (PORT=1622))) (CONNECT_DATA=(SERVICE_NAME=svc_pohk5ccd_ngw_gl_bat.hk.standardchartered.com))) (DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP) (HOST=HKLPDSS2B1B-SCAN.HK.STANDARDCHARTERED.COM) (PORT=1622))) (CONNECT_DATA=(SERVICE_NAME=svc_pohk5ccd_ngw_gl_bat.hk.standardchartered.com))))	
CADM.HK.STANDARDCHARTERED.COM	(DESCRIPTION_LIST=(LOAD_BALANCE=off) (FAILOVER=on) (DESCRIPTION=(ADDRESS_LIST=(ADDRESS-=(PROTOCOL=TCP) (HOST=HKLPDPS2B1A-SCAN.HK.STANDARDCHARTERED.COM) (PORT=1622))) (CONNECT_DATA=(SERVICE_NAME=svc_pohk4ccd_cad_gl_onl.hk.standardchartered.com))) (DESCRIPTION=(ADDRESS_LIST=(ADDRESS-=(PROTOCOL=TCP) (HOST=HKLPDPS2B1B-SCAN.HK.STANDARDCHARTERED.COM) (PORT=1622))) (CONNECT_DATA=(SERVICE_NAME=svc_pohk4ccd_cad_gl_bat.hk.standardchartered.com))))	4
OLAP.HK.STANDARDCHARTERED.COM	(DESCRIPTION_LIST=(LOAD_BALANCE=off) (FAILOVER=on) (DESCRIPTION=(ADDRESS_LIST=(ADDRESS-EPROTOCOL=TCP) (HOST=HKLPDPS2B1A-SCAN_HK.STANDARDCHARTERED.COM) (PORT=1622))) (CONNECT_DATA=(SERVICE_NAME=svc_pohk5cd_ngw_gl_onl.hk.standardchartered.com))) (DESCRIPTION=(ADDRESS_LIST=(ADDRESS-	4

OLAP.HK.STANDARDCHARTERED.COM	=(PROTOCOL=TCP) (HOST=HKLPDPS2B1B-SCAN.HK.STANDARDCHARTERED.COM) (PORT=1622))) (CONNECT_DATA=(SERVICE_NAME=svc_pohk5ccd_ngw_gl_bat.hk. standardchartered.com))))	4
QL_PRDHK_1.HK.STANDARDCHARTERED. COM	(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP) (HOST = 10.20.231.94) (PORT = 1577)) (CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = al_prdbk)))	4

Extended Evidence:

Statistics:

Query returned 4 rows

(1.72) 101150 List of public database links present in the database(CIS-34)(oracle19:1:1621: Passed MEDIUM POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

DBOUERY: 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.hk. Patandardchartered.com)

Passed HIGH

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.

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

(1.73) 1051 Status of the 'os_roles=' setting in init.ora(oracle19:1:1621:POHK4CCD.hk. standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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+05	30)	
	FALSE		
Extended E	Evidence:		
NAME		VALUE	
os_roles		FALSE	
os_roles		FALSE	
os_roles		FALSE	

(1.73) 1051 Status of the 'os_roles=' setting in init.ora(oracle19:1:1621:POHK5CCD.hk. standardchartered.com)

Passed HIGH

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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+05	30)	
	FALSE		
Extended E	vidence:		
NAME		VALUE	
os_roles		FALSE	
os_roles		FALSE	
os_roles		FALSE	

(1.73) 1051 Status of the 'os_roles=' setting in init.ora(oracle19:1:1621:POHK1RCT.hk. standardchartered.com)

Passed HIGH

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

Oracle_ATOS - 20240806 page 565

HIGH

Passed

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+05	530)
	FALSE	
Extended E	Evidence:	
NAME		VALUE
os_roles		FALSE
os_roles		FALSE
os roles		FALSE

(1.73) 1051 Status of the 'os_roles=' setting in init.ora(oracle19:1:1621:POHK1CAT.hk. standardchartered.com)

Passed HIGH

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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+05	30)	
	FALSE		
Extended E	ividence:		
NAME		VALUE	
os_roles		FALSE	
os_roles		FALSE	
os_roles		FALSE	

(1.73) 1051 Status of the 'os_roles=' setting in init.ora(oracle19:1:1621:POHK1CCD.hk. standardchartered.com)

Passed HIGH

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(1.73) 1051 Status of the 'os_roles=' setting in init.ora(oracle19:1:1621:POHK2CCD.hk. standardchartered.com)

Passed HIGH

1 10 1 1001 DOLLY200

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(1.73) 1051 Status of the 'os_roles=' setting in init.ora(oracle19:1:1621:POHK3CCD.hk. standardchartered.com)

Passed

HIGH

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

Actual

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

FALSE

Extended Evidence:

NAME

os_roles

os_roles

os_roles

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:POHK1CCD.hk.standardchartered.com)

Passed

HIGH

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 r

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

(1.74) 101064 Status of instance configuration (alter database / alter system) are captured in the security events(oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

Passed HIGH

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(1.74) 101064 Status of instance configuration (alter database / alter system) are captured in the security events(oracle19:1:1621:POHK1CAT.hk.standardchartered.com) **HIGH** Passed

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

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) DBQUERY:

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

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

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE
SCB_AUDIT_DDL_POLICY	ALTER DATABASE	SYSTEM PRIVILEGE
SCB_AUDIT_DDL_POLICY	ALTER SYSTEM	SYSTEM PRIVILEGE
SCB AUDIT DDL POLICY	ALTER SYSTEM	STANDARD ACTION

Extended Evidence:

Statistics:

Query returned 3 rows

(1.74) 101064 Status of instance configuration (alter database / alter system) are captured in the **HIGH Passed** security events(oracle19:1:1621:POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

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) DBQUERY:

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

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

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

Extended Evidence:

Statistics:

(1.74) 101064 Status of instance configuration (alter database / alter system) are captured in the **Passed HIGH** security events(oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Passed Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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:

*

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) DBQUERY:

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

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

> 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

(1.74) 101064 Status of instance configuration (alter database / alter system) are captured in the security events(oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

HIGH Passed

oracle19:1:1621:POHK4CCD.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

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) DBQUERY:

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

(1.74) 101064 Status of instance configuration (alter database / alter system) are captured in the security events(oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

Passed

HIGH

oracle19:1:1621:POHK2CCD.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

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) DBOUERY:

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

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

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

(1.74) 101064 Status of instance configuration (alter database / alter system) are captured in the **Passed HIGH** security events(oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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:

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) DBQUERY:

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

MEDIUM (2.1) 101311 Ensure all Users are authenticated before access to an information System(IAM-340) **Failed** (oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Instance oracle 19:1:1621:POHK1CCD.hk.standardchartered.com

Failed **Previous Status**

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')

is contained in regular expression list **Expected**

DB Column Name: AUTHENTICATION_TYPE

^PASSWORD\$

OR, any of the selected values below:

Set status to PASS if no data found

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

AUTHENTICATION_TYPE

EXTERNAL PASSWORD

Extended Evidence:

Statistics:

Query returned 2 rows

Cause of Failure:

Unexpected values

Additional values found in failed controls:

EXTERNAL

(2.1) 101311 Ensure all Users are authenticated before access to an information System(IAM-340) **Failed MEDIUM** (oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

oracle19:1:1621:POHK3CCD.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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:

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

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

EXTERNAL

PASSWORD

Extended Evidence:

Statistics:

Query returned 2 rows

Cause of Failure:

Unexpected values

Additional values found in failed controls:

EXTERNAL

(2.1) 101311 Ensure all Users are authenticated before access to an information System(IAM-340) **MEDIUM Passed** (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

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

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

(2.1) 101311 Ensure all Users are authenticated before access to an information System(IAM-340) **MEDIUM Passed** (oracle19:1:1621:POHK1API.hk.standardchartered.com)

oracle19:1:1621:POHK1API.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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',

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

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

AUTHENTICATION_TYPE

PASSWORD

Extended Evidence:

Statistics:

(2.1) 101311 Ensure all Users are authenticated before access to an information System(IAM-340) Failed MEDIUM (oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

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

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

OR, any of the selected values below:

^PASSWORD\$

PASSWORD

Set status to PASS if no data found

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

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

AUTHENTICATION_TYPE

EXTERNAL

Extended Evidence:

Statistics:

Query returned 2 rows

Cause of Failure:

Unexpected values found in failed controls:

EXTERNAL

(2.1) 101311 Ensure all Users are authenticated before access to an information System(IAM-340) Failed MEDIUM (oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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

EXTERNAL PASSWORD

Statistics:

Query returned 2 rows

Cause of Failure:

Unexpected values

Additional values found in failed controls:

EXTERNAL

(2.1) 101311 Ensure all Users are authenticated before access to an information System(IAM-340) Failed **MEDIUM** (oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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:

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

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

EXTERNAL PASSWORD

Extended Evidence:

Statistics:

Query returned 2 rows

Cause of Failure:

Unexpected values

Additional values found in failed controls:

EXTERNAL

(2.1) 101311 Ensure all Users are authenticated before access to an information System(IAM-340) **MEDIUM Failed** (oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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

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

AUTHENTICATION_TYPE

EXTERNAL PASSWORD

Extended Evidence:

Statistics:

Query returned 2 rows

Cause of Failure:

Unexpected values

Instance

Additional values found in failed controls:

EXTERNAL

(2.2) 101319 Status of 'DBA_%' granted to grantees (direct and indirect grants)(CIS-43)

Passed HIGH

(oracle19:1:1621:POHK1CCD.hk.standardchartered.com) oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

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%' DBQUERY:

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

(2.2) 101319 Status of 'DBA_%' granted to grantees (direct and indirect grants)(CIS-43) (oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

Passed HIGH

oracle19:1:1621:POHK3CCD.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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:

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', 'CCS_SCAN', 'SECADMIN', 'SCB_ADMIN', '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%' DBQUERY:

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

Set status to PASS if no data found

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

No data found

Extended Evidence:

Statistics:

Instance

Query returned 0 rows

(2.2) 101319 Status of 'DBA_%' granted to grantees (direct and indirect grants)(CIS-43)

HIGH **Passed**

(oracle19:1:1621:POHK1CAT.hk.standardchartered.com) oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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:

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 DBOUERY:

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', 'GRANTEE NOT IN ('CCS_SCAN', 'SECADMIN', 'SCB_ADMIN', 'GRANTEE', 'ORDS_ADMIN', 'ORDS_METADATA') AND GRANTEE NOT like '%CDC%' and GRANTEE not like 'PATROL%' and GRANTEE not like 'APEX%'

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

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

(2.2) 101319 Status of 'DBA_%' granted to grantees (direct and indirect grants)(CIS-43) (oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

Passed HIGH

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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:

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%' DBOUERY:

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

(2.2) 101319 Status of 'DBA_%' granted to grantees (direct and indirect grants)(CIS-43) (oracle19:1:1621:POHK1API.hk.standardchartered.com)

oracle 19:1:1621:POHK1API.hk.standardchartered.com

Previous Status

Instance

Evaluation Date 08/04/2024 at 10:38:34 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:

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', 'GRANTEE NOT IN ('CCS_SCAN', 'SECADMIN', 'META_OZ', 'PUPPETAM', 'ORDS_ADMIN', 'ORDS_METADATA') AND GRANTEE NOT like 'MCDO'' and GRANTEE not like 'PATPOLO'' and GRANTEE not like 'ADEYO'. DBQUERY:

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

(2.2) 101319 Status of 'DBA_%' granted to grantees (direct and indirect grants)(CIS-43)

HIGH **Passed**

HIGH

Passed

(oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

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%' DBQUERY:

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:

Instance

Query returned 0 rows

(2.2) 101319 Status of 'DBA_%' granted to grantees (direct and indirect grants)(CIS-43)

HIGH Passed

(oracle19:1:1621:POHK4CCD.hk.standardchartered.com) oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

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%' DBQUERY:

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

(2.2) 101319 Status of 'DBA_%' granted to grantees (direct and indirect grants)(CIS-43)

Passed HIGH

(oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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:

SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS A WHERE TABLE_NAME LIKE 'DBA_%' AND OWNER = 'SYS' AND GRANTEE DBQUERY:

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%'

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

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:POHK1CCD.hk.standardchartered.com)

Passed

HIGH

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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')

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

Set status to PASS if no data found

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

No data found

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:POHK1CAT.hk.standardchartered.com)

Passed HIGH

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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', 'ORAMED 1', '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

(2.3) 101322 Ensure 'DBA_SYS_PRIVS.%' Is Revoked from Unauthorized 'GRANTEE' with 'ADMIN_OPTION'(CIS-46)(oracle19:1:1621:POHK2CCD.hk.standardchartered.com) **Passed HIGH**

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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

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

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.hk.standardchartered.com)

Passed HIGH

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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

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

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:POHK5CCD.hk.standardchartered.com)

HIGH Passed

oracle19:1:1621:POHK5CCD.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(2.3) 101322 Ensure 'DBA_SYS_PRIVS.%' Is Revoked from Unauthorized 'GRANTEE' with **Passed** 'ADMIN_OPTION'(CIS-46)(oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

HIGH

oracle19:1:1621:POHK4CCD.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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', 'ORAMĒD2', '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

(2.3) 101322 Ensure 'DBA_SYS_PRIVS.%' Is Revoked from Unauthorized 'GRANTEE' with HIGH Passed 'ADMIN_OPTION'(CIS-46)(oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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', 'ORAMED 1', '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

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

Extended Evidence:

Statistics:

Query returned 0 rows

(2.3) 101322 Ensure 'DBA_SYS_PRIVS.%' Is Revoked from Unauthorized 'GRANTEE' with HIGH Passed 'ADMIN_OPTION'(CIS-46)(oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

oracle19:1:1621:POHK3CCD.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.4) 101323 Ensure 'EXEMPT ACCESS POLICY' Is Revoked from Unauthorized 'GRANTEE'(CIS-52) Passed **HIGH** (oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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

(2.4) 101323 Ensure 'EXEMPT ACCESS POLICY' Is Revoked from Unauthorized 'GRANTEE'(CIS-52) **HIGH Passed** (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(2.4) 101323 Ensure 'EXEMPT ACCESS POLICY' Is Revoked from Unauthorized 'GRANTEE'(CIS-52) Passed **HIGH** (oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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:

DBOUERY:

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 (SELECT ROLE FROM CDB ROLES WHERE ORACLE_MAINTAINED=Y) AND GRANTEE NOT IN (SCE_LINK, 'REPO_OWNER)

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

Set status to PASS if no data found

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.4) 101323 Ensure 'EXEMPT ACCESS POLICY' Is Revoked from Unauthorized 'GRANTEE' (CIS-52) **Passed HIGH** (oracle19:1:1621:POHK1API.hk.standardchartered.com)

Instance oracle 19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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

(2.4) 101323 Ensure 'EXEMPT ACCESS POLICY' Is Revoked from Unauthorized 'GRANTEE' (CIS-52) Passed **HIGH** (oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(2.4) 101323 Ensure 'EXEMPT ACCESS POLICY' Is Revoked from Unauthorized 'GRANTEE'(CIS-52) Passed **HIGH** (oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

Instance oracle 19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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

(2.4) 101323 Ensure 'EXEMPT ACCESS POLICY' Is Revoked from Unauthorized 'GRANTEE'(CIS-52) **HIGH Passed** (oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(2.4) 101323 Ensure 'EXEMPT ACCESS POLICY' Is Revoked from Unauthorized 'GRANTEE' (CIS-52) Failed (oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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:

DBOUERY:

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 (SELECT ROLE FROM CDB ROLES WHERE ORACLE_MAINTAINED=Y) AND GRANTEE NOT IN (SCE_LINK, 'REPO_OWNER)

Oracle ATOS - 20240806 page 585

HIGH

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

Set status to PASS if no data found

Actual

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

GRANTEE	PRIVILEGE	CON_ID
GGADMIN	EXEMPT ACCESS POLICY	1
GGADMIN	EXEMPT ACCESS POLICY	3

Extended Evidence:

Statistics:

Query returned 2 rows

(2.5) 101325 Status of '%ANY%' system privilege granted to grantees (direct and indirect grants) **HIGH Passed** (CIS-45)(oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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)

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) **Passed HIGH** (CIS-45)(oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

DBOUERY: SELECT GRANTEE, PRIVILEGE

FROM DBA_SYS_PRIVS WHERE PRIVILEGE LIKE '%ANY%'

AND GRANTEE NOT IN (SELECT USERNAME FROM DBA_USERS WHERE

ORACLE MAINTAINED='Y'

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%'

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

Set status to PASS if no data found

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

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:POHK2CCD.hk.standardchartered.com) **Passed HIGH**

oracle19:1:1621:POHK2CCD.hk.standardchartered.com Instance

Previous Status

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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:

SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS DBOUERY:

WHERE PRĪVILĒGE LIKE '%ANY%'

WHERE PRIVILEGE LIRE '80AN1'8
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',

"SCB_LINK', 'ORACLE', 'ORAMED2', 'PATROL', 'SPATIAL_CSW_ADMIN_USR', 'SPATIAL_WFS_ADMIN_USR', 'PUPPETAM',

"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 'PERF%' and GRANTEE not like 'SCB_PERFSTAT%' and GRANTEE not like 'SPLEX%' and GRANTEE not like 'SQLT%' and GRANTEE not like 'MSYSADM%'

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.hk.standardchartered.com) HIGH Failed

oracle19:1:1621:POHK1API.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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:

SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS DBOUERY:

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 'SCB_PERFSTAT%' and GRANTEE not like 'SPLEX%' and GRANTEE not like 'SOLT%' and GRANTEE not like 'SYSADM%'

not like 'SQLT%' and GRANTEE not like '%SYSADM%

Expected any of the selected values below:

Set status to PASS if no data found

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

> **GRANTEE PRIVILEGE** CC_ITRS SELECT ANY DICTIONARY

Extended Evidence:

Statistics:

Query returned 1 rows

(2.5) 101325 Status of '%ANY%' system privilege granted to grantees (direct and indirect grants) (CIS-45)(oracle19:1:1621:POHK5CCD.hk.standardchartered.com) **Passed** HIGH

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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%'

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

"CROWLED AND THE TOTAL OR AND THE CONTROL OF THE PROPERTY OF THE PROPE

'%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)

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:POHK4CCD.hk.standardchartered.com) Passed HIGH

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 COLE FROM DBA_COLES 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_SSW_ADMIN_USR', 'SPATIAL_WFS_ADMIN_USR', 'PUPPETAM', 'SCB_LINK', 'ORACLE', 'ORAMED2', 'PATROL', 'SPATIAL_CANADATAN', 'ADALASTAN', 'ADALA

'HCVPWDMANID_ROOT', 'HCVPWDMANID,'ORDS_ADMIN') and GRANTEE not like 'WCDC%' 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

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

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) **HIGH** Passed (CIS-45)(oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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:

SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS DBQUERY:

WHERE PRĪVILĒGE LIKE '%ANY%

AND GRANTEE NOT IN (SELECT USERNAME FROM DBA_USERS WHERE ORACLE_MAINTAINED=Y')

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)

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) **Passed HIGH** (CIS-45)(oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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 PRĪVILĒGE LIKE '%ANY%'

AND GRANTEE NOT IN (SELECT USERNAME FROM DBA_USERS WHERE

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', 'DBARO', '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 '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)

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.6) 101326 Status of username and account status granted SELECT ANY TABLE privilege(CIS-50) HIGH (oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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 'APEXM' 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

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

Set status to PASS if no data found

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

No data found

Extended Evidence:

Statistics:

Ouery returned 0 rows

(2.6) 101326 Status of username and account status granted SELECT ANY TABLE privilege(CIS-50) **HIGH** (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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 'WCDC' and GRANTEE not like 'GGADM' and GRANTEE not like 'PATROL', 'AND GRANTEE NOT IN ('GRANTEE NOT IN GRANTEE N 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

(2.6) 101326 Status of username and account status granted SELECT ANY TABLE privilege(CIS-50) Passed **HIGH** (oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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', 'ORARO2', 'ORAMED1', 'GGADMIN', 'SCB_LINK',
'ORACLE', 'ORAMED2', 'PATROL', 'PUPPETAM', 'ORDS, ADMIN') and GRANTEE not like 'GCDC' 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

(2.6) 101326 Status of username and account status granted SELECT ANY TABLE privilege(CIS-50) Passed **HIGH** (oracle19:1:1621:POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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', 'DBARO', 'ORAMED1', 'GRADMIN', 'SCB_ADMIN', 'SCB_LINK',
'ORACLE', 'ORAMED2', 'PATROL', 'PUPPETAM', 'ORDS, ADMIN') and GRANTEE not like 'WCDC', 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

(2.6) 101326 Status of username and account status granted SELECT ANY TABLE privilege(CIS-50) Passed **HIGH** (oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 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 'WCDC' 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

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.6) 101326 Status of username and account status granted SELECT ANY TABLE privilege(CIS-50) HIGH (oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

oracle19:1:1621:POHK4CCD.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.6) 101326 Status of username and account status granted SELECT ANY TABLE privilege(CIS-50) **Passed HIGH** (oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

Instance oracle 19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_MONS'
'AOGEM%' 'AOGEM%'

Expected any of the selected values below:

Set status to PASS if no data found

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.6) 101326 Status of username and account status granted SELECT ANY TABLE privilege(CIS-50) Passed (oracle19:1:1621:POHK3CCD.hk.standardchartered.com) HIGH

oracle19:1:1621:POHK3CCD.hk.standardchartered.com Instance

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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%'

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

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: **Passed** HIGH POHK1RCT.hk.standardchartered.com)

oracle19:1:1621:POHK1RCT.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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

(2.7) 101334 Status of the 'execute any procedure' privilege for user DBSNMP(oracle19:1:1621: HIGH **Passed** POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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

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

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: HIGH Passed POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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'

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

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: **HIGH Passed** POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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'

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

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: Passed HIGH

POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

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

POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

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

POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

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

POHK3CCD.hk.standardchartered.com)

oracle19:1:1621:POHK3CCD.hk.standardchartered.com Instance

Passed Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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:

Instance

Query returned 0 rows

(2.8) 101332 Status of the FAILED_LOGIN_ATTEMPTS resource parameter set in all Oracle profiles **HIGH Passed**

(oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

oracle19:1:1621:POHK1RCT.hk.standardchartered.com

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:

Actual Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) PROFILE||':'||LIMIT DEFAULT:UNLIMITED SCB_STATIC_APP:UNLIMITED SCB_SUPP:3 ORA_STIG_PROFILE:6

Extended Evidence:

Statistics:

Query returned 4 rows

(2.8) 101332 Status of the FAILED_LOGIN_ATTEMPTS resource parameter set in all Oracle profiles Failed HIGH (oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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

SCB_STATIC_APP_PSS:UNLIMITED

SCB_STATIC_APP_ATX:UNLIMITED

SCB_STATIC_APP_PAY:UNLIMITED

SCB_STATIC_APP_ATX_IDLE30:UNLIMITED

SCB_STATIC_APP:UNLIMITED

DEFAULT:UNLIMITED

SCB_APP_CCS:UNLIMITED

ORA_STIG_PROFILE:6

SCB_SUPP:3

SCB_STATIC_APP_CCS:UNLIMITED

Extended Evidence:

Statistics:

Query returned 10 rows

Cause of Failure:

	Additional values found in failed controls:
values	

(2.8) 101332 Status of the FAILED_LOGIN_ATTEMPTS resource parameter set in all Oracle profiles Passed HIGH (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

DEFAULT:UNLIMITED

ORA_STIG_PROFILE:6

SCB_STATIC_APP:UNLIMITED

SCB_SUPP:3

SCB_STATIC_APP_ATX:UNLIMITED

SCB_INFRA_SUPP:3

SCB_INFRA_APP:UNLIMITED

SCB_STATIC_APP_CCS:UNLIMITED

SCB_STATIC_APP_ATX_IDLE30:UNLIMITED

Extended Evidence:

Statistics:

Query returned 9 rows

(2.8) 101332 Status of the FAILED_LOGIN_ATTEMPTS resource parameter set in all Oracle profiles Passed HIGH (oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

DBOUERY: 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

SCB_STATIC_APP:UNLIMITED

SCB_SUPP:3

ORA_STIG_PROFILE:6

SCB_STATIC_APP_PSS:UNLIMITED

SCB_STATIC_APP_NGO:UNLIMITED

DEFAULT:UNLIMITED

SCB_STATIC_APP_WEB:UNLIMITED

SCB_STATIC_APP_NGO_1000:UNLIMITED

Extended Evidence:

Statistics:

Query returned 8 rows

(2.8) 101332 Status of the FAILED_LOGIN_ATTEMPTS resource parameter set in all Oracle profiles **Passed** HIGH (oracle19:1:1621:POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

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

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_STATIC_APP_PSS:UNLIMITED

SCB_STATIC_APP_ATX:UNLIMITED

DEFAULT:UNLIMITED

SCB_INFRA_SUPP:3

SCB_STATIC_APP:UNLIMITED

SCB_INFRA_APP:UNLIMITED

SCB_SUPP:3

Statistics:

Query returned 8 rows

(2.8) 101332 Status of the FAILED_LOGIN_ATTEMPTS resource parameter set in all Oracle profiles Passed HIGH (oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

DEFAULT:UNLIMITED

SCB_STATIC_APP_PSS:UNLIMITED

SCB_INFRA_APP:UNLIMITED

SCB_STATIC_APP:UNLIMITED

SCB_SUPP:3

SCB_STATIC_APP_INF:UNLIMITED

SCB_STATIC_APP_NGW:UNLIMITED

ORA_STIG_PROFILE:6

Extended Evidence:

Statistics:

Query returned 8 rows

(2.8) 101332 Status of the FAILED_LOGIN_ATTEMPTS resource parameter set in all Oracle profiles Passed HIGH (oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

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_STATIC_APP_PSS:UNLIMITED

DEFAUL<u>T:UNLIMITED</u>

SCB_INFRA_APP:UNLIMITED

SCB_STATIC_APP_CAD:UNLIMITED

SCB_STATIC_APP:UNLIMITED

SCB_SUPP:3

Extended Evidence:

Statistics:

Query returned 7 rows

(2.8) 101332 Status of the FAILED_LOGIN_ATTEMPTS resource parameter set in all Oracle profiles **Passed** HIGH (oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

oracle19:1:1621:POHK3CCD.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

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

is contained in regular expression list **Expected**

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

SCB_STATIC_APP:UNLIMITED

SCB_SUPP:3

ORA_STIG_PROFILE:6

SCB_STATIC_APP_PSS:UNLIMITED

SCB_STATIC_APP_QLDSADMIN:UNLIMITED

SCB_STATIC_APP_TDC:UNLIMITED

SCB_STATIC_APP_DS:UNLIMITED

DEFAULT:UNLIMITED SCB_STATIC_APP_TNG:UNLIMITED

Statistics:

Query returned 9 rows

(2.9) 101336 Status of the login & logoff security events for administrators_SLM-010 (oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

Passed HIGH

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

Statistics:

Query returned 60 rows

(2.9) 101336 Status of the login & logoff security events for administrators_SLM-010 (oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

HIGH **Passed**

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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

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

Scan Parameters:

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

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 STANDARD ACTION
SCB_AUDIT_DDL_POLICY	DROP SEQUENCE	STANDARD ACTION STANDARD ACTION
	CREATE SYNONYM	STANDARD ACTION STANDARD ACTION
SCB_AUDIT_DDL_POLICY		
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
	1	1-7-31 11011011

Statistics:

Query returned 60 rows

(2.9) 101336 Status of the login & logoff security events for administrators_SLM-010 (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

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

Passed

HIGH

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	DROP PROFILE	SYSTEM PRIVILEGE
SCB_AUDIT_DDL_POLICY	ALTER PROFILE	SYSTEM PRIVILEGE
SCB_AUDIT_DDL_POLICY	CREATE PROFILE	SYSTEM PRIVILEGE
SCB_AUDIT_DDL_POLICY	ALTER DATABASE	SYSTEM PRIVILEGE
SCB_AUDIT_DDL_POLICY	CREATE ROLE	SYSTEM PRIVILEGE
SCB_AUDIT_DDL_POLICY	CREATE DATABASE LINK	SYSTEM PRIVILEGE
SCB_AUDIT_DDL_POLICY	DROP USER	SYSTEM PRIVILEGE
SCB_AUDIT_DDL_POLICY	ALTER USER	SYSTEM PRIVILEGE
SCB_AUDIT_DDL_POLICY	CREATE USER	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	ALTER SYSTEM	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

	DROP PROCEDURE	STANDARD ACTION
Loop Attracts and Dollars		
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

Statistics:

Query returned 69 rows

(2.9) 101336 Status of the login & logoff security events for administrators_SLM-010 (oracle19:1:1621:POHK2CCD.hk.standardchartered.com) **Passed** HIGH

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

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') DBQUERY:

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 SCB_AUDIT_DDL_POLICY	DROP INDEX	STANDARD ACTION
	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 STANDARD ACTION
SCB_AUDIT_DDL_POLICY	DROP DIRECTORY	STANDARD ACTION 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

Statistics:

(2.9) 101336 Status of the login & logoff security events for administrators_SLM-010 (oracle19:1:1621:POHK1API.hk.standardchartered.com)

Passed HIGH

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

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

Previous Status Passed

*

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

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 symposium list.

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

Statistics:

Query returned 60 rows

(2.9) 101336 Status of the login & logoff security events for administrators_SLM-010 (oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Passed HIGH

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

Statistics:

Query returned 60 rows

(2.9) 101336 Status of the login & logoff security events for administrators_SLM-010 (oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

Passed HIGH

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

POLICY_NAME FI

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

DBQUERY:

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 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 STANDARD ACTION
SCB_AUDIT_DDL_POLICY	CREATE DIRECTORY	STANDARD ACTION STANDARD ACTION
SCB_AUDIT_DDL_POLICY	DROP DIRECTORY	STANDARD ACTION 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

Statistics:

Query returned 60 rows

(2.9) 101336 Status of the login & logoff security events for administrators_SLM-010(oracle19:1:1621: Passed HIGH POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

Statistics:

Query returned 60 rows

(2.10) 101339 Status of the PASSWORD_LOCK_TIME resource parameter set in all Oracle profiles Passed HIGH (oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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
DEFAULT:UNLIMITED
ORA_STIG_PROFILE:UNLIMITED
SCB_SUPP:UNLIMITED
SCB_STATIC_APP:UNLIMITED

Extended Evidence:

Statistics:

Query returned 4 rows

(2.10) 101339 Status of the PASSWORD_LOCK_TIME resource parameter set in all Oracle profiles Passed HIGH (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

DBOUERY: 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

SCB_SUPP:UNLIMITED

DEFAULT:UNLIMITED

SCB_INFRA_SUPP:UNLIMITED

ORA_STIG_PROFILE:UNLIMITED

SCB_STATIC_APP:UNLIMITED

SCB_STATIC_APP_ATX:UNLIMITED

SCB_INFRA_APP:UNLIMITED

SCB_STATIC_APP_CCS:UNLIMITED

SCB_STATIC_APP_ATX_IDLE30:UNLIMITED

Extended Evidence:

Statistics:

Query returned 9 rows

(2.10) 101339 Status of the PASSWORD_LOCK_TIME resource parameter set in all Oracle profiles Passed HIGH (oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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\$

MONT INTERNAL HEED DROCH E HALLA

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)

ROFILE ':' LIMIT
B_STATIC_APP:UNLIMITED
B_SUPP:UNLIMITED
B_STATIC_APP_PSS:UNLIMITED
B_STATIC_APP_NGO:UNLIMITED
RA_STIG_PROFILE:UNLIMITED
FAULT:UNLIMITED
B_STATIC_APP_WEB:UNLIMITED
B_STATIC_APP_NGO_1000:UNLIMITED

Extended Evidence:

Statistics:

Query returned 8 rows

(2.10) 101339 Status of the PASSWORD_LOCK_TIME resource parameter set in all Oracle profiles Passed HIGH (oracle19:1:1621:POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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	
SCB_SUPP:UNLIMITED	
SCB_STATIC_APP_PSS:UNLIMITED	
SCB_INFRA_SUPP:UNLIMITED	
ORA_STIG_PROFILE:UNLIMITED	
SCB_STATIC_APP_ATX:UNLIMITED	
DEFAULT:UNLIMITED	
SCB_STATIC_APP:UNLIMITED	
SCB_INFRA_APP:UNLIMITED	

Statistics:

Query returned 8 rows

(2.10) 101339 Status of the PASSWORD_LOCK_TIME resource parameter set in all Oracle profiles Passed HIGH (oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

DEFAULT:UNLIMITED

SCB_STATIC_APP_PSS:UNLIMITED

SCB_INFRA_APP:UNLIMITED

ORA_STIG_PROFILE:UNLIMITED

SCB_SUPP:UNLIMITED

SCB_STATIC_APP:UNLIMITED

SCB_STATIC_APP_INF:UNLIMITED

SCB_STATIC_APP_NGW:UNLIMITED

Extended Evidence:

Statistics:

Query returned 8 rows

(2.10) 101339 Status of the PASSWORD_LOCK_TIME resource parameter set in all Oracle profiles Failed HIGH (oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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

SCB_STATIC_APP_PSS:UNLIMITED

SCB_STATIC_APP_ATX:UNLIMITED

SCB_STATIC_APP_PAY:UNLIMITED

SCB_STATIC_APP_ATX_IDLE30:UNLIMITED

SCB_SUPP:UNLIMITED

SCB_STATIC_APP:UNLIMITED

DEFAULT:UNLIMITED

SCB_APP_CCS:UNLIMITED

ORA_STIG_PROFILE:UNLIMITED

SCB_STATIC_APP_CCS:UNLIMITED

Extended Evidence:

Statistics:

Query returned 10 rows

Cause of Failure:

Unexpected values

Additional values found in failed controls:

SCB_APP_CCS:UNLIMITED

(2.10) 101339 Status of the PASSWORD_LOCK_TIME resource parameter set in all Oracle profiles Failed HIGH (oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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 DEFAULT:UNLIMITED SCB_INFRA_APP:UNLIMITED SCB_STATIC_APP_CAD:UNLIMITED SCB_SUPP:UNLIMITED SCB_SUPP:1 SCB_STATIC_APP_PSS:UNLIMITED

Extended Evidence:

Statistics:

Query returned 8 rows

Cause of Failure:

Unexpected values

Additional values found in failed controls:

SCB_SUPP:1

(2.10) 101339 Status of the PASSWORD_LOCK_TIME resource parameter set in all Oracle profiles HIGH **Passed** (oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

ORA_STIG_PROFILE:UNLIMITED SCB_STATIC_APP:UNLIMITED

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 SCB_STATIC_APP:UNLIMITED SCB_SUPP:UNLIMITED SCB_STATIC_APP_PSS:UNLIMITED SCB_STATIC_APP_QLDSADMIN:UNLIMITED ORA_STIG_PROFILE:UNLIMITED SCB_STATIC_APP_DS:UNLIMITED DEFAULT:UNLIMITED SCB_STATIC_APP_TNG:UNLIMITED SCB_STATIC_APP_TDC:UNLIMITED

Extended Evidence:

Statistics:

Query returned 9 rows

(2.11) 101340 Status of the PASSWORD_LIFE_TIME resource parameter set in all Oracle profiles Passed HIGH (oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

DEFAULT:UNLIMITED

SCB_STATIC_APP:UNLIMITED

SCB_SUPP:83

ORA_STIG_PROFILE:83

Extended Evidence:

Statistics:

Query returned 4 rows

(2.11) 101340 Status of the PASSWORD_LIFE_TIME resource parameter set in all Oracle profiles Passed HIGH (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

DEFAULT:UNLIMITED

SCB_INFRA_SUPP:83

SCB_SUPP:83

ORA_STIG_PROFILE:83

SCB_STATIC_APP:UNLIMITED

SCB_STATIC_APP-UNLIMITED

SCB_STATIC_APP-ATX:UNLIMITED

SCB_STATIC_APP_CCS:UNLIMITED

SCB_STATIC_APP_CCS:UNLIMITED

SCB_STATIC_APP_ATX_IDLE30:UNLIMITED

Extended Evidence:

Statistics:

Query returned 9 rows

(2.11) 101340 Status of the PASSWORD_LIFE_TIME resource parameter set in all Oracle profiles Passed HIGH (oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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)

ROFILE ':' LIMIT
EFAULT:UNLIMITED
CB_STATIC_APP_PSS:UNLIMITED
CB_INFRA_APP:UNLIMITED
CB_STATIC_APP:UNLIMITED
CB_STATIC_APP_INF:UNLIMITED
CB_STATIC_APP_NGW:UNLIMITED
CB_SUPP:83
RA_STIG_PROFILE:83

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:POHK2CCD.hk.standardchartered.com)

oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status

Instance

Evaluation Date 08/04/2024 at 10:38:34 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:

DBOUERY: 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

ORA_STIG_PROFILE:83

SCB_STATIC_APP:UNLIMITED

SCB_STATIC_APP_PSS:UNLIMITED SCB_STATIC_APP_NGO:UNLIMITED

DEFAULT:UNLIMITED

SCB_SUPP:83

SCB_STATIC_APP_WEB:UNLIMITED

SCB_STATIC_APP_NGO_1000:UNLIMITED

Extended Evidence:

Statistics:

Instance

Query returned 8 rows

(2.11) 101340 Status of the PASSWORD_LIFE_TIME resource parameter set in all Oracle profiles

Passed HIGH

(oracle19:1:1621:POHK1API.hk.standardchartered.com) oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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\$

Oracle ATOS - 20240806 page 622

Passed

HIGH

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_STATIC_APP_PSS:UNLIMITED

SCB STATIC APP ATX:UNLIMITED

DEFAULT:UNLIMITED

ORA_STIG_PROFILE:83

SCB_STATIC_APP:UNLIMITED

SCB_INFRA_APP:UNLIMITED

SCB_INFRA_SUPP:83

SCB_SUPP:83

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:POHK1CCD.hk.standardchartered.com)

Failed

HIGH

oracle19:1:1621:POHK1CCD.hk.standardchartered.com Instance

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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_STATIC_APP_PSS:UNLIMITED

SCB_STATIC_APP_ATX:UNLIMITED

SCB_SUPP:83

SCB_STATIC_APP_PAY:UNLIMITED

SCB_STATIC_APP_ATX_IDLE30:UNLIMITED

SCB_STATIC_APP:UNLIMITED

DEFAULT:UNLIMITED

SCB_APP_CCS:UNLIMITED

ORA_STIG_PROFILE:83

SCB_STATIC_APP_CCS:UNLIMITED

Extended Evidence:

Statistics:

Query returned 10 rows

Cause of Failure:

Unexpected values

Additional values found in failed controls:

SCB_APP_CCS:UNLIMITED

(2.11) 101340 Status of the PASSWORD_LIFE_TIME resource parameter set in all Oracle profiles (oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

Passed

HIGH

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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\$

SCD_INFKA_AFF. .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
DEFAULT:UNLIMITED

SCB_SUPP:83

SCB_INFRA_APP:UNLIMITED

SCB_STATIC_APP_CAD:UNLIMITED

SCB_STATIC_APP_PSS:UNLIMITED

ORA_STIG_PROFILE:83

SCB_STATIC_APP:UNLIMITED

Extended Evidence:

Statistics:

Query returned 7 rows

(2.11) 101340 Status of the PASSWORD_LIFE_TIME resource parameter set in all Oracle profiles (oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

Passed

HIGH

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

ORA_STIG_PROFILE:83

SCB_STATIC_APP:UNLIMITED

SCB_STATIC_APP_PSS:UNLIMITED

SCB_STATIC_APP_QLDSADMIN:UNLIMITED

SCB_STATIC_APP_DS:UNLIMITED

DEFAULT:UNLIMITED

SCB_SUPP:83

SCB_STATIC_APP_TNG:UNLIMITED

SCB_STATIC_APP_TDC:UNLIMITED

Extended Evidence:

Statistics:

Query returned 9 rows

(2.12) 101341 Status of the PASSWORD_REUSE_MAX resource parameter set in all Oracle profiles Passed HIGH (oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_STATIC_APP:UNLIMITED

ORA_STIG_PROFILE:20

SCB SUPP:20

Extended Evidence:

Statistics:

Query returned 4 rows

(2.12) 101341 Status of the PASSWORD_REUSE_MAX resource parameter set in all Oracle profiles Passed HIGH (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:UNLIMITED

SCB_STATIC_APP_ATX:UNLIMITED

ORA_STIG_PROFILE:20

SCB_SUPP:20

SCB_INFRA_APP:UNLIMITED

SCB_STATIC_APP_CCS:UNLIMITED

SCB_STATIC_APP_ATX_IDLE30:UNLIMITED

Extended Evidence:

Statistics:

Query returned 9 rows

(2.12) 101341 Status of the PASSWORD_REUSE_MAX resource parameter set in all Oracle profiles Passed HIGH (oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

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_STATIC_APP_PSS:UNLIMITED

SCB_INFRA_APP:UNLIMITED

SCB_STATIC_APP:UNLIMITED

ORA_STIG_PROFILE:20

SCB_STATIC_APP_INF:UNLIMITED

SCB_SUPP:20

SCB_STATIC_APP_NGW:UNLIMITED

Extended Evidence:

Statistics:

Query returned 8 rows

(2.12) 101341 Status of the PASSWORD_REUSE_MAX resource parameter set in all Oracle profiles Passed HIGH (oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

SCB_STATIC_APP:UNLIMITED

SCB_STATIC_APP_PSS:UNLIMITED

SCB_STATIC_APP_NGO:UNLIMITED

DEFAULT:UNLIMITED

SCB_SUPP:20
SCB_STATIC_APP_WEB:UNLIMITED
SCB_STATIC_APP_NGO_1000:UNLIMITED
ORA_STIG_PROFILE:20

Extended Evidence:

Statistics:

Query returned 8 rows

(2.12) 101341 Status of the PASSWORD_REUSE_MAX resource parameter set in all Oracle profiles Passed HIGH (oracle19:1:1621:POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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
SCB_STATIC_APP_PSS:UNLIMITED

SCB_STATIC_APP_ATX:UNLIMITED

DEFAULT:UNLIMITED
ORA_STIG_PROFILE:20

SCB_INFRA_SUPP:20

SCB_STATIC_APP:UNLIMITED

SCB_INFRA_APP:UNLIMITED

SCB_SUPP:20

Extended Evidence:

Statistics:

Query returned 8 rows

(2.12) 101341 Status of the PASSWORD_REUSE_MAX resource parameter set in all Oracle profiles Failed HIGH (oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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

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

PROFILE||':'||LIMIT

SCB_STATIC_APP_PSS:UNLIMITED

SCB_STATIC_APP_ATX:UNLIMITED

SCB_STATIC_APP_PAY:UNLIMITED

SCB_STATIC_APP_ATX_IDLE30:UNLIMITED

SCB_STATIC_APP:UNLIMITED

DEFAULT:UNLIMITED

SCB_APP_CCS:UNLIMITED

ORA_STIG_PROFILE:20

SCB_SUPP:20

SCB STATIC APP CCS:UNLIMITED

Extended Evidence:

Statistics:

Query returned 10 rows

Cause of Failure:

Unexpected values

Additional values found in failed controls:

SCB_APP_CCS:UNLIMITED

(2.12) 101341 Status of the PASSWORD_REUSE_MAX resource parameter set in all Oracle profiles **Passed** HIGH (oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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'

is contained in regular expression list **Expected**

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
	SCB_STATIC_APP_PSS:UNLIMITED
	SCB_STATIC_APP:UNLIMITED
	DEFAULT:UNLIMITED
	SCB_SUPP:20
	SCB_INFRA_APP:UNLIMITED
	SCB_STATIC_APP_CAD:UNLIMITED
	ORA STIG PROFILE:20

Statistics:

Query returned 7 rows

(2.12) 101341 Status of the PASSWORD_REUSE_MAX resource parameter set in all Oracle profiles Passed HIGH (oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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
SCB_STATIC_APP:UNLIMITED
SCB_STATIC_APP_PSS:UNLIMITED
SCB_STATIC_APP_QLDSADMIN:UNLIMITED
SCB_STATIC_APP_DS:UNLIMITED
DEFAULT:UNLIMITED
SCB_STATIC_APP_TNG:UNLIMITED
SCB_SUPP:20
SCB_STATIC_APP_TDC:UNLIMITED
ORA_STIG_PROFILE:20

Extended Evidence:

Statistics:

Query returned 9 rows

(2.13) 101342 Status of the PASSWORD_REUSE_TIME resource parameter set in all Oracle profiles Passed HIGH (oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

DEFAULT:UNLIMITED

ORA_STIG_PROFILE:UNLIMITED

SCB_SUPP:UNLIMITED

SCB_STATIC_APP:UNLIMITED

Extended Evidence:

Statistics:

Query returned 4 rows

(2.13) 101342 Status of the PASSWORD_REUSE_TIME resource parameter set in all Oracle profiles Passed HIGH (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

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

Extended Evidence:

Statistics:

Query returned 9 rows

(2.13) 101342 Status of the PASSWORD_REUSE_TIME resource parameter set in all Oracle profiles Passed HIGH (oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

SCB_STATIC_APP_ATX_IDLE30:UNLIMITED

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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
DEFAULT:UNLIMITED
SCB_STATIC_APP_PSS:UNLIMITED
SCB_INFRA_APP:UNLIMITED
DRA_STIG_PROFILE:UNLIMITED
SCB_SUPP:UNLIMITED
SCB_STATIC_APP:UNLIMITED
SCB_STATIC_APP_INF:UNLIMITED
SCB_STATIC_APP_NGW:UNLIMITED

Extended Evidence:

Statistics:

Query returned 8 rows

(2.13) 101342 Status of the PASSWORD_REUSE_TIME resource parameter set in all Oracle profiles Passed HIGH (oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

SCB_STATIC_APP:UNLIMITED

SCB_SUPP:UNLIMITED

SCB_STATIC_APP_PSS:UNLIMITED

SCB_STATIC_APP_NGO:UNLIMITED
ORA_STIG_PROFILE:UNLIMITED

SCB_STATIC_APP_NGO_1000:UNLIMITED

DEFAULT:UNLIMITED

SCB_STATIC_APP_WEB:UNLIMITED

Extended Evidence:

Statistics:

Query returned 8 rows

(2.13) 101342 Status of the PASSWORD_REUSE_TIME resource parameter set in all Oracle profiles Passed HIGH (oracle19:1:1621:POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 SCB_SUPP:UNLIMITED SCB_STATIC_APP_PSS:UNLIMITED SCB_INFRA_SUPP:UNLIMITED ORA_STIG_PROFILE:UNLIMITED SCB_STATIC_APP_ATX:UNLIMITED SCB_STATIC_APP_ATX:UNLIMITED SCB_STATIC_APP_ED SCB_STATIC_APP:UNLIMITED SCB_STATIC_APP:UNLIMITED SCB_STATIC_APP:UNLIMITED SCB_STATIC_APP:UNLIMITED

Extended Evidence:

Statistics:

Query returned 8 rows

(2.13) 101342 Status of the PASSWORD_REUSE_TIME resource parameter set in all Oracle profiles Failed HIGH (oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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)

Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)	
PROFILE ':' LIMIT	
SCB_STATIC_APP_PSS:UNLIMITED	
SCB_STATIC_APP_ATX:UNLIMITED	
SCB_STATIC_APP_PAY:UNLIMITED	
SCB_STATIC_APP_ATX_IDLE30:UNLIMITED	
SCB_SUPP:UNLIMITED	
SCB_STATIC_APP:UNLIMITED	
DEFAULT:UNLIMITED	
SCB_APP_CCS:UNLIMITED	
ORA_STIG_PROFILE:UNLIMITED	
SCB_STATIC_APP_CCS:UNLIMITED	

Extended Evidence:

Statistics:

Query returned 10 rows

Cause of Failure:

Unexpected values

Additional values found in failed controls:

SCB_APP_CCS:UNLIMITED

(2.13) 101342 Status of the PASSWORD_REUSE_TIME resource parameter set in all Oracle profiles Passed HIGH (oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

DEFAULT:UNLIMITED

SCB_INFRA_APP:UNLIMITED

SCB_SUPP:UNLIMITED

SCB_STATIC_APP_PSS:UNLIMITED

ORA_STIG_PROFILE:UNLIMITED
SCB_STATIC_APP_CAD:UNLIMITED

SCB_STATIC_APP:UNLIMITED

Extended Evidence:

Statistics:

Query returned 7 rows

(2.13) 101342 Status of the PASSWORD_REUSE_TIME resource parameter set in all Oracle profiles Passed HIGH (oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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 SCB_STATIC_APP:UNLIMITED SCB_SUPP:UNLIMITED SCB_STATIC_APP_PSS:UNLIMITED SCB_STATIC_APP_QLDSADMIN:UNLIMITED ORA_STIG_PROFILE:UNLIMITED SCB_STATIC_APP_DS:UNLIMITED SCB_STATIC_APP_DS:UNLIMITED SCB_STATIC_APP_TSC:UNLIMITED SCB_STATIC_APP_TNG:UNLIMITED

Extended Evidence:

Statistics:

Query returned 9 rows

(2.14) 101343 Status of the PASSWORD_GRACE_TIME resource parameter set in all Oracle profiles Passed MEDIUM (oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

SCB_STATIC_APP_TDC:UNLIMITED

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:

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	
ORA_STIG_PROFILE:7	
DEFAULT:7	
SCB_STATIC_APP:7	
SCB SUPP-7	

Extended Evidence:

Statistics:

Query returned 4 rows

(2.14) 101343 Status of the PASSWORD_GRACE_TIME resource parameter set in all Oracle profiles Passed MEDIUM (oracle19:1:1621:POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_STATIC_APP:7

SCB_SUPP:7

ORA_STIG_PROFILE:7

SCB_STATIC_APP_ATX:7

SCB_STATIC_APP_PSS:7

SCB_INFRA_APP:7

SCB_INFRA_SUPP:7

DEFAULT:7

Extended Evidence:

Statistics:

Query returned 8 rows

(2.14) 101343 Status of the PASSWORD_GRACE_TIME resource parameter set in all Oracle profiles Passed MEDIUM (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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\$

SCB_SUFF. ./ \$

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 U

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

PROFILE||':'||LIMIT SCB_INFRA_SUPP:7

DEFAULT:7

SCB_STATIC_APP_ATX_IDLE30:7

SCB_INFRA_APP:7

SCB_STATIC_APP:7

SCB_SUPP:7

SCB_STATIC_APP_CCS:7

ORA_STIG_PROFILE:7

SCB_STATIC_APP_ATX:7

Extended Evidence:

Statistics:

Query returned 9 rows

(2.14) 101343 Status of the PASSWORD_GRACE_TIME resource parameter set in all Oracle profiles Passed MEDIUM (oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

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

ORA_STIG_PROFILE:7

DEFAULT:7

SCB_STATIC_APP:7

SCB_STATIC_APP_PSS:7

SCB_INFRA_APP:7

SCB_SUPP:7

SCB_STATIC_APP_INF:7

SCB_STATIC_APP_NGW:7

Statistics:

Query returned 8 rows

(2.14) 101343 Status of the PASSWORD_GRACE_TIME resource parameter set in all Oracle profiles Passed MEDIUM (oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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
DEFAULT:7

SCB_STATIC_APP_PSS:7

SCB_STATIC_APP:7

SCB_STATIC_APP_WEB:7

SCB_STATIC_APP_NGO:7

SCB_SUPP:7

ORA_STIG_PROFILE:7

SCB_STATIC_APP_NGO_1000:7

Extended Evidence:

Statistics:

Query returned 8 rows

(2.14) 101343 Status of the PASSWORD_GRACE_TIME resource parameter set in all Oracle profiles Failed MEDIUM (oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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

ORA_STIG_PROFILE:7

SCB_STATIC_APP_ATX_IDLE30:7

SCB_STATIC_APP_CCS:7

SCB_STATIC_APP_PAY:7

SCB_STATIC_APP:7

SCB_STATIC_APP:7

SCB_SUPP:7

SCB_STATIC_APP_ATX:7

SCB_APP_CCS:7

DEFAULT:7

SCB_STATIC_APP_PSS:7

Extended Evidence:

Statistics:

Query returned 10 rows

Cause of Failure:

Unexpected values

Additional values found in failed controls:

SCB_APP_CCS:7

(2.14) 101343 Status of the PASSWORD_GRACE_TIME resource parameter set in all Oracle profiles Passed MEDIUM (oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_STATIC_APP:7 SCB_INFRA_APP:7 SCB_SUPP:7 ORA_STIG_PROFILE:7 DEFAULT:7

Extended Evidence:

Statistics:

Query returned 7 rows

(2.14) 101343 Status of the PASSWORD_GRACE_TIME resource parameter set in all Oracle profiles Passed MEDIUM (oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

SCB_STATIC_APP_PSS:7 SCB_STATIC_APP_CAD:7

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\$

ORA_STIG_PROFILE:7 SCB_STATIC_APP_TNG: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
DEFAULT:7
SCB_STATIC_APP_TDC:7
SCB_STATIC_APP_PSS:7
SCB_STATIC_APP_QLDSADMIN:7
SCB_STATIC_APP:7
SCB_STATIC_APP_DS:7
SCB_SUPP:7

Extended Evidence:

Statistics:

Query returned 9 rows

(2.15) 101344 Ensure No Users Are Assigned the 'DEFAULT' Profile_(CIS-32)(oracle19:1:1621: Failed HIGH POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

test_control_101116

test_control_101116

Scan Parameters:

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 DBQUERY:

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
CCS_SCAN	1
ORARO	1
SCB_LINK	1
ORAMED2	1
DBARO	1
DBADDM	1
AOGEMS	1
OEMUSER	1
ORAMED1	1
SCB_ADMIN	1
SCB_ADMIN	3
CCS_SCAN	3
ORARO	3
SCB_LINK	3
ORAMED2	3
DBARO	3
DBADDM	3
AOGEMS	3
D42ULADM	3
OEMUSER	3
ORAMED1	3

Extended Evidence:

Statistics:

Query returned 21 rows

(2.15) 101344 Ensure No Users Are Assigned the 'DEFAULT' Profile_(CIS-32)(oracle19:1:1621: **Failed** HIGH POHK1API.hk.standardchartered.com)

oracle19:1:1621:POHK1API.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

test_control_101116

test_control_101116

Scan Parameters:

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<> 2DBQUERY:

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
D42ULADM	4

Statistics:

Query returned 2 rows

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

POHK1CAT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com Previous Status

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

test_control_101116

test_control_101116

Scan Parameters:

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 DBQUERY:

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
PDBADMIN	4
PDBADMIN	5

Extended Evidence:

Statistics:

Query returned 2 rows

(2.15) 101344 Ensure No Users Are Assigned the 'DEFAULT' Profile_(CIS-32)(oracle19:1:1621: **Failed** HIGH POHK5CCD.hk.standardchartered.com)

oracle19:1:1621:POHK5CCD.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

test control 101116

test control 101116

Scan Parameters:

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 DBQUERY:

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
CCS_SCAN	1
ORARO	1
SCB_LINK	1
ORAMED2	1
DBARO	1
DBADDM	1
AOGEMS	1
OEMUSER	1
ORAMED1	1
SECADMIN	1
CCS_SCAN	3
ORARO	3
SCB_LINK	3

ORAMED2	3
DBARO	3
DBADDM	3
AOGEMS	3
D42ULADM	3
OEMUSER	3
ORAMED1	3
SECADMIN	3
SQLTXADMIN	3
SQLTXPLAIN	3

Statistics:

Query returned 23 rows

(2.15) 101344 Ensure No Users Are Assigned the 'DEFAULT' Profile_(CIS-32)(oracle19:1:1621: POHK2CCD.hk.standardchartered.com) **Failed** HIGH

oracle 19:1:1621:POHK2CCD.hk. standard chartered. comInstance

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

test_control_101116

test_control_101116

Scan Parameters:

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 DBQUERY:

Expected any of the selected values below:

Set status to PASS if no data found

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

USERNAME	CON_ID
CCS_SCAN	1
ORARO	1
SCB_LINK	1
ORAMED2	1
DBARO	1
DBADDM	1
AOGEMS	1
OEMUSER	1
ORAMED1	1
SECADMIN	1
SCB_ADMIN	1
SCB_ADMIN	3
CCS_SCAN	3
ORARO	3
SCB_LINK	3
ORAMED2	3
DBARO	3
DBADDM	3
AOGEMS	3
D42ULADM	3
OEMUSER	3
ORAMED1	3
SECADMIN	3
SCB_ADMIN	4
CCS_SCAN	4
ORARO	4
SCB_LINK	4

ORAMED2 4 DBARO 4 DBADDM 4 AOGEMS 4 D42ULADM 4 OEMUSER 4 ORAMED1 4 SECADMIN 4 SCB_ADMIN 6 CCS_SCAN 6 ORARO 6 SCB_LINK 6 ORAMED2 6 DBARO 6 DBADDM 6 AOGEMS 6 D42ULADM 6 OEMUSER 6 ORAMED1 6 OEMUSER 6 ORAMED1 6 SECADMIN 6		
DBADDM 4 AOGEMS 4 D42ULADM 4 OEMUSER 4 ORAMEDI 4 SECADMIN 4 SCB_ADMIN 6 CCS_SCAN 6 ORARO 6 SCB_LINK 6 ORAMED2 6 DBARO 6 DBADDM 6 AOGEMS 6 D42ULADM 6 OEMUSER 6 ORAMED1 6	ORAMED2	4
AOGEMS 4 D42ULADM 4 OEMUSER 4 ORAMED1 4 SECADMIN 4 SCB_ADMIN 6 CCS_SCAN 6 ORARO 6 SCB_LINK 6 ORAMED2 6 DBARO 6 DBADDM 6 AOGEMS 6 D42ULADM 6 OEMUSER 6 ORAMED1 6	DBARO	4
D42ULADM 4 OEMUSER 4 ORAMED1 4 SECADMIN 4 SCB_ADMIN 6 CCS_SCAN 6 ORARO 6 SCB_LINK 6 ORAMED2 6 DBARO 6 DBADDM 6 AOGEMS 6 D42ULADM 6 OEMUSER 6 ORAMED1 6	DBADDM	4
OEMUSER 4 ORAMED1 4 SECADMIN 4 SCB_ADMIN 6 CCS_SCAN 6 ORARO 6 SCB_LINK 6 ORAMED2 6 DBARO 6 DBADDM 6 AOGEMS 6 D42ULADM 6 OEMUSER 6 ORAMED1 6	AOGEMS	4
ORAMED1 4 SECADMIN 4 SCB_ADMIN 6 CCS_SCAN 6 ORARO 6 SCB_LINK 6 ORAMED2 6 DBARO 6 DBADDM 6 AOGEMS 6 D42ULADM 6 OEMUSER 6 ORAMED1 6	D42ULADM	4
SECADMIN 4 SCB_ADMIN 6 CCS_SCAN 6 ORARO 6 SCB_LINK 6 ORAMED2 6 DBARO 6 DBADDM 6 AOGEMS 6 D42ULADM 6 OEMUSER 6 ORAMED1 6	OEMUSER	4
SCB_ADMIN 6 CCS_SCAN 6 ORARO 6 SCB_LINK 6 ORAMED2 6 DBARO 6 DBADDM 6 AOGEMS 6 D42ULADM 6 OEMUSER 6 ORAMED1 6	ORAMED1	4
CCS_SCAN 6 ORARO 6 SCB_LINK 6 ORAMED2 6 DBARO 6 DBADDM 6 AOGEMS 6 D42ULADM 6 OEMUSER 6 ORAMED1 6	SECADMIN	4
ORARO 6 SCB_LINK 6 ORAMED2 6 DBARO 6 DBADDM 6 AOGEMS 6 D42ULADM 6 OEMUSER 6 ORAMED1 6	SCB_ADMIN	6
SCB_LINK 6 ORAMED2 6 DBARO 6 DBADDM 6 AOGEMS 6 D42ULADM 6 OEMUSER 6 ORAMED1 6	CCS_SCAN	6
ORAMED2 6 DBARO 6 DBADDM 6 AOGEMS 6 D42ULADM 6 OEMUSER 6 ORAMED1 6	ORARO	6
DBARO 6 DBADDM 6 AOGEMS 6 D42ULADM 6 OEMUSER 6 ORAMED1 6	SCB_LINK	6
DBADDM 6 AOGEMS 6 D42ULADM 6 OEMUSER 6 ORAMED1 6	ORAMED2	6
AOGEMS 6 D42ULADM 6 OEMUSER 6 ORAMED1 6	DBARO	6
D42ULADM 6 OEMUSER 6 ORAMED1 6	DBADDM	6
OEMUSER 6 ORAMED1 6	AOGEMS	6
ORAMED1 6	D42ULADM	6
	OEMUSER	6
SECADMIN 6	ORAMED1	6
	SECADMIN	6

Statistics:

Query returned 47 rows

(2.15) 101344 Ensure No Users Are Assigned the 'DEFAULT' Profile_(CIS-32)(oracle19:1:1621: POHK1CCD.hk.standardchartered.com) **Failed** HIGH

Instance oracle 19:1:1621:POHK1CCD.hk. standard chartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

test_control_101116

test_control_101116

Scan Parameters:

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<> 2DBQUERY:

Expected any of the selected values below:

Set status to PASS if no data found

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

USERNAME	CON_ID
SCB_ADMIN	3
CCS_SCAN	3
ORARO	3
SCB_LINK	3
ORAMED2	3
DBARO	3
DBADDM	3
AOGEMS	3
D42ULADM	3
OEMUSER	3
ORAMED1	3
SECADMIN	3
SCB_ADMIN	5
CCS_SCAN	5
ORARO	5
SCB_LINK	5
ORAMED2	5

DBARO	5
DBADDM	5
AOGEMS	5
D42ULADM	5
OEMUSER	5
ORAMED1	5
SECADMIN	5
CCS_SCAN	1
ORARO	1
SCB_LINK	1
ORAMED2	1
DBARO	1
DBADDM	1
AOGEMS	1
OEMUSER	1
ORAMED1	1
SECADMIN	1
SCB_ADMIN	1
SCB_ADMIN	4
CCS_SCAN	4
ORARO	4
SCB_LINK	4
ORAMED2	4
DBARO	4
DBADDM	4
AOGEMS	4
D42ULADM	4
OEMUSER	4
ORAMED1	4
SECADMIN	4
SCB_ADMIN	7
CCS_SCAN	7
ORARO	7
SCB_LINK	7
ORAMED2	7
DBARO	7
DBADDM	7
AOGEMS	7
D42ULADM	7
OEMUSER	7
ORAMED1	7
SECADMIN	7

Statistics:

Query returned 59 rows

(2.15) 101344 Ensure No Users Are Assigned the 'DEFAULT' Profile_(CIS-32)(oracle19:1:1621: POHK4CCD.hk.standardchartered.com) **Failed** HIGH

Instance oracle 19:1:1621:POHK4CCD.hk. standard chartered.com

Failed **Previous Status**

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

test_control_101116

test_control_101116

Scan Parameters:

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 DBQUERY:

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)

Last Opuated.00/04/2024 at 00.01.09 FM (GM1+0330)	T T
USERNAME	CON_ID
SCB_ADMIN	4
CCS_SCAN	4
ORARO	4
SCB_LINK	4
ORAMED2	4
DBARO	4
DBADDM	4
AOGEMS	4
D42ULADM	4
OEMUSER	4
ORAMED1	4
SECADMIN	4
SCB_ADMIN	5
CCS_SCAN	5
PDBADMIN	5
ORARO	5
SCB_LINK	5
ORAMED2	5
DBARO	5
DBADDM	5
AOGEMS	5
OEMUSER	5
ORAMED1	5
SECADMIN	5
CCS_SCAN	1
ORARO	1
SCB_LINK	1
ORAMED2	1
DBARO	1
DBADDM	1
AOGEMS	1
OEMUSER	1
ORAMED1	1
SECADMIN	1
SCB_ADMIN	1
SCB_ADMIN	3
CCS_SCAN	3
ORARO	3
SCB_LINK	3
ORAMED2	3
DBARO	3
DBADDM	3
AOGEMS	3
D42ULADM	3
OEMUSER	3
ORAMED1	3
SECADMIN	3
SECADIVIII	J

Extended Evidence:

Statistics:

Query returned 47 rows

(2.15) 101344 Ensure No Users Are Assigned the 'DEFAULT' Profile_(CIS-32)(oracle19:1:1621: POHK3CCD.hk.standardchartered.com) **Failed** HIGH

oracle19:1:1621:POHK3CCD.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

test_control_101116

 $test_control_101116$

Scan Parameters:

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<> 2DBQUERY:

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)

243t Opdated.00/04/2024 at 00:01:03 f iii (Oiii 1 +0000)		
USERNAME	CON_ID	
CCS_SCAN	1	
ORARO	1	
SCB_LINK	1	
ORAMED2	1	
DBARO	1	
DBADDM	1	
AOGEMS	1	
OEMUSER	1	
ORAMED1	1	
SECADMIN	1	
SCB_ADMIN	1	
SCB_ADMIN	3	
CCS_SCAN	3	
ORARO	3	
SCB_LINK	3	
ORAMED2	3	
DBARO	3	
DBADDM	3	
AOGEMS	3	
D42ULADM	3	
OEMUSER	3	
ORAMED1	3	
SECADMIN	3	
SCB_ADMIN	4	
CCS_SCAN	4	
ORARO	4	
SCB_LINK	4	
ORAMED2	4	
DBARO	4	
DBADDM	4	
AOGEMS	4	
D42ULADM	4	
OEMUSER	4	
ORAMED1	4	
SECADMIN	4	
SCB_ADMIN	5	
CCS_SCAN	5	
ORARO	5	
SCB_LINK	5	
ORAMED2	5	
DBARO		
	5	

AOGEMS	5
D42ULADM	5
OEMUSER	5
ORAMED1	5
SECADMIN	5

Extended Evidence:

Statistics:

Query returned 47 rows

(2.16) 101345 Ensure 'GRANT ANY OBJECT PRIVILEGE' Is Revoked from Unauthorized 'GRANTEE' **HIGH Passed** (CIS-58)(oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

DBOUERY: 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

(2.16) 101345 Ensure 'GRANT ANY OBJECT PRIVILEGE' Is Revoked from Unauthorized 'GRANTEE' **HIGH Passed** (CIS-58)(oracle19:1:1621:POHK1API.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.16) 101345 Ensure 'GRANT ANY OBJECT PRIVILEGE' Is Revoked from Unauthorized 'GRANTEE' Passed HIGH (CIS-58)(oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

oracle19:1:1621:POHK1CAT.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.16) 101345 Ensure 'GRANT ANY OBJECT PRIVILEGE' Is Revoked from Unauthorized 'GRANTEE' **Passed HIGH** (CIS-58)(oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.16) 101345 Ensure 'GRANT ANY OBJECT PRIVILEGE' Is Revoked from Unauthorized 'GRANTEE' **Passed HIGH** (CIS-58)(oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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')

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

Set status to PASS if no data found

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.16) 101345 Ensure 'GRANT ANY OBJECT PRIVILEGE' Is Revoked from Unauthorized 'GRANTEE' **Passed HIGH** (CIS-58)(oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

oracle19:1:1621:POHK3CCD.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

DBOUERY: SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS

WHERE PRIVILEGE FROM DBA_STARYO WHERE PROVIDED TO SHARE 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

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.16) 101345 Ensure 'GRANT ANY OBJECT PRIVILEGE' Is Revoked from Unauthorized 'GRANTEE' **Passed HIGH** (CIS-58)(oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

oracle19:1:1621:POHK1CCD.hk.standardchartered.com Instance

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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:

SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS DBQUERY:

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', 'PÙPPETAM', '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

(2.16) 101345 Ensure 'GRANT ANY OBJECT PRIVILEGE' Is Revoked from Unauthorized 'GRANTEE' **HIGH** Passed (CIS-58)(oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

Ouery returned 0 rows

(2.17) 101347 Ensure 'GRANT ANY PRIVILEGE' Is Revoked from Unauthorized 'GRANTEE'(CIS-60) **Passed HIGH** (oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

oracle19:1:1621:POHK1RCT.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(2.17) 101347 Ensure 'GRANT ANY PRIVILEGE' Is Revoked from Unauthorized 'GRANTEE'(CIS-60) **Passed HIGH** (oracle19:1:1621:POHK1API.hk.standardchartered.com)

oracle19:1:1621:POHK1API.hk.standardchartered.com Instance

Passed Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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:

DBOUERY:

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 GRĀNTEE not in ('SEĆADMIN', 'SCB_ADMIN', 'PÙPPETAM','HCVPWDMANĪD_ROOT','HCVPWDMANĪD')

Expected any of the selected values below:

Set status to PASS if no data found

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.17) 101347 Ensure 'GRANT ANY PRIVILEGE' Is Revoked from Unauthorized 'GRANTEE'(CIS-60) HIGH **Passed** (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

oracle 19:1:1621:POHK1CAT.hk.standardchartered.com Instance

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.17) 101347 Ensure 'GRANT ANY PRIVILEGE' Is Revoked from Unauthorized 'GRANTEE'(CIS-60) **HIGH Passed** (oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

oracle19:1:1621:POHK5CCD.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

DBOUERY:

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

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.17) 101347 Ensure 'GRANT ANY PRIVILEGE' Is Revoked from Unauthorized 'GRANTEE'(CIS-60) **HIGH Passed** (oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

oracle19:1:1621:POHK2CCD.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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', 'HCVPWDMANĪD_ROOT', 'HCVPWDMANĪD')

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) **Passed** HIGH (oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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')

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

Set status to PASS if no data found

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.17) 101347 Ensure 'GRANT ANY PRIVILEGE' Is Revoked from Unauthorized 'GRANTEE'(CIS-60) **Passed** HIGH (oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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

(2.17) 101347 Ensure 'GRANT ANY PRIVILEGE' Is Revoked from Unauthorized 'GRANTEE'(CIS-60) HIGH **Passed** (oracle19:1:1621:POHK4CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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:

DBOUERY:

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

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.18) 101352 Ensure 'trace files public'ls Set to 'FALSE'(oracle19:1:1621:POHK1RCT.hk. **Passed HIGH**

standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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

(2.18) 101352 Ensure '_trace_files_public'ls Set to 'FALSE'(oracle19:1:1621:POHK1API.hk. standardchartered.com) **HIGH Passed**

oracle19:1:1621:POHK1API.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

Ensure ' trace files public'ls 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

(2.18) 101352 Ensure '_trace_files_public'ls Set to 'FALSE'(oracle19:1:1621:POHK1CAT.hk. Passed standardchartered.com)

HIGH

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(2.18) 101352 Ensure '_trace_files_public'ls Set to 'FALSE'(oracle19:1:1621:POHK5CCD.hk. Passed HIGH standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(2.18) 101352 Ensure 'trace files public'ls Set to 'FALSE'(oracle19:1:1621:POHK2CCD.hk.

Passed

HIGH

standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

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

No data found

Extended Evidence:

Statistics:

Instance

Query returned 0 rows

(2.18) 101352 Ensure '_trace_files_public'ls Set to 'FALSE'(oracle19:1:1621:POHK3CCD.hk. standardchartered.com)

oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Passed HIGH

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(2.18) 101352 Ensure '_trace_files_public'ls Set to 'FALSE'(oracle19:1:1621:POHK1CCD.hk. standardchartered.com)

Passed HIGH

oracle19:1:1621:POHK1CCD.hk.standardchartered.com Instance

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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

(2.18) 101352 Ensure '_trace_files_public'ls Set to 'FALSE'(oracle19:1:1621:POHK4CCD.hk.

HIGH **Passed**

standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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';

matches regular expression list **Expected**

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.hk. standardchartered.com)

Passed

HIGH

oracle19:1:1621:POHK1API.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

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:POHK1CAT.hk. **HIGH Passed** standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

password length

password length

Scan Parameters:

select name,max(instr(text,'ora_complexity_check(password, chars => 25, uppercase => 1, lowercase => 1, digit => 1, special => 1)'))
Position from dba_source where DBQUERY:

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

(2.19) 101354 Ensure password complexity as per standards(oracle19:1:1621:POHK5CCD.hk. **Passed HIGH** standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(2.19) 101354 Ensure password complexity as per standards(oracle19:1:1621:POHK1RCT.hk. **Passed** standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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)'))

HIGH

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

(2.19) 101354 Ensure password complexity as per standards(oracle19:1:1621:POHK3CCD.hk. **Passed HIGH** standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(2.19) 101354 Ensure password complexity as per standards(oracle19:1:1621:POHK1CCD.hk. **Passed** HIGH standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

password length

password length

Scan Parameters:

DBOUERY: 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

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.19) 101354 Ensure password complexity as per standards(oracle19:1:1621:POHK4CCD.hk. **Passed** HIGH standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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

match all equal to **Expected**

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

HIGH (2.19) 101354 Ensure password complexity as per standards(oracle19:1:1621:POHK2CCD.hk. **Passed** standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

password length

password length

Scan Parameters:

 $select\ name, max(instr(text, 'ora_complexity_check(password, \ chars => 25, \ uppercase => 1, \ lowercase => 1, \ digit => 1, \ special => 1)'))$ Position from dba_source where DBQUERY:

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.hk. Passed **HIGH** standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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)

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

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:POHK1CAT.hk. Passed **HIGH** standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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')

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:

Ouery returned 0 rows

(2.20) 101356 Status of 'DBA' role granted to grantees (roles)(CIS-63)(oracle19:1:1621:POHK5CCD. **Failed HIGH** hk.standardchartered.com)

oracle19:1:1621:POHK5CCD.hk.standardchartered.com Instance

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 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')

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)

PATH	GRANTEE	GRANTED_ROLE	CON_ID
GRANT	SQLTXPLAIN	DBA	3
GRANT	SOLTXADMIN	DBA	3

Extended Evidence:

Statistics:

Query returned 2 rows

(2.20) 101356 Status of 'DBA' role granted to grantees (roles)(CIS-63)(oracle19:1:1621:POHK1RCT.hk. Passed **HIGH** standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

DBOUERY:

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

SHION 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:

Instance

Query returned 0 rows

(2.20) 101356 Status of 'DBA' role granted to grantees (roles)(CIS-63)(oracle19:1:1621:POHK3CCD. **HIGH Passed** hk.standardchartered.com)

oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(2.20) 101356 Status of 'DBA' role granted to grantees (roles)(CIS-63)(oracle19:1:1621:POHK1CCD. **HIGH** Passed hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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')

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

(2.20) 101356 Status of 'DBA' role granted to grantees (roles)(CIS-63)(oracle19:1:1621:POHK4CCD. **HIGH Passed** hk.standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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')

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

(2.20) 101356 Status of 'DBA' role granted to grantees (roles)(CIS-63)(oracle19:1:1621:POHK2CCD. HIGH Passed hk.standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) Evaluation Date

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')

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) HIGH **Passed** (oracle19:1:1621:POHK5CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

Set status to PASS if no data found

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 ROÒT','HCVPWDMANĪD')

Expected any of the selected values below:

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

No data found

Extended Evidence:

Statistics:

Instance

Query returned 0 rows

(2.21) 101361 Ensure 'GRANT ANY ROLE' Is Revoked from Unauthorized 'GRANTEE'(CIS-59) **Passed**

HIGH

HIGH

(oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

oracle19:1:1621:POHK1RCT.hk.standardchartered.com **Previous Status** Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

Instance

Query returned 0 rows

(2.21) 101361 Ensure 'GRANT ANY ROLE' Is Revoked from Unauthorized 'GRANTEE'(CIS-59) **Passed** (oracle19:1:1621:POHK3CCD.hk.standardchartered.com)

oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS DBQUERY:

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:

(2.21) 101361 Ensure 'GRANT ANY ROLE' Is Revoked from Unauthorized 'GRANTEE'(CIS-59) **Passed HIGH**

(oracle19:1:1621:POHK1CCD.hk.standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

Instance

Query returned 0 rows

(2.21) 101361 Ensure 'GRANT ANY ROLE' Is Revoked from Unauthorized 'GRANTEE'(CIS-59) **Passed HIGH**

(oracle19:1:1621:POHK4CCD.hk.standardchartered.com) oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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:

Instance

Query returned 0 rows

(2.21) 101361 Ensure 'GRANT ANY ROLE' Is Revoked from Unauthorized 'GRANTEE'(CIS-59) **Passed HIGH**

(oracle19:1:1621:POHK1API.hk.standardchartered.com)

oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

DBOUERY:

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

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.21) 101361 Ensure 'GRANT ANY ROLE' Is Revoked from Unauthorized 'GRANTEE'(CIS-59) **Passed** (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

oracle19:1:1621:POHK1CAT.hk.standardchartered.com Instance

Previous Status Passed

08/04/2024 at 10:38:34 PM (GMT+0530) **Evaluation Date**

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')

HIGH

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) **Passed** HIGH (oracle19:1:1621:POHK2CCD.hk.standardchartered.com)

oracle19:1:1621:POHK2CCD.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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:

DBOUERY:

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

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

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.hk. HIGH **Failed** standardchartered.com)

oracle19:1:1621:POHK1API.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

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

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

Scan Parameters:

DBOUERY:

SELECT TABLE_NAME, PRIVILEGE, GRANTEE, CON_ID
DATABASE FROM CDB_TAB_PRIVS A WHERE TABLE_NAME in
('CDB_LOCAL_ADMINAUTH\$', 'DEFAULT_PWD\$', 'ENC\$', 'HISTGRM\$', 'HIST_HEAD\$', 'LINK\$'
,'PDB_SYNC\$', 'SCHEDULER\$_CREDENTIAL', 'USER\$', 'USER_HISTORY\$', 'XS\$VERIFIERS')
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 '%CDC%'

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)

TABLE_NAME	PRIVILEGE	GRANTEE	DATABASE
USER\$	SELECT	CC_ITRS	3
USER\$	SELECT	CC_ITRS	4

Extended Evidence:

Statistics:

Query returned 2 rows

(2.22) 101367 Ensure 'ALL' Is Revoked on 'Sensitive' Tables(CIS-44)(oracle19:1:1621:POHK1CAT.hk. **HIGH** Passed standardchartered.com)

oracle19:1:1621:POHK1CAT.hk.standardchartered.com Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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
DATABASE FROM CDB_TAB_PRIVS A WHERE TABLE_NAME in
('CDB_LOCAL_ADMINAUTH\$','DEFAULT_PWD\$','ENC\$','HISTGRM\$','HIST_HEAD\$','LINK\$'
,'PDB_SYNC\$','SCHEDULER\$_CREDENTIAL','USER\$','USER_HISTORY\$','XS\$VERIFIERS')

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 '%CDC%'

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:POHK5CCD.hk. Failed **HIGH** standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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
DATABASE FROM CDB_TAB_PRIVS A WHERE TABLE_NAME in
('CDB_LOCAL_ADMINAUTH\$','DEFAULT_PWD\$','ENC\$','HISTGRM\$','HIST_HEAD\$','LINK\$'
,'PDB_SYNC\$','SCHEDULER\$_CREDENTIAL','USER\$','USER_HISTORY\$','XS\$VERIFIERS')

AND OWNER = 'SY

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 '%CDC%'

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)

TABLE_NAME	PRIVILEGE	GRANTEE	DATABASE
USER\$	SELECT	CC_ITRS	3
USER\$	SELECT	CC_PSS_VIEW	3

Extended Evidence:

Statistics:

Query returned 2 rows

(2.22) 101367 Ensure 'ALL' Is Revoked on 'Sensitive' Tables(CIS-44)(oracle19:1:1621:POHK1RCT.hk. **HIGH** standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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
DATABASE FROM CDB_TAB_PRIVS A WHERE TABLE_NAME in
('CDB_LOCAL_ADMINAUTH\$','DEFAULT_PWD\$','ENC\$','HISTGRM\$','HIST_HEAD\$','LINK\$','PDB_SYNC\$','SCHEDULER\$_CREDENTIAL','USER\$','USER_HISTORY\$','XS\$VERIFIERS')

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 '%CDC%'

Expected any of the selected values below:

Set status to PASS if no data found

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

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:POHK3CCD.hk. Failed **HIGH** standardchartered.com)

oracle19:1:1621:POHK3CCD.hk.standardchartered.com Instance

Failed Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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
DATABASE FROM CDB_TAB_PRIVS A WHERE TABLE_NAME in
('CDB_LOCAL_ADMINAUTH\$', 'DEFAULT_PWD\$', 'ENC\$', 'HISTGRM\$', 'HIST_HEAD\$', 'LINK\$'
,'PDB_SYNC\$', 'SCHEDULER\$_CREDENTIAL', 'USER\$', 'USER_HISTORY\$', 'XS\$VERIFIERS')
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 '%CDC''

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)

TABLE_NAME	PRIVILEGE	GRANTEE	DATABASE
USER\$	SELECT	CC_ITRS	3
USER\$	SELECT	CC_ITRS	4
USER\$	SELECT	CC_ITRS	5

Extended Evidence:

Statistics:

Query returned 3 rows

(2.22) 101367 Ensure 'ALL' Is Revoked on 'Sensitive' Tables(CIS-44)(oracle19:1:1621:POHK1CCD.hk. Failed HIGH standardchartered.com)

oracle19:1:1621:POHK1CCD.hk.standardchartered.com Instance

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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
DATABASE FROM CDB_TAB_PRIVS A WHERE TABLE_NAME in
('CDB_LOCAL_ADMINAUTH\$','DEFAULT_PWD\$','ENC\$','HISTGRM\$','HIST_HEAD\$','LINK\$'
,'PDB_SYNC\$','SCHEDULER\$_CREDENTIAL','USER\$','USER_HISTORY\$','XS\$VERIFIERS')
AND OWNIED__'SVE'

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 '%CDC''

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)

TABLE_NAME	PRIVILEGE	GRANTEE	DATABASE
USER\$	SELECT	CC_ITRS	3
USER\$	SELECT	CC_ITRS	4
USER\$	SELECT	CC_ITRS	5
USER\$	SELECT	CC ITRS	7

Extended Evidence:

Statistics:

Query returned 4 rows

(2.22) 101367 Ensure 'ALL' Is Revoked on 'Sensitive' Tables(CIS-44)(oracle19:1:1621:POHK4CCD.hk. Failed **HIGH** standardchartered.com)

oracle19:1:1621:POHK4CCD.hk.standardchartered.com Instance

Previous Status Failed

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

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

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

Scan Parameters:

DBOUERY:

SELECT TABLE_NAME, PRIVILEGE, GRANTEE, CON_ID
DATABASE FROM CDB_TAB_PRIVS A WHERE TABLE_NAME in
('CDB_LOCAL_ADMINAUTH\$', 'DEFAULT_PWD\$', 'ENC\$', 'HISTGRM\$', 'HIST_HEAD\$', 'LINK\$'
,'PDB_SYNC\$', 'SCHEDULER\$_CREDENTIAL', 'USER\$', 'USER_HISTORY\$', 'XS\$VERIFIERS')
AND OWNER = 'SYS'

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 '%CDC%'

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

Set status to PASS if no data found

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

TABLE_NAME	PRIVILEGE	GRANTEE	DATABASE
USER\$	SELECT	CC_ITRS	3
USER\$	SELECT	CC ITRS	4

Extended Evidence:

Statistics:

Query returned 2 rows

(2.22) 101367 Ensure 'ALL' Is Revoked on 'Sensitive' Tables(CIS-44)(oracle19:1:1621:POHK2CCD.hk. Failed **HIGH** standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 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
DATABASE FROM CDB_TAB_PRIVS A WHERE TABLE_NAME in
('CDB_LOCAL_ADMINAUTH\$','DEFAULT_PWD\$','ENC\$','HISTGRM\$','HIST_HEAD\$','LINK\$'
,'PDB_SYNC\$','SCHEDULER\$_CREDENTIAL','USER\$','USER_HISTORY\$','XS\$VERIFIERS')

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 '%CDC%'

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)

TABLE_NAME	PRIVILEGE	GRANTEE	DATABASE
USER\$	SELECT	CC_ITRS	3
USER\$	SELECT	CC_ITRS	4
USER\$	SELECT	CC_ITRS	6

Extended Evidence:

Statistics:

Query returned 3 rows

(2.23) 101337 Status of DB admin audit options_SLM-010(oracle19:1:1621:POHK1API.hk. standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(2.23) 101337 Status of DB admin audit options_SLM-010(oracle19:1:1621:POHK1CAT.hk. standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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:

(2.23) 101337 Status of DB admin audit options_SLM-010(oracle19:1:1621:POHK5CCD.hk. Passed MEDIUM standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(2.23) 101337 Status of DB admin audit options_SLM-010(oracle19:1:1621:POHK1RCT.hk. Passed MEDIUM standardchartered.com)

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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_LOGOFF_PRIVUSER
SCB_LOGON_ALL_FAILURES
SCB_AUDIT_DDL_POLICY

SCB_AUDIT_DROP_POLICY

Extended Evidence:

Statistics:

Query returned 4 rows

(2.23) 101337 Status of DB admin audit options_SLM-010(oracle19:1:1621:POHK3CCD.hk. standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(2.23) 101337 Status of DB admin audit options_SLM-010(oracle19:1:1621:POHK1CCD.hk. standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(2.23) 101337 Status of DB admin audit options_SLM-010(oracle19:1:1621:POHK4CCD.hk. standardchartered.com)

Passed

MEDIUM

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(2.23) 101337 Status of DB admin audit options_SLM-010(oracle19:1:1621:POHK2CCD.hk. standardchartered.com)

Passed MEDIUM

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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.hk. Passed MEDIUM standardchartered.com)

Instance oracle19:1:1621:POHK1API.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(2.24) 101366 Ensure secure encryption standards are configured(oracle19:1:1621:POHK1CAT.hk. Passed MEDIUM standardchartered.com)

Instance oracle19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(2.24) 101366 Ensure secure encryption standards are configured(oracle19:1:1621:POHK5CCD.hk. **Passed MEDIUM** standardchartered.com)

Instance oracle19:1:1621:POHK5CCD.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

Ensure secure encryption standards are configured

Ensure secure encryption standards are configured

Scan Parameters:

DBOUERY: 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

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

Instance oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Previous Status

Evaluation Date 08/04/2024 at 10:38:34 PM (GMT+0530)

Ensure secure encryption standards are configured

Ensure secure encryption standards are configured

Scan Parameters:

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

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:

(2.24) 101366 Ensure secure encryption standards are configured(oracle19:1:1621:POHK3CCD.hk. Passed MEDIUM standardchartered.com)

Instance oracle19:1:1621:POHK3CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(2.24) 101366 Ensure secure encryption standards are configured(oracle19:1:1621:POHK1CCD.hk. Passed MEDIUM standardchartered.com)

Instance oracle19:1:1621:POHK1CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(2.24) 101366 Ensure secure encryption standards are configured(oracle19:1:1621:POHK4CCD.hk. Passed MEDIUM standardchartered.com)

Instance oracle19:1:1621:POHK4CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

(2.24) 101366 Ensure secure encryption standards are configured(oracle19:1:1621:POHK2CCD.hk. Passed MEDIUM standardchartered.com)

Instance oracle19:1:1621:POHK2CCD.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:38:34 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

10.21.199.141 (hklpdps2b002.hk.standardchartered.com)

Red Hat Enterprise Linux Server 7.9 cpe:/o:redhat: enterprise_linux:7.9::server:

Controls:	196
Passed:	176 (89.8%)
Failed:	20 (10.2%)
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:	5f8ee406-02e2-0002-a436-a0423f33a5e6