No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.18) 101352 Ensure '_trace_files_public'ls Set to 'FALSE'(oracle19:1:1621:POHK1API2)

Passed HIGH

Instance oracle19:1:1621:POHK1API2

Previous Status Passed

Evaluation Date 08/04/2024 at 09:27:34 PM (GMT+0530)

Ensure '_trace_files_public'Is Set to 'FALSE'

Ensure '_trace_files_public'Is Set to 'FALSE'

Scan Parameters:

DBOUERY: 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:

Query returned 0 rows

(2.19) 101354 Ensure password complexity as per standards(oracle19:1:1621:POHK1API2)

Passed HIGH

Instance oracle19:1:1621:POHK1API2

Previous Status Passed

Evaluation Date 08/04/2024 at 09:27:34 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:POHK1RCT.hk.

Passed HIGH

standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 09:27:34 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

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

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:POHK1API2) **Passed** HIGH

Instance oracle19:1:1621:POHK1API2

Previous Status Passed

Evaluation Date 08/04/2024 at 09:27:34 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:POHK1RCT.hk. Passed **HIGH** standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 09:27:34 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')

SCHON'S 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

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

No data found

Extended Evidence:

Statistics:

Instance

Query returned 0 rows

(2.21) 101361 Ensure 'GRANT ANY ROLE' Is Revoked from Unauthorized 'GRANTEE'(CIS-59)

Passed HIGH

(oracle19:1:1621:POHK1API2) oracle19:1:1621:POHK1API2

Previous Status Passed

08/04/2024 at 09:27:34 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 FROM DBA_313_FRIVS
WHERE PRIVILEGE FROM DBA_USERS WHERE
ORACLE_MAINTAINED='Y') AND GRANTEE NOT IN (SELECT ROLE FROM DBA_ROLES WHERE ORACLE_MAINTAINED='Y')
AND GRANTEE not in ('SECADMIN', 'SCB_ADMIN', 'SPATIAL_WFS_ADMIN_USR', 'SPATIAL_CSW_ADMIN_USR', 'PUPPETAM',
'HCVPWDMANID_ROOT', 'HCVPWDMANID')

Expected any of the selected values below:

Set status to PASS if no data found

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.21) 101361 Ensure 'GRANT ANY ROLE' Is Revoked from Unauthorized 'GRANTEE'(CIS-59) **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 09:27:34 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:

Query returned 0 rows

(2.22) 101367 Ensure 'ALL' Is Revoked on 'Sensitive' Tables(CIS-44)(oracle19:1:1621:POHK1API2) **Failed HIGH**

Instance oracle19:1:1621:POHK1API2

Previous Status Failed

Evaluation Date 08/04/2024 at 09:27:34 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:POHK1RCT.hk. Passed **HIGH** standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 09:27:34 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
OPACLE MAINTAINED_'V')

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

(2.23) 101337 Status of DB admin audit options_SLM-010(oracle19:1:1621:POHK1API2)

oracle19:1:1621:POHK1API2 Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 09:27:34 PM (GMT+0530)

Oracle_ATOS - 20240806 page 774

Passed

MEDIUM

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. standardchartered.com)

Passed MEDIUM

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

Previous Status Passed

Evaluation Date 08/04/2024 at 09:27:34 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:POHK1API2) Passed MEDIUM

Instance oracle19:1:1621:POHK1API2

Previous Status Passed

Evaluation Date 08/04/2024 at 09:27:34 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:POHK1RCT.hk. Passed MEDIUM standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 09:27:34 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

10.21.199.144 (hklpdps2b003.hk.standardchartered.com)

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

Controls:	294
Passed:	270 (91.84%)
Failed:	24 (8.16%)
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:	5f8f4b9d-02e0-0002-9c5b-a0423f33a5e6

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, OCT_2020_ALL_STATUS_ASIA_Mannual, ALL_STATUS_HONG_KONG_PROD, 2021 Q1 Validation Internal, ICV-OS-Red Hat Enterprise Linux, AIVS_ASS_ASIA_UNIX_PROD, 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, May_2022_GDC_CDC_NC_scanned, 2022 Q3 Validation Internal, Aug_2022_GDC_CDC_NC_scanned, Sep_2022_GDC_CDC_NC_scanned, Oct_2022_GDC_CDC_NC_scanned, In Scope Asset Groups, OpenSSL-Asia-Prod, Nov_2022_GDC_CDC_NC_scanned, 2022 Q4 Validation Internal, Purge Activity, Jan_2023_CDC_GDC_NC_Scanned, Feb_2023_CDC_GDC_NC_Scanned, Self_Service_AG_UM, 2023_Q1 Validation Internal, Mar_2023_CDC_GDC_NC_Scanned, Apr_2023_CDC_GDC_NC_Scanned, Apr_2023_CDC_GDC_NC_Scanned, Apr_2023_CDC_GDC_NC_Scanned, Apr_2023_CDC_GDC_NC_Scanned, Apr_2023_CDC_GDC_NC_Scanned, Apr_2023_CDC_GDC_NC_Scanned, Apr_2023_CDC_GDC_NC_Scanned, Apr_2023_CDC_GDC_NC_Scanned, 2023_Q2 Validation Internal, AlVS_ASS_Server_All, Jun_2023_CDC_GDC_NC_Scanned, Sep_2023_CDC_GDC_NC_Scanned, Apr_2024_GDC_EAST, Jan_2024_CDC_GDC_NC_Scanned, April_2024_GDC_EAST, Feb_2024_GDC_NC_Scanned, MAR_2024_GDC_EAST, May_2024_GDC_EAST, May_2024_GDC_EAST, May_2024_GDC_EAST, May_2024_GDC_EAST, May_2024_GDC_EAST, May_2024_GDC_EAST, April_2024_CDC_GDC_NC_Scanned, AUTH REPORT, JUL_2024_GDC_EAST, CVE-2024-6387-Asia Remaining, July_2024_CDC_GDC_

Oracle 19c

1. Database Controls

(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 10:09:56 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	30)
	FALSE	
Extended E	vidence:	
NAME		VALUE
remote_os_au	ıthent	FALSE
remote_os_au	ıthent	FALSE
remote_os_authent		FALSE

(1.1) 1049 Status of the 'remote_os_authent(remote OS authentication without password)' setting via Passed HIGH 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 10:09:56 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	30)
	FALSE	
Extended I	Evidence:	
NAME		VALUE
remote_os_a	uthent	FALSE
remote_os_a	uthent	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:POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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	30)
	FALSE	
Extended E	vidence:	
NAME		VALUE
remote_os_au	ıthent	FALSE
remote_os_au	ıthent	FALSE
remote_os_au	ıthent	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 10:09:56 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:POHK1RCT.hk. Passed HIGH standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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:POHK1API3) Passed HIGH

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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+0	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:POHK1CAT.hk.standardchartered.com)

Passed HIGH

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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_security		TRUE

TRUE

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

Passed HIGH

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

Previous Status Passec

sql92_security

Evaluation Date 08/04/2024 at 10:09:56 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.

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_secur	ity	TRUE
sql92_secur	ity	TRUE
sql92_secur	ity	TRUE

(1.3) 1057 Status of the 'sql92_security=' (table-level SELECT privileges) in init.ora (oracle19:1:1621:POHK1API3)

Passed HIGH

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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	vidence:	
NAME		VALUE
sql92_securit	ý.	TRUE
sql92_securit	ý	TRUE
sal92 security		TRUE

(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 10:09:56 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+053	30)	
	EXCLUSIVE		
Extended E	vidence:		
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 POHK1RCT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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 I	Extended Evidence:		
NAME	AME 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 POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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	pected 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	NAME VALUE		
remote_login_passwordfile		EXCLUSIVE	
remote_login_passwordfile		EXCLUSIVE	
remote_login_passwordfile		EXCLUSIVE	

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

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 PM (GMT+0530)

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

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

Expected matches regular expression list .*(\-\-\-|\-\-x|\-w\r\-\-|\r\-x|r\-\-|\r\-x|r\-\-|\r\-x|r\-\-|\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:POHK1RCT.hk. Passed HIGH standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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)(\-\-\-\-\-\x r\-\-\-\x r\-\-\-\x r\-\-\x x\-\-\-\x x\-\-\-\x\x\x\x\x\x\x\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:POHK1API3) Passed HIGH

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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)(\-\-\-\-\-\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)
	root:root:r-xr-xr-x:/bin

(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 10:09:56 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.

permissions.		
matches regular expression list		
.*(\-\-\-\-\-\-\-\-\-\r\-x)(\-\-\-\-\-\-\-\-\-\-\-\-\\-\-\-\-\\-\\-		
OR, any of the selected values below:		
File not found		
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 10:09:56 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	
	.*(\-\-\-\\-\x \-wx r\-\- r\-x rw\- rwx)(\-\-\-\-\-\x r\-\-\r\-x r\-\-\r\-x 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	

(1.6) 3463 Permissions set for the 'ORACLE_HOME' directory(oracle19:1:1621:POHK1API3) Failed HIGH

Instance oracle19:1:1621:POHK1API3

Previous Status Failed

Evaluation Date 08/04/2024 at 10:09:56 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.

9 Pro-	, Feetings - 1 Feet	
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)	
	File not found	

Cause of Failure:

Unexpected values	Additional values found in failed controls:	
	File not found	
Missing values	Expected values not found in failed controls:	
	.*(\-\-\-\\-\\-\\-\\-\\-\\-\\-\\-\\-\\-\\-	
	OR, any of the selected values below:	

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

Passed MEDIUM

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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)

/u01/app/oracle/local/scripts/BANNER/dbbanner.txt

Extended Evidence:

File name
Setting
Value
/u01/app/oracle/local/network/admin/sqlnet.
ora
SEC_USER_AUDIT_ACTION_BANNER
/u01/app/oracle/local/scripts/BANNER/dbbanner.txt

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

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

Previous Status Failed

Evaluation Date 08/04/2024 at 10:09:56 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	Actual Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)		
Actual		0.01.03 1 M (CM170330)	
	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

(1.7) 3498 Status of the 'SEC_USER_AUDIT_ACTION_BANNER' parameter in sqlnet.ora Faile (oracle19:1:1621:POHK1API3)

Failed MEDIUM

Instance oracle19:1:1621:POHK1API3

Previous Status Failed

Evaluation Date 08/04/2024 at 10:09:56 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.

·	s zot ourig talle(s) it illumine the line and pain defined for the oze-courig terror - retroit zot have been also equivalent
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)
Actual	Last Opuated.00/04/2024 at 00.01.03 FM (GM1+0330)
	File not found
Extended E	Evidence:
Information	
File not found	d, please verify authentication record file paths.

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:POHK1CAT.hk. standardchartered.com)

Passed MEDIUM

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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:POHK1RCT.hk	Passed	MEDILIM

standardchartered.com)

oracle 19:1:1621:POHK1RCT.hk. standard chartered.comInstance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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:POHK1API3) **Passed MEDIUM**

oracle19:1:1621:POHK1API3 Instance

Previous Status Passed

08/04/2024 at 10:09:56 PM (GMT+0530) **Evaluation Date**

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 (O)	

Extended Evidence:	
VALUE	
0	

(1.9) 5676 Current installed Oracle version(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 10:09:56 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:POHK1API3)

Passed HIGH

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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:POHK1CAT.hk.standardchartered. Passed HIGH com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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.

TP1 C 11 ·	Trace 1 (ANC) is a day of the field of the control
	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 E	vidence:
VERSION	
19.2	
(1.10) 8033	Setting for the 'sec_case_sensitive_logon' parameter(oracle19:1:1621:POHK1RCT.hk. Passed MEDIUM standardchartered.com)
Instance	oracle19:1:1621:POHK1RCT.hk.standardchartered.com
Previous Status	
Evaluation Dat	e 08/04/2024 at 10:09:56 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 to meter to TRUE if the October 2012 CPU/PSU or later was applied. If the patch was not applied it is ed to set this parameter to FALSE to avoid this vulnerability.
The following been implement	List String value X indicates the status of the sec_case_sensitive_logon parameter. A value of TRUE shows that case-sensitive login has ented.
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	······································
VALUE	
TRUE	
TRUE	
TRUE	
(4.48) 2000	0.41-4.41-1.41-4.42-4.42-4.42-4.42-4.42-4
•	Setting for the 'sec_case_sensitive_logon' parameter(oracle19:1:1621:POHK1API3) Passed MEDIUM
Instance Previous Status	oracle19:1:1621:POHK1API3 s Passed
Evaluation Dat	
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 to meter to TRUE if the October 2012 CPU/PSU or later was applied. If the patch was not applied it is ed to set this parameter to FALSE to avoid this vulnerability.
The following been implement	
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	Svidence:
VALUE	-viuence.
TRUE	
TRUE	
TRUE	
INCL	
(1.10) 8033	Setting for the 'sec_case_sensitive_logon' parameter(oracle19:1:1621:POHK1CAT.hk. Passed MEDIUM standardchartered.com)
Instance Previous Statu	oracle19:1:1621:POHK1CAT.hk.standardchartered.com s Passed
Evaluation Dat	e 08/04/2024 at 10:09:56 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 to 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 has ented.
Expected	matches regular expression list
	TRUE
	OR, any of the selected values below:
	Parameter not found
A = (1	L ==(Llm d=(= d 00/04/0004 =(00-04/00 RM (OMT 0000)
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)
	TRUE
Extended E	Evidence:
VALUE	
TRUE	
TRUE	
TRUE	
(1.11) 8034	Status of the 'sec_max_failed_login_attempts' parameter setting(oracle19:1:1621: Passed HIGH POHK1RCT.hk.standardchartered.com)
Instance	oracle19:1:1621:POHK1RCT.hk.standardchartered.com
Previous Statu	
Evaluation Dat	e 08/04/2024 at 10:09:56 PM (GMT+0530)
the login co brute-force	AX_FAILED_LOGIN_ATTEMPTS parameter determines the number of failed logins that can occur before Oracle close nnection. 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

Oracle_ATOS - 20240806 page 790

Extended Evidence:

VALUE			
3			
3			
3			
(1.11) 8034	Status of the 'sec_max_failed_login_attempts' parameter setting(oracle19:1:1621: Pas POHK1API3)	ssed H	IGН
Instance	oracle19:1:1621:POHK1API3		
Previous Statu			
Evaluation Da	te 08/04/2024 at 10:09:56 PM (GMT+0530)		
the login co brute-force	MAX_FAILED_LOGIN_ATTEMPTS parameter determines the number of failed logins that can occurrence on nection. As not limiting the number of failed login attempts for a user connection can facile login attacks and the occurrence of Denial-of-Service conditions, this value should be set are organization.	ilitate both	
The followin requirement	ng List String value X indicates the status of the sec_max_failed_login_attempts parameter. A value of 1 - UNLIM has been implemented.	IITED shows t	hat 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 I	Evidence:		
VALUE			
3			
3			
3			
(1.11) 8034	Status of the 'sec_max_failed_login_attempts' parameter setting(oracle19:1:1621: Parameter Status of the 'sec_max_failed_login_attempts	ssed H	IGH
Instance	oracle19:1:1621:POHK1CAT.hk.standardchartered.com		
Previous Statu			
Evaluation Da	tte 08/04/2024 at 10:09:56 PM (GMT+0530)		
the login co brute-force	MAX_FAILED_LOGIN_ATTEMPTS parameter determines the number of failed logins that can occurrence on nection. As not limiting the number of failed login attempts for a user connection can facile login attacks and the occurrence of Denial-of-Service conditions, this value should be set are organization.	ilitate both	
The followin requirement	ng List String value X indicates the status of the sec_max_failed_login_attempts parameter. A value of 1 - UNLIN has been implemented.	IITED shows t	hat 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 I	Evidence:		
VALUE			
3			
3			
3			

(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 10:09:56 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 Evidence:			
VALUE			
CONTINUE			
CONTINUE			
CONTINUE			

Cause of Failure:

Unexpected values	Additional values found in failed controls:
	CONTINUE
Missing values	Expected values not found in failed controls:
	^\(DROP3\)\$
	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 POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Failed

Evaluation Date 08/04/2024 at 10:09:56 PM (GMT+0530)

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

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

Expected matches regular expression list

^\(DROP\,3\)\\$

OR, any of the selected values below:

Parameter not found

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

CONTINUE

Extended Evidence:

VALUE

CONTINUE	
CONTINUE	
CONTINUE	

Cause of Failure:

Unexpected values	Additional values found in failed controls:
	CONTINUE
Missing values	Expected values not found in failed controls:
	^\(DROP3\)\$
	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 10:09:56 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.

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 POHK1RCT.hk.standardchartered.com)

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

Previous Status Failed

Evaluation Date 08/04/2024 at 10:09:56 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	
VALUE	-viuence.
TRACE	
TRACE	
TRACE	
Cause of F	ailure:
Unexpecte	d Additional values found in failed controls:
values	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 POHK1API3)
Instance	oracle19:1:1621:POHK1API3
Previous Statu	
Evaluation Dat	e 08/04/2024 at 10:09:56 PM (GMT+0530)
packets rec packets car Denial-of-So	ROTOCOL_ERROR_TRACE_ACTION setting determines the Oracle's server's logging response level to bad/malformed eived from the client, by generating ALERT, LOG, or TRACE levels of detail in the log files. As incoming bad a 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 s 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	
INACE	

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 POHK1CAT.hk.standardchartered.com)

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

Previous Status Failed

Evaluation Date 08/04/2024 at 10:09:56 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.

	o croute a trace me mas seen impremented.
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:POHK1RCT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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	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:POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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

(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

FALSE FALSE

Evaluation Date 08/04/2024 at 10:09:56 PM (GMT+0530)

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

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

Expected matches regular expression list FALSE OR, any of the selected values below: Parameter not found

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

(1.15) 9597 Ownership and permissions set on \$ORACLE_HOME/network/admin directory and files 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 10:09:56 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).* | ``grid \circ install \circ (0|1|2|3|4|5|6|7)(0|1|4|5).* | ``grid \circ install \circ (0|1|4|5).* | ``grid \circ (0|1|4|5).* | ``grid \circ (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/shrept.lst

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

Extended Evidence:

Owner Group Perm FileName 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

(1.15) 9597 Ownership and permissions set on \$ORACLE_HOME/network/admin directory and files Failed HIGH (oracle19:1:1621:POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Failed

Evaluation Date 08/04/2024 at 10:09:56 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).* | ``grid \circ install \circ (0|1|4|5).* | ``grid \circ (0$

OR, any of the selected values below:

File(s) not found

Actual Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)
File(s) not found

Extended Evidence:
File name
/network/admin

Cause of Failure:

Unexpected values

Additional values found in failed controls:

File(s) not found

Missing values

Expected values not found in failed controls:

^oracle\ oinstall\ (0|1|2|3|4|5|6|7)(0|1|4|5).*|^grid\ oinstall\ (0|1|2|3|4|5|6|7)(0|1|4|5).*

OR, any of the selected values below:

(1.15) 9597 Ownership and permissions set on \$ORACLE_HOME/network/admin directory and files 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 10:09:56 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

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

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

Extended Evidence:

Owner Group Perm FileName

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

(1.16) 9598 Ownership and permissions set on \$ORACLE_HOME/dbs and \$ORACLE_HOME/dbs/*(oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

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

Previous Status Failed

Evaluation Date 08/04/2024 at 10:09:56 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

Failed

HIGH

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

 $$$\operatorname{constall} (0|1|2|3|4|5|6|7)(0|1|4|5). $$\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_1_14651038828910_27-04-2020

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

 $oracle\ oinstall\ 640\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/spfile RESTOR 19. oracle\ oinstall\ 640\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/spfile RESTOR 19. oracle oinstall\ 640\ /u01/app/oracle/product/db/19. oracle oinstall\ 640\ /u01/app/oracle oinstall\ 640\ /u01/app/oracle$

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

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

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

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

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

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

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

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/dbs/*(oracle19:1:1621:POHK1API3)

Failed

HIGH

Instance oracle19:1:1621:POHK1API3

Previous Status Failed

Evaluation Date 08/04/2024 at 10:09:56 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

OR, any of the selected values below:

	File(s) not found	
	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)	
	File(s) not found	
Extended Evidence:		
File name	ime	
/dbs		

Cause of Failure:

Unexpected values	Additional values found in failed controls:	
	File(s) not found	
Missing values	Expected values not found in failed controls:	
	$ \begin{tabular}{ll} $$ \operatorname{oinstall} (0 1 2 3 4 5 6 7)(0 1 4 5).* & \operatorname{oracle} (0 1 2 3 4 5 6 7)(0 1 4 5).* \\ \end{tabular} $	
	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 10:09:56 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.

required permission level of 0750. Expected matches regular expression list

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

 $oracle\ oinstall\ 640\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/snapcf_DUK 31BLD 1.f$

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

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

 $oracle\ oinstall\ 640\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/db_arch_DUK 31BLD_dmuumh 6c_1_1_14621038828748_27-04-2020$ $oracle\ oinstall\ 640\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/db_arch_DUK 31BLD_dluumh 6c_1_1_14611038828748_27-04-2020$

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

 $oracle\ oinstall\ 640\ /u01/app/oracle/product/db/19.7.0.0. Apr 2020/dbs/snapcf_DUK 31BLD 1.foracle\ oinstall\ 640\ /u01/app/oracle/product/db/19.7.0. Apr 2020/dbs/snapcf_DUK 31BLD 1.foracle\ oinstall\ 640\ /u01/app/oracle/product/db/19.7. Apr 2020/dbs/snapcf_DUK 31BLD 1.foracle\ oinstall\ 640\ /u01/app/oracle/product/db/19.0. Apr 2020/dbs/snapcf_DUK 31BLD 1.foracle\ oinstall\ 640\ /u01/app/oracle\ oinstall\ 640\$

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

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:POHK1API3)

Passed MEDIUM

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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 unined additing is chabled.			
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	ETER VALUE		
Unified Auditing		TRUE	

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

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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 additing is enabled.								
Expected	regular expression match							
	TRUE							
	OR, any of the selected values below:							
	Setting not found							
	Table not found							
Actual	Local Lindoted-09/04/2024 at 06-04-00 DM (CMT-05)	201						
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+053	ou)						
	TRUE							
Extended Evidence:								
PARAMETER	PARAMETER VALUE							
Unified Auditin	ng	TRUE						

(1.17) 12623 Status of Unified Auditing mode(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 10:09:56 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				
A = 1 1					
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)				
	TRUE				
Extended E	vidence:				
PARAMETER		VALUE			
Unified Auditi	ησ	TRUE			

(1.18) 12624 Status of policies enabled for Unified Auditing(oracle19:1:1621:POHK1API3) **MEDIUM Passed**

oracle19:1:1621:POHK1API3 Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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 CHARLES AND A CONTROL OF THE CON

Expected	contains ro	gular expression list					
xpecteu		•					
		_DDL_POLICY:.*:.*:					
		_DROP_POLICY:.*:.*					
		N_ALL_FAILURES:.*:.*:.*					
		N_LOGOFF_PRIVUSER:.*:.*:					
	OR, any of	the selected values below					
	Setting not	found					
	Table not f	ound					
ctual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)						
	ALL USERS:SO	B_AUDIT_DDL_POLICY:BY USI	ER:YES:YES				
	ALL USERS:SO	B_AUDIT_DROP_POLICY:BY U	SER:YES:YES				
	ALL USERS:SO	B_LOGON_ALL_FAILURES:BY	USER:NO:YES				
	ALL USERS:SO	B_LOGON_LOGOFF_PRIVUSER	R:BY USER:YES:YES				
xtended E	Evidence:						
NTITY_NAN		POLICY_NAME	ENABLED_OPTION	SUCCESS	FAILURE		
LL USERS		SCB_LOGON_LOGOFF_PRIVUSER	BY USER	YES	YES		
LL USERS		SCB_LOGON_ALL_FAILURES	BY USER	NO	YES		
I HEEDE		SCB_AUDIT_DDL_POLICY	BY USER	YES	YES		
LL USERS							

(1.18) 12624 Status of policies enabled for Unified Auditing(oracle19:1:1621:POHK1CAT.hk. standardchartered.com)

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

Previous Status

Evaluation Date

contains regular expression list .*:SCB AUDIT DDL POLICY:.*:.*:

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_DROP_POLICY:.*:.*								
	.*:SCB_LOGON_ALL_FAILURES:.*:.*								
	.*:SCB_LOGON_LOGOFF_PRIVUSER:.*:.*								
	OR, any of the	he selected values below:	1						
	Setting not	found							
	Table not fo	ound							
Actual	Last Undata	d:08/04/2024 at 06:01:09 F	OM (CMT+0520)						
Actual	-								
	ALL USERS:SC	B_AUDIT_DDL_POLICY:BY USF	ER:YES:YES						
	ALL USERS:SC	B_AUDIT_DROP_POLICY:BY U	SER:YES:YES						
	ALL USERS:SC	B_LOGON_ALL_FAILURES:BY I	JSER:NO:YES						
	ALL USERS:SC	B_LOGON_LOGOFF_PRIVUSER	::BY USER:YES:YES						
Extended E	vidence:								
ENTITY_NAM	ΙE	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				

YES

YES

MEDIUM

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

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

SCB_AUDIT_DROP_POLICY BY USER

Previous Status Passed

ALL USERS

08/04/2024 at 10:09:56 PM (GMT+0530) **Evaluation Date**

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

MEDIUM Passed

Instance

08/04/2024 at 10:09:56 PM (GMT+0530)

page 803

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

(1.19) 12707 Status of 'extproc' in listener.ora(oracle19:1:1621:POHK1API3)

Failed HIGH

Instance oracle19:1:1621:POHK1API3

Previous Status Failed

Evaluation Date 08/04/2024 at 10:09:56 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

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)

File not found

Extended Evidence:

Information

File not found, please verify authentication record file paths.

Cause of Failure:

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

(1.19) 12707 Status of 'extproc' in listener.ora(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 10:09:56 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 (G	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:POHK1CAT.hk.standardchartered. **Passed** HIGH com)

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

Passed **Previous Status**

08/04/2024 at 10:09:56 PM (GMT+0530) **Evaluation Date**

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 para	nmeter 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/ora	cle/local/network/admin/listener.ora	EXTPROC				

(1.20) 14340 Status of auditing for 'CREATE USER' privilege (Unified Auditing)(oracle19:1:1621: **Passed MEDIUM** POHK1API3)

oracle19:1:1621:POHK1API3 Instance

Previous Status Passed

OLICY

Evaluation Date 08/04/2024 at 10:09:56 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 separated value	List Strii ies of po	ng value(s) of X indi licy_name, audit_op	cates the status of the ption, audit_option_typ	CREATE USER audit e, success, failure, er	option type defined on abled_option, and en	n the database. The ou tity_name.	itput contains colon			
Expected	matches regular expression list									
	.*:CREA	.*:CREATE USER:.*:YES:YES:.*:.*								
	OR, ar	ny of the selected	d values below:							
	Setti	ing not found								
	Tabl	le 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 Ex	vidence	e:								
POLICY_NAM	E A	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCR AUDIT D	DI P- C	REATE LISER	STANDARD ACTION	YFS	YFS	BY LISER	ALL LISERS			

(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 10:09:56 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	matches regular expression list								
	.*:CRE	.*:CREATE USER:.*:YES:YES:.*:*								
	OR, any of the selected values below:									
	Set	ting not found								
	Ta	ble 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										
Extended	Extended Evidence:									
POLICY_NAI	ME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCB_AUDIT_ OLICY	DDL_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 10:09:56 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	matcl	natches regular expression list						
	.*:CRE	.*:CREATE USER:.*:YES:YES::*:.*						
	OR, any of the selected values below:							
	Setting not found							
Table not found								
Actual		_ast 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							
	SCB_AUDIT_DDL_POLICY:CREATE USER:SYSTEM PRIVILEGE: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-	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	

(1.21) 14341 Status of auditing for 'ALTER USER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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 *:ALTER USER:.*:YES:YES:.*:.* OR, any of the selected values below: Setting not found Table not found Actual Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) SCB_AUDIT_DDL_POLICY:ALTER USER:STANDARD ACTION:YES:YES:BY USER:ALL USERS **Extended Evidence:** POLICY_NAME AUDIT OPTION AUDIT OPTION TYPE SUCCESS **FAILURE** ENABLED OPTION ENTITY NAME SCB_AUDIT_DDL_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 POHK1RCT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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:** POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS **FAILURE** ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_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 10:09:56 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

.*:/	LTER USER:.*:YES:YES:.*	*					
OF	OR, any of the selected values below:						
	Setting not found						
	Table not found						
Actual La	st Updated:08/04/202	24 at 06:01:09 PM ((GMT+0530)				
SC	B_AUDIT_DDL_POLICY:A	ALTER USER:STANDAF	RD ACTION:YES:YES:B	Y USER:ALL USERS			
SC	B_AUDIT_DDL_POLICY:#	ALTER USER:SYSTEM	PRIVILEGE:YES:YES:B	Y USER:ALL USERS			
Extended Evide	nce:						
POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_DDL_ OLICY	P- ALTER USER	SYSTEM PRIVILEGE	YES	YES	BY USER	ALL USERS	
SCB_AUDIT_DDL_ OLICY	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 POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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:							
	Set	tting not found						
	Ta	ble not found						
Actual	1	Llm dete 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:I	DROP USER:STANDAR	D ACTION:YES:YES:BY	USER:ALL USERS			
Extended Ex	/iden	ce:						
POLICY_NAM	Е	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_D	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 POHK1RCT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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.

1	y = y = y = y
Expected	matches regular expression list
	.*:DROP 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	B_AUDIT_DDL_POLICY:	DROP USER:STANDAR	D 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 OLICY	_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 POHK1CAT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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.

Extended Evidence:								
POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_DDL_P- OLICY	DROP USER	SYSTEM PRIVILEGE	YES	YES	BY USER	ALL USERS		
SCB_AUDIT_DDL_P- OLICY	DROP USER	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.23) 14343 Status of auditing for 'CREATE ROLE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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_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 E	vidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_P- OLICY	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: POHK1RCT.hk.standardchartered.com) **Passed MEDIUM**

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

Previous Status

Evaluation Date 08/04/2024 at 10:09:56 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						
	.*:CRE	ATE ROLE:.*:YES:YES:	.*.*				
	OR, any of the selected values below:						
	Setting not found						
	Tal	ble not found					
Astront	1	Lll	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:0	CREATE ROLE:STANDA	ARD 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-	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)

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

Previous Status

08/04/2024 at 10:09:56 PM (GMT+0530) **Evaluation Date**

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 separated value	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 eparated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.								
Expected	matc	hes regular expre	ssion list						
	.*:CRE	.*:CREATE ROLE:.*: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_A	AUDIT_DDL_POLICY:0	CREATE ROLE:STANDA	ARD ACTION:YES:YES:	BY USER:ALL USERS				
	SCB_A	AUDIT_DDL_POLICY:0	CREATE ROLE:SYSTEM	1 PRIVILEGE: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	SYSTEM PRIVILEGE	YES	YES	BY USER	ALL USERS		
SCB_AUDIT_D OLICY	DL_P-	CREATE ROLE	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.24) 14344 Status of auditing for 'ALTER ROLE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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. matches regular expression list **Expected** *:ALTER 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:ALTER ROLE: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 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)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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.

separated valu	es of p	olicy_name, audit_op	tion, audit_option_typ	e, success, failure, en	abled_option, and ent	ity_name.	•	
Expected	Expected matches regular expression list							
	.*:ALT	ER ROLE:.*:YES:YES:.*	·. * 					
	OR, any of the selected values below:							
	Set	ting not found						
	Tal	ole not found						
Actual	Loot	l la data d.00/04/20	24 at 06:04:00 DM /	CMT - 0520\				
Actual	Last	Updated:06/04/20/	24 at 06:01:09 PM (GIVI I +0530)				
	SCB_A	AUDIT_DDL_POLICY:/	ALTER ROLE:STANDAF	RD ACTION:YES:YES:B	Y 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 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 POHK1CAT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 PM (GMT+0530)

The 'ALTER ROLE' command is a powerful database tool, allowing the alteration of a 'role' that can be assigned to a large

numbers of users who need the same object/system privileges. Logging and monitoring of all attempts to alter roles, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

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

Expected	matches regular expression list									
	.*:ALT	.*:ALTER ROLE:.*:YES:YES:.*:.*								
	OR, any of the selected values below:									
	Set	ting not found								
	Tal	ole not found								
Actual	Lact		24 at 06:01:09 PM (CMT+0530)						
Actual		_ -		•	WHOED ALL HODDO					
	SCB_F	AUDIT_DDL_POLICY:A	LTER ROLE:STANDAF	RD ACTION:YES:YES:B	Y USER:ALL USERS					
Extended E	vidend	e:								
POLICY_NAM	Е	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			

(1.25) 14345 Status of auditing for 'DROP ROLE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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.

separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.							
Expected matches regular expression list							
	.*:DRC	OP ROLE:.*:YES:YES:.*:	. *				
	OR, any of the selected values below:						
	Set	ting not found					
	Table not found						
A . 4 . 1		11 - 1 - 4 - 1 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_A	AUDIT_DDL_POLICY:I	OROP ROLE:STANDAR	D ACTION:YES:YES:I	BY USER: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-	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 POHK1RCT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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, a	PR, any of the selected values below:						
	Set	Setting not found						
	Tal	ole not found						
Actual	Last	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 E	viden	ce:						
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 POHK1CAT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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	natches regular expression list						
	.*:DRC	OP ROLE:.*:YES:YES:.*:	*					
	OR, a	any of the selected	I values below:					
	Set	ting not found						
	Tal	ole not found						
Actual	Lact		24 at 06:01:09 PM (CMT - 0530\				
Actual	Lasi	Opualeu.00/04/202	4 at 00.01.09 Fivi (GW1 +0330)				
	SCB_A	AUDIT_DDL_POLICY:E	ROP ROLE:STANDAR	D ACTION:YES:YES:BY	USER:ALL USERS			
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 ROLE	STANDARD ACTION	YES	YES	BY USER	ALL USERS	

(1.26) 14346 Status of auditing for 'GRANT' privilege (Unified Auditing)(oracle19:1:1621:POHK1API3) Passed MEDIUM

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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.

separated valu	les 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

(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 10:09:56 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.

separated value	ies of p	olicy_name, audit_op	tion, audit_option_typ	e, success, failure, en	abled_option, and enti	ity_name.	ilitaliis cololi	
Expected	matc	matches regular expression list						
	.*:GRA	*:GRANT:.*:YES:YES:.**						
	OR, any of the selected values below:							
	Set	ting not found						
	Table not found							
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM ((GMT+0530)				
	SCB_AUDIT_DDL_POLICY:GRANT:STANDARD ACTION:YES:YES:BY USER:ALL USERS							
Extended E	vidend	e:						
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_D OLICY	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:POHK1CAT. Passed MEDIUM hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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	List String value(s) of X indicates the status of the GRANT audit option type defined on the database. The output contains colon use 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	_ast Updated:08/04/20	st Updated:08/04/2024 at 06:01:09 PM (GMT+0530)							
C	CB_AUDIT_DDL_POLICY:	GRANT:STANDARD AC	TION:YES:YES:BY USE	R:ALL USERS					
Extended Evi	dence:								
POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCB_AUDIT_DD	L_P- GRANT	STANDARD ACTION	YES	YES	BY USER	ALL USERS			

(1.27) 14347 Status of auditing for 'REVOKE' privilege (Unified Auditing)(oracle19:1:1621: POHK1API3)

Passed MEDIUM

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 PM (GMT+0530)

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

The following List String value(s) of X indicates the status of the REVOKE audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name. **Expected** matches regular expression list *:REVOKE:.*:YES:YES:.*:.* OR, any of the selected values below: Setting not found Table not found Actual Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) SCB_AUDIT_DDL_POLICY:REVOKE:STANDARD ACTION:YES:YES:BY USER:ALL USERS **Extended Evidence:** POLICY_NAME AUDIT OPTION AUDIT_OPTION_TYPE SUCCESS **FAILURE** ENTITY_NAME ENABLED_OPTION SCB_AUDIT_DDL_P- REVOKE OLICY STANDARD ACTION YES YES BY USER ALL USERS

(1.27) 14347 Status of auditing for 'REVOKE' 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 10:09:56 PM (GMT+0530)

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

The following List String value(s) of X indicates the status of the REVOKE audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name. **Expected** matches regular expression list .*:REVOKE:.*:YES:YES:.*:.* OR, any of the selected values below: Setting not found Table not found Actual Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) SCB_AUDIT_DDL_POLICY:REVOKE:STANDARD ACTION:YES:YES:BY USER:ALL USERS **Extended Evidence:** AUDIT_OPTION_TYPE SUCCESS POLICY_NAME AUDIT_OPTION **FAILURE** ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P- REVOKE STANDARD ACTION YES BY USER ALL USERS YES

(1.27) 14347 Status of auditing for 'REVOKE' 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 10:09:56 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 val	List St ues of p	ring value(s) of X indi policy_name, audit_op	cates the status of the tion, audit_option_typ	REVOKE audit option be, success, failure, en	type defined on the cabled_option, and ent	database. The output o ity_name.	contains colon
Expected	mato	matches regular expression list					
	.*:RE\	.*:REVOKE:.*:YES:YES:.*:.*					
	OR,	OR, any of the selected values below:					
	Se	Setting not found					
	Table not found						
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM ((GMT+0530)			
	SCB_AUDIT_DDL_POLICY:REVOKE: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 OLICY	DDL_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 POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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	ed value	es of policy_name, au	dit_option, audit_optic	on_type, success, failu	re, enabled_option, ar	nd 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 E	videnc	e:					
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 10:09:56 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 expre	ssion list						
	:CREATE PROFILE:.: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:0	CREATE PROFILE:STAI	NDARD ACTION:YES:Y	ES:BY USER:ALL USEF	RS			
Extended Ev	vidence:							
POLICY_NAMI	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 POHK1CAT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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	matc	natches regular expression list						
	.*:CRE	*:CREATE PROFILE::*:YES:YES::*:.*						
	OR, a	OR, any of the selected values below:						
	Set	Setting not found						
	Tal	ole not found						
Actual	Last	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_A	AUDIT_DDL_POLICY:0	CREATE PROFILE:SYST	TEM PRIVILEGE:YES:Y	ES:BY USER:ALL USE	RS		
Extended E	vidend	e:						
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_D OLICY	DL_P-	CREATE PROFILE	SYSTEM PRIVILEGE	YES	YES	BY USER	ALL USERS	
SCB_AUDIT_D 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 POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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 m	natches regular expi	ression list				
*	:ALTER PROFILE:.*:YES:	YES:.*:.*				
0	R, any of the select	ed values below:				
	Setting not found					
	Table not found					
Actual L	ast Updated:08/04/2	024 at 06:01:09 PM (GMT+0530)			
SO	CB_AUDIT_DDL_POLICY	Y:ALTER PROFILE:STANI	DARD ACTION:YI	ES:YES:BY USER:ALL \	USERS	
Extended Evic	dence:					
OLICY_NAME	AUDIT_OPTION	AUDIT OPTION TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
	P_ ALTER PROFILE	STANDARD ACTION	YES	YES	BY USER	ALL USERS
.29) 14349 S	status of auditing for	' 'ALTER PROFILE' p	rivilege (Unifi	ed Auditing)(orac	le19:1:1621: Passe	ed MEDIU
P	OHK1RCT.hk.stand	ardchartered.com)				
stance		OHK1RCT.hk.standardch	nartered.com			
evious Status aluation Date	Passed	:09:56 PM (GMT+0530)				
successful, ı	may provide clues a	and forensic eviden ropriate to the need	ces about pot	tential suspicious	ter profiles, whether solution/ unauthorized activitie	s. This loggin
•	• •	dicates the status of the	ALTER PROFILE			
he following Lis	st String value(s) of X in	dicates the status of the		audit option type de	fined on the database. The	output contains
			e, success, failur	audit option type de e, enabled_option, an	fined on the database. The ad entity_name.	output contains o
xpected m	natches regular exp	ression list	e, success, failur	audit option type de e, enabled_option, an	fined on the database. The d entity_name.	output contains (
xpected m	natches regular expi :ALTER PROFILE:.*:YES:	ression list YES:.*:.*	e, success, failur	audit option type de e, enabled_option, an	fined on the database. The d entity_name.	output contains
expected m	natches regular expi :ALTER PROFILE: *:YES: PR, any of the select	ression list YES:.*:.*	e, success, failur	audit option type de e, enabled_option, an	fined on the database. The ad entity_name.	output contains
expected m	natches regular expi :ALTER PROFILE:.*:YES:	ression list YES:.*:.*	e, success, failur	audit option type de e, enabled_option, an	fined on the database. The ad entity_name.	output contains
expected m * O	natches regular expi :ALTER PROFILE:.*:YES: PR, any of the select Setting not found Table not found ast Updated:08/04/2	ression list YES:.*:.* ed values below: 024 at 06:01:09 PM (GMT+0530)			output contains
expected m * O	natches regular expi :ALTER PROFILE:.*:YES: PR, any of the select Setting not found Table not found ast Updated:08/04/2	ression list YES:.** ed values below:	GMT+0530)			output contains
expected m * O Actual L	hatches regular expirations: ALTER PROFILE:.*:YES: OR, any of the select Setting not found Table not found ast Updated:08/04/2 CB_AUDIT_DDL_POLICY	ression list YES:.*:.* ed values below: 024 at 06:01:09 PM (GMT+0530)			output contains
expected m * Contactual L Solution Sixtended Evices	natches regular expi :ALTER PROFILE:.*:YES: OR, any of the select Setting not found Table not found ast Updated:08/04/2 CB_AUDIT_DDL_POLICY dence:	ression list YES:.*:.* ed values below: 024 at 06:01:09 PM (GMT+0530) Dard action:Yi			
Expected m * * * * * * * * * * * * *	natches regular expi :ALTER PROFILE:.*:YES: OR, any of the select Setting not found Table not found ast Updated:08/04/2 CB_AUDIT_DDL_POLICY dence:	ression list YES:.*:.* ed values below: 024 at 06:01:09 PM (Y:ALTER PROFILE:STANI	GMT+0530) DARD ACTION:YI SUCCESS	ES:YES:BY USER:ALL I	USERS	
Expected m * Column * * * * * * * * * * * * *	natches regular explorations: ALTER PROFILE: *: YES: PR, any of the select Setting not found Table not found ast Updated: 08/04/2 CB_AUDIT_DDL_POLICY dence: AUDIT_OPTION L_P- ALTER PROFILE	ression list YES:.*:.* ed values below: 024 at 06:01:09 PM (Y:ALTER PROFILE:STANI AUDIT_OPTION_TYPE STANDARD ACTION	GMT+0530) DARD ACTION:YI SUCCESS YES	ES:YES:BY USER:ALL U FAILURE YES	USERS ENABLED_OPTION BY USER	ENTITY_NAME ALL USERS
expected m * Continue L Solution Scientific Scientif	natches regular explorations. ALTER PROFILE: *: YES: PR, any of the select Setting not found Table not found ast Updated: 08/04/2 CB_AUDIT_DDL_POLICY dence: AUDIT_OPTION PP— ALTER PROFILE Status of auditing for OHK1CAT.hk.standa	ression list YES:.*:.* ed values below: 024 at 06:01:09 PM (Y:ALTER PROFILE:STANI AUDIT_OPTION_TYPE STANDARD ACTION T'ALTER PROFILE' pardchartered.com)	GMT+0530) DARD ACTION:YI SUCCESS YES privilege (Unifi	ES:YES:BY USER:ALL U FAILURE YES	USERS ENABLED_OPTION BY USER	ENTITY_NAME ALL USERS
Expected m * * Actual L SC Extended Evic POLICY_NAME CB_AUDIT_DDL DLICY .29) 14349 S	natches regular explorations. ALTER PROFILE: *: YES: PR, any of the select Setting not found Table not found ast Updated: 08/04/2 CB_AUDIT_DDL_POLICY dence: AUDIT_OPTION PP— ALTER PROFILE Status of auditing for OHK1CAT.hk.standa	ression list YES:.*:.* ed values below: 024 at 06:01:09 PM (Y:ALTER PROFILE:STANI AUDIT_OPTION_TYPE STANDARD ACTION	GMT+0530) DARD ACTION:YI SUCCESS YES privilege (Unifi	ES:YES:BY USER:ALL U FAILURE YES	USERS ENABLED_OPTION BY USER	ENTITY_NAMI ALL USERS

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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	ies 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 Las	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)									
SCE	SCB_AUDIT_DDL_POLICY:ALTER PROFILE:STANDARD ACTION:YES:YES:BY USER:ALL USERS									
SCE	SCB_AUDIT_DDL_POLICY:ALTER PROFILE: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_I	P- ALTER PROFILE	SYSTEM PRIVILEGE	YES	YES	BY USER	ALL USERS				
SCB_AUDIT_DDL_I	2- ALTER PROFILE	STANDARD ACTION	YES	YES	BY USER	ALL USERS				

(1.30) 14350 Status of auditing for 'DROP PROFILE' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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	natcnes regular expre	ssion list						
_	*:DROP PROFILE:.*:YES:YE	S:.*:.*						
	OR, any of the selected	d values below:						
	Setting not found							
	Table not found							
Actual I	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)							
	SCB_AUDIT_DDL_POLICY:1	DROP PROFILE:STAND	ARD ACTION:YES:YES	S:BY USER:ALL USERS				
Extended Evi	dence:							
POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_DD OLICY	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 POHK1RCT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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.

separateu van	ies of policy_name, addit_op	nion, addit_option_type, success, failu	re, enabled_option, and	entity_name.					
Expected	matches regular expre	ssion list							
	.*:DROP PROFILE:.*:YES:YE	S:.*:.*							
	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:I	DROP PROFILE:STANDARD ACTION:Y	ES: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_DDL_P- D	ROP PROFILE	STANDARD ACTION	YES	YES	BY USER	ALL USERS
OLICY						

(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

Expected

Evaluation Date 08/04/2024 at 10:09:56 PM (GMT+0530)

matches regular expression list

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.

	.*:DROP PROFILE:.*:YES: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_AUDIT_DDL_POLICY:DROP PROFILE:STANDARD ACTION:YES:YES:BY USER:ALL USERS									
	SCB_A	.UDIT_DDL_POLICY:E	ROP PROFILE:SYSTE	M PRIVILEGE:YES:YES	:BY USER:ALL USERS					
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 PROFILE	SYSTEM PRIVILEGE	YES	YES	BY USER	ALL USERS			
SCB_AUDIT_D	DL_P-	DROP PROFILE	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:POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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 expre	ssion list							
_	*:CREATE DATABASE LINK	:.*:YES:YES:.*:.*							
	OR, any of the selected values below:								
	Setting not found								
	Table not found								
Actual I	Last Updated:08/04/202	2/ at 06:01:00 DM /	(CMT±0530)						
Actual	Lasi Opualeu.00/04/20/	24 at 00.01.03 F W ((GW11+0330)						
9	SCB_AUDIT_DDL_POLICY:(CREATE DATABASE LI	NK:STANDARD ACTIO	N:YES:YES:BY USER:A	LL USERS				
Extended Evidence:									
POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCB_AUDIT_DD	L_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:POHK1RCT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 PM (GMT+0530)

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

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

Expected

matches regular expression list

:CREATE DATABASE LINK:.:YES:YES:.*:.*

OR, any of the selected values below:

Setting not found
Table not found

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

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

Extended Evidence:

POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME

SCB_AUDIT_DDL_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:POHK1CAT.hk.standardchartered.com)

Passed MEDIUM

MEDIUM

Passed

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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

SCB_AUDIT_DDL_POLICY:CREATE DATABASE LINK:SYSTEM PRIVILEGE:YES:YES:BY USER:ALL USERS

Extended Evidence:

AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS **FAILURE** ENABLED_OPTION ENTITY_NAME POLICY_NAME CREATE DATABASE SCB_AUDIT_DDL_P-SYSTEM PRIVILEGE YES BY USER ALL USERS YES LINK SCB_AUDIT_DDL_P- CREATE DATABASE | STANDARD ACTION | YES YES BY USER ALL USERS LINK

(1.32) 14352 Status of auditing for 'ALTER DATABASE LINK' privilege (Unified Auditing) (oracle19:1:1621:POHK1API3)

Passed MEDIUM

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 PM (GMT+0530)

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

The following List String value(s) of X indicates the status of the ALTER DATABASE LINK audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name. **Expected** matches regular expression list *:ALTER DATABASE LINK:.*:YES:YES:.*:.* OR, any of the selected values below: Setting not found Table not found Actual Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) SCB_AUDIT_DDL_POLICY:ALTER DATABASE LINK:STANDARD ACTION:YES:YES:BY USER:ALL USERS **Extended Evidence:** POLICY_NAME AUDIT OPTION AUDIT OPTION TYPE SUCCESS **FAILURE** ENABLED OPTION ENTITY NAME SCB_AUDIT_DDL_P- 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:POHK1RCT.hk.standardchartered.com)

Passed MEDIUM

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 PM (GMT+0530)

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.

matches regular expression list **Expected** *: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:** POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS **FAILURE** ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P-ALTER DATABASE STANDARD ACTION YES YES BY USER ALL USERS

(1.32) 14352 Status of auditing for 'ALTER DATABASE LINK' privilege (Unified Auditing) Past (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 10:09:56 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	TER DATABASE LINK:.	*:YES: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:ALTER DATABASE LINK:STANDARD 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 OLICY	DL_P-	ALTER DATABASE LINK	STANDARD ACTION	YES	YES	BY USER	ALL USERS	
(1.33) 14353	Stati	us of auditing for ' cle19:1:1621:POH	DROP DATABASE (1API3)	LINK' privilege (U	nified Auditing)	Passe	d MEDIUM	
Instance		oracle19:1:1621:POI	HK1API3					
Previous Status		Passed						
Evaluation Date	9	08/04/2024 at 10:0	9:56 PM (GMT+0530)					
available wit database lin	hout f ks, wl	further authentica nether successful	establish database tion once the link i or unsuccessful, r This logging requi	s established. Lo may provide clues	gging and monitors and forensic evice	ring of all attempts dences about pote	s to drop ential	
The following	List St	ring value(s) of X indi	cates the status of the	DROP DATABASE LIN	IK audit option type d	efined on the database	e. The output	

Expected									
	.*:DRC	OP DATABASE LINK:.*	:YES:YES:.*:.*						
	OR, a	any of the selected	d values below:						
	Setting not found								
	Tal	Table not found							
A -41	1	Un dete de00/04/20	04 -+ 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:	DROP DATABASE LINK	STANDARD ACTION:	YES:YES:BY USER:ALL	USERS			
Extended E	vidono	· · ·							
LAICHUCU L	videiid	<i>,</i> G.							
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_D	DL_P-	DROP DATABASE	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.

(1.33) 14353 Status of auditing for 'DROP DATABASE LINK' privilege (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 10:09:56 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_type, success, failure, enabled_option, and entity_name.

Expected

matches regular expression list

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

OR, any of the selected values below:

Setting not found

Table not found

Actual

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

SCB AUDIT DDL POLICY:DROP DATABASE LINK:STANDARD ACTION:YES:YES:BY USER:ALL USERS

Extended Evidence:									
POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCB_AUDIT_DDL_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:POHK1CAT.hk.standardchartered.com)

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

Passed Previous Status

Evaluation Date 08/04/2024 at 10:09:56 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 contains color	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	matc	hes regular expre	ssion list						
	.*:DRC	*:DROP DATABASE LINK:.*:YES:YES::*:.*							
	OR, any of the selected values below:								
	Setting not found								
	Tal	Table not found							
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM (GMT+0530)					
	SCB_A	AUDIT_DDL_POLICY:I	DROP DATABASE LINK	:STANDARD ACTION	YES:YES:BY USER:ALL	USERS			
Extended Ex	vidend	ce:							
POLICY_NAM	Е	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_D OLICY	DL_P-	DROP DATABASE LINK	STANDARD ACTION	YES	YES	BY USER	ALL USERS		

(1.34) 14354 Status of auditing for 'CREATE SYNONYM' privilege (Unified Auditing)(oracle19:1:1621: Passed **MEDIUM** POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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	hes regular expres	ssion list					
	.*:CRE	ATE SYNONYM:.*:YES	S:YES:.*:.*					
	OR, any of the selected values below:							
	Setting not found							
	Table not found							
Actual		•	24 at 06:01:09 PM (•				
	SCB_A	AUDIT_DDL_POLICY:C	CREATE SYNONYM:ST	ANDARD ACTION:YES	S:YES:BY USER:ALL US	SERS		
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 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)

Oracle ATOS - 20240806 page 824

MEDIUM

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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	hes regular expres	ssion list						
	.*:CRE	EATE SYNONYM:.*:YES	S:YES:.*:.*						
	OR, any of the selected values below:								
	Set	Setting not found							
	Ta	Table not found							
				·					
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM ((GMT+0530)					
	SCB_A	AUDIT_DDL_POLICY:0	CREATE SYNONYM:ST	ANDARD ACTION:YES	:YES:BY USER:ALL US	ERS			
Extended E	viden	~ ~ •							
LAteriaea L	viacii	.							
POLICY_NAM	E	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 POHK1CAT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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.

colori separated values of policy_name, addit_option_type, success, familie, enabled_option, and entity_name.									
Expected	matches regular expression list								
	.*:CRE	EATE SYNONYM:.*:YES	S:YES:.*:.*						
	OR, any of the selected values below:								
	Setting not found								
	Table not found								
		11 - 1 - 1 - 1 - 00/0 //00/	04 - 4 00 04 00 DIA	(ONT OFON)					
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM ((GMT+0530)					
	SCB_A	AUDIT_DDL_POLICY:0	CREATE SYNONYM:ST	ANDARD ACTION:YE	S:YES:BY USER:ALL US	SERS			
Extended E	Evidend	ce:							
POLICY_NAM	POLICY_NAME AUDIT_OPTION A		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 Status of auditing for 'ALTER SYNONYM' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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.

Expected	matches regular expression list									
		ER SYNONYM:.*:YES								
	OR,	any of the selecte	d values below:							
	Setting not found									
		ble not found								
Actual	Last	Updated:08/04/20	24 at 06:01:09 PM (GMT+0530)						
		•	ALTER SYNONYM:STA	•	YES:YES:BY USER:ALI	L USERS				
Extended E	viden	e.								
POLICY_NAM		AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
		ALTER SYNONYM	STANDARD ACTION		YES	BY USER	ALL USERS			
OLIC I										
(1.35) 14355	Statu POH	us of auditing for K1CAT.hk.standa	'ALTER SYNONYM' rdchartered.com)	privilege (Uni	fied Auditing)(ora	cle19:1:1621: Passe	ed MEDIUM			
nstance		oracle19:1:1621:PO	HK1CAT.hk.standardch	nartered.com						
Previous Status		Passed	00 50 D1 ((0) 55 - 5 - 1							
Evaluation Date	е	08/04/2024 at 10:0	09:56 PM (GMT+0530))						
An Oracle da	ataba	se svnonvm is us	sed to create an alt	ernative name	e for a database o	object such as table, v	iew. procedure.			
						alter synonyms, whe				
unsuccessfu	ıl, may	provide clues a	nd forensic eviden	ces about pot	ential suspicious/	unauthorized activitie				
equirement	shou	d be set as appr	opriate to the need	ls of the busin	ess.					
The following	List St	ring value(s) of X ind	icates the status of the	ALTER SYNONY	M audit option type d	lefined on the database. Th	e output contains			
colon separate	ed valu	es of policy_name, at	udit_option, audit_option	on_type, success,	failure, enabled_opti	on, and entity_name.	1			
Expected	mato	hes regular expre	ession list							
	.*:ALT	ER SYNONYM:.*:YES	:YES:.*:.*							
		any of the selecte	d values below:							
		tting not found								
	Ta	ble not found								
	Last	Updated:08/04/20	24 at 06:01:09 PM (GMT+0530)						
Actual		LIDIT DDI DOLLON	ALTER SYNONYM:STA	NDARD ACTION:	YES:YES:BY USER:ALI	L USERS				
Actual	SCB_A	AUDIT_DDL_POLICY:								
Actual Extended E										
	viden			SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
Extended E POLICY_NAM SCB_AUDIT_D	viden Œ	ce:	AUDIT_OPTION_TYPE STANDARD ACTION		FAILURE YES	ENABLED_OPTION BY USER	ENTITY_NAME ALL USERS			
Extended E POLICY_NAM	viden Œ	Ce: AUDIT_OPTION	AUDIT_OPTION_TYPE			-				
Extended E POLICY_NAM SCB_AUDIT_D OLICY	viden E DDL_P-	AUDIT_OPTION ALTER SYNONYM us of auditing for	AUDIT_OPTION_TYPE STANDARD ACTION 'ALTER SYNONYM'	YES	YES	BY USER	ALL USERS			
Extended E POLICY_NAM SCB_AUDIT_D OLICY (1.35) 14355	viden E DDL_P-	AUDIT_OPTION ALTER SYNONYM us of auditing for K1RCT.hk.standa	AUDIT_OPTION_TYPE STANDARD ACTION 'ALTER SYNONYM' rdchartered.com)	YES privilege (Uni	YES	BY USER	ALL USERS			
Extended E POLICY_NAM SCB_AUDIT_E OLICY (1.35) 14355	viden E DDL_P- S Statu POH	AUDIT_OPTION ALTER SYNONYM IS of auditing for K1RCT.hk.standa oracle19:1:1621:PO	AUDIT_OPTION_TYPE STANDARD ACTION 'ALTER SYNONYM'	YES privilege (Uni	YES	BY USER	ALL USERS			
Extended E POLICY_NAM SCB_AUDIT_E OLICY (1.35) 14355 Instance Previous Status	videno E DDL_P- S Statu POH	AUDIT_OPTION ALTER SYNONYM AS of auditing for K1RCT.hk.standa oracle19:1:1621:PO Passed	AUDIT_OPTION_TYPE STANDARD ACTION "ALTER SYNONYM" rdchartered.com)	YES privilege (Uninartered.com	YES	BY USER	ALL USERS			
Extended E POLICY_NAM SCB_AUDIT_E OLICY (1.35) 14355 Instance Previous Status	videno E DDL_P- S Statu POH	AUDIT_OPTION ALTER SYNONYM AS of auditing for K1RCT.hk.standa oracle19:1:1621:PO Passed	AUDIT_OPTION_TYPE STANDARD ACTION 'ALTER SYNONYM' rdchartered.com)	YES privilege (Uni	YES	BY USER	ALL USERS			
Extended E POLICY_NAM SCB_AUDIT_E OLICY (1.35) 14355 Instance Previous Status Evaluation Date An Oracle date	State POH	AUDIT_OPTION ALTER SYNONYM US of auditing for K1RCT.hk.standa oracle19:1:1621:PO Passed 08/04/2024 at 10:0 See Synonym is us	AUDIT_OPTION_TYPE STANDARD ACTION 'ALTER SYNONYM' rdchartered.com) HK1RCT.hk.standardch D9:56 PM (GMT+0530) sed to create an alt	yES privilege (Uninartered.com	YES fied Auditing)(oracle) e for a database of	BY USER cle19:1:1621: Passe	all users ed MEDIUM view, procedure,			
Extended E POLICY_NAM SCB_AUDIT_D OLICY (1.35) 14355 Instance Previous Status Evaluation Date An Oracle da java object of	Statu POH	AUDIT_OPTION ALTER SYNONYM US of auditing for K1RCT.hk.standa oracle19:1:1621:PO Passed 08/04/2024 at 10:0 See synonym is us n another synony	AUDIT_OPTION_TYPE STANDARD ACTION 'ALTER SYNONYM' rdchartered.com) HK1RCT.hk.standardch D9:56 PM (GMT+0530) sed to create an alt rm, etc. Logging ar	privilege (Uninartered.com	YES fied Auditing)(oracle for a database of all attempts to	BY USER cle19:1:1621: Passe object such as table, valter synonyms, where	ALL USERS ed MEDIUM view, procedure, ther successful or			
Extended E POLICY_NAM SCB_AUDIT_D OLICY (1.35) 14355 Instance Previous Status Evaluation Date An Oracle datava object counsuccessfu	Statu POH atabas atabas or eve	AUDIT_OPTION ALTER SYNONYM US of auditing for K1RCT.hk.standa oracle19:1:1621:PO Passed 08/04/2024 at 10:0 See synonym is usen another synony y provide clues a	AUDIT_OPTION_TYPE STANDARD ACTION 'ALTER SYNONYM' rdchartered.com) HK1RCT.hk.standardch D9:56 PM (GMT+0530) sed to create an alt rm, etc. Logging ar	privilege (Uninartered.com ternative name and monitoring ces about pot	YES fied Auditing)(oracle for a database of all attempts to ential suspicious/	BY USER cle19:1:1621: Passe	ALL USERS ed MEDIUM view, procedure, ther successful or			
Extended E POLICY_NAM SCB_AUDIT_D OLICY (1.35) 14355 Instance Previous Status Evaluation Date An Oracle da java object of unsuccessfurequirement The following	Statu POH atabas or eve ul, may	AUDIT_OPTION ALTER SYNONYM US of auditing for K1RCT.hk.standa oracle19:1:1621:PO Passed 08/04/2024 at 10:0 See synonym is us an another synony y provide clues a d be set as approximately and the set as approximately provides of X indicates a synonym in the synonym is used to be set as approximately and the set as approximately and the synonym is used to be set as approximately and the synonym is used to be set as approximately and the synonym is used to be set as approximately and the synonym is used to be set as approximately and the synonym is used to be set as approximately and the synonym is used to be set as approximately and the synonym is used to be set as approximately and the synonym is used to be set as approximately and the synonym is used to be set as approximately and the synonym is used to be set as approximately and the synonym is used to be set as approximately and the synonym is used to be set as approximately and the synonym is used to be set as approximately and the synonym is used to be set as approximately and the synonym is used to be set as approximately and the synonym is used to be set as approximately and the synonym is used to be set as approximately and the synonym is used to be set as approximately approximately and the synonym is used to be set as approximately and the synonym is used to be set as a proximately and the synonym is used to be set as a proximately and the synonym is used to be set as a proximately and the synonym is used to be set as a proximately and the synonym is used to be set as a proximately and the synonym is used to be set as a proximately and the synonym is used to be set as a proximately and the synonym is used to be set as a proximately and the synonym is used to be set as a proximately and the synonym is used to be set as a proximately and the synonym is used to be set as a proximately and the synonym is used to be set as a proximately and the synonym is used to be something the synonym is used to be something the synonym is used to be something the syno	AUDIT_OPTION_TYPE STANDARD ACTION "ALTER SYNONYM" rdchartered.com) "HK1RCT.hk.standardch D9:56 PM (GMT+0530) sed to create an alt rm, etc. Logging ar nd forensic eviden- opriate to the need	privilege (Uninartered.com ernative name of monitoring ces about pot is of the busin	YES fied Auditing)(oracle for a database of all attempts to ential suspicious/ess.	BY USER cle19:1:1621: Passe object such as table, was alter synonyms, where an authorized activities lefined on the database. The	ALL USERS ed MEDIUM view, procedure, ther successful or s. This logging			
Extended E POLICY_NAM SCB_AUDIT_E OLICY (1.35) 14355 Instance Previous Status Evaluation Date An Oracle da java object of unsuccessfurequirement The following colon separate	Statu POH atabaa or eve ul, may shou	AUDIT_OPTION ALTER SYNONYM Is of auditing for K1RCT.hk.standa oracle19:1:1621:PO Passed 08/04/2024 at 10:0 se synonym is us n another synony / provide clues a d be set as appro-	AUDIT_OPTION_TYPE STANDARD ACTION "ALTER SYNONYM" rdchartered.com) OP:56 PM (GMT+0530) sed to create an alt rm, etc. Logging ar nd forensic evidence opriate to the need icates the status of the idit_option, audit_option	privilege (Uninartered.com ernative name of monitoring ces about pot is of the busin	YES fied Auditing)(oracle for a database of all attempts to ential suspicious/ess.	BY USER cle19:1:1621: Passe object such as table, was alter synonyms, where an authorized activities lefined on the database. The	ALL USERS ed MEDIUM view, procedure, ther successful or s. This logging			
Extended E POLICY_NAM SCB_AUDIT_D OLICY (1.35) 14355 instance Previous Status Evaluation Date An Oracle day ava object counsuccessfurequirement	State POH atabas or eve ul, may shoul	AUDIT_OPTION ALTER SYNONYM Is of auditing for K1RCT.hk.standa oracle19:1:1621:PO Passed 08/04/2024 at 10:0 se synonym is us n another synony y provide clues a d be set as appro-	AUDIT_OPTION_TYPE STANDARD ACTION "ALTER SYNONYM" rdchartered.com) OP:56 PM (GMT+0530) sed to create an alt rm, etc. Logging ar nd forensic eviden- opriate to the need icates the status of the adit_option, audit_option	privilege (Uninartered.com ernative name of monitoring ces about pot is of the busin	YES fied Auditing)(oracle for a database of all attempts to ential suspicious/ess.	BY USER cle19:1:1621: Passe object such as table, was alter synonyms, where an authorized activities lefined on the database. The	ALL USERS ed MEDIUM view, procedure, ther successful or s. This logging			
Extended E POLICY_NAM SCB_AUDIT_E OLICY (1.35) 14355 Instance Previous Status Evaluation Date ava object of unsuccessfurequirement The following colon separate	Statue POH Statue	AUDIT_OPTION ALTER SYNONYM IS of auditing for K1RCT.hk.standa oracle19:1:1621:PO Passed 08/04/2024 at 10:0 See synonym is usen another synony provide clues a d be set as appro- ring value(s) of X indes of policy_name, auches regular expressions is the segular expressions and the segular expressions are supported to the segular expressions and the segular expressions are supported to the segular expressions and the segular expressions are supported to the segular expressions and the segular expressions are supported to the segular expressions and the segular expressions are supported to the segular expre	AUDIT_OPTION_TYPE STANDARD ACTION 'ALTER SYNONYM' rdchartered.com) HK1RCT.hk.standardch D9:56 PM (GMT+0530) sed to create an alt rm, etc. Logging ar nd forensic evidence opriate to the need icates the status of the adit_option, audit_option ession list :YES:.*:*	privilege (Uninartered.com ernative name of monitoring ces about pot is of the busin	YES fied Auditing)(oracle for a database of all attempts to ential suspicious/ess.	BY USER cle19:1:1621: Passe object such as table, was alter synonyms, where an authorized activities lefined on the database. The	ALL USERS ed MEDIUM view, procedure, ther successful or s. This logging			
Extended E POLICY_NAM SCB_AUDIT_E OLICY (1.35) 14355 Instance Previous Status Evaluation Date ava object of unsuccessfurequirement The following colon separate	atabaa atabaa or eve all, may shou List St ed valu mato *:ALT	AUDIT_OPTION ALTER SYNONYM Is of auditing for K1RCT.hk.standa oracle19:1:1621:PO Passed 08/04/2024 at 10:0 se synonym is us n another synony y provide clues a d be set as appro-	AUDIT_OPTION_TYPE STANDARD ACTION 'ALTER SYNONYM' rdchartered.com) HK1RCT.hk.standardch D9:56 PM (GMT+0530) sed to create an alt rm, etc. Logging ar nd forensic evidence opriate to the need icates the status of the adit_option, audit_option ession list :YES:.*:*	privilege (Uninartered.com ernative name of monitoring ces about pot is of the busin	YES fied Auditing)(oracle for a database of all attempts to ential suspicious/ess.	BY USER cle19:1:1621: Passe object such as table, was alter synonyms, where an authorized activities lefined on the database. The	ALL USERS ed MEDIUM view, procedure, ther successful or s. This logging			

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_DDLOLICY	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** POHK1API3)

oracle19:1:1621:POHK1API3 Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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

colori separated values of policy_name, addit_option_type, success, failure, enabled_option, and entity_name.								
Expected	matc	hes regular expres	ssion list					
	.*:DRC	OP SYNONYM:.*:YES:Y	ES:.*:.*					
	OR, any of the selected values below:							
	Set	ting not found						
	Tal	Table not found						
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM (GMT+0530)				
	SCB_A	AUDIT_DDL_POLICY:D	ROP SYNONYM:STAN	NDARD ACTION:YES:Y	ES:BY USER:ALL USEF	RS		
Extended Ev	/iden	ce:						
POLICY_NAMI	3	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_D	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 10:09:56 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 separate	d value	es of policy_name, au	dit_option, audit_option	on_type, success, failu	re, enabled_option, ar	nd entity_name.	 	
Expected	matc	hes regular expre	ssion list					
	.*:DRC	OP SYNONYM:.*:YES:Y	ES:.*:.*					
	OR, any of the selected values below:							
	Setting not found							
	Tal	ole not found						
Actual	Lact		24 at 06:01:09 PM (GMT+0530\				
Actual		-	PROP SYNONYM:STAN	•	EC.DV HCED.ALL HCED)C		
			TRUE STINONTINI.STAN	IDARD ACTION.TES.T.	ES.DI USEK.ALL USEK	.O		
Extended Ex	ridenc	e:						
POLICY_NAMI	3	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME	
SCB_AUDIT_DI	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)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 PM (GMT+0530)

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

The following List String value(s) of X indicates the status of the DROP SYNONYM audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name. **Expected** matches regular expression list *:DROP SYNONYM:.*:YES:YES:.*:.* OR, any of the selected values below: Setting not found Table not found Actual Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) SCB_AUDIT_DDL_POLICY:DROP SYNONYM:STANDARD ACTION:YES:YES:BY USER:ALL USERS **Extended Evidence:** POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS **FAILURE** ENABLED_OPTION ENTITY_NAME SCB AUDIT DDL P- DROP SYNONYM STANDARD ACTION YES BY USER ALL USERS YES

(1.37) 14359 Status of auditing for 'ALTER SYSTEM' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

OLICY

Evaluation Date 08/04/2024 at 10:09:56 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, audit_option, audit_option_type, success, failure, enabled_option, and entity_name.							
Expected	matc	hes regular expre	ssion list				
	.*:ALT	ER SYSTEM:.*:YES:YE	S:.*:.*				
	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)			
710100.			•	•	S: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-	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 POHK1CAT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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:STANDARD ACTION:YES:YES:BY USER:ALL USERS

SCB_AUDIT_DDL_POLICY:ALTER SYSTEM:SYSTEM PRIVILEGE:YES:YES:BY USER:ALL USERS

Extended Evidence:										
POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME				
SCB_AUDIT_DDL_P- OLICY	ALTER SYSTEM	SYSTEM PRIVILEGE	YES	YES	BY USER	ALL USERS				
SCB_AUDIT_DDL_P- OLICY	ALTER 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 POHK1RCT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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

(1.38) 14360 Status of auditing for 'CREATE TRIGGER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1API3)

YES

BY USER

ALL USERS

SYSTEM PRIVILEGE YES

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

SCB_AUDIT_DDL_P- ALTER SYSTEM

Evaluation Date 08/04/2024 at 10:09:56 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

YES

ALL USERS

BY USER

(1.38) 14360 Status of auditing for 'CREATE TRIGGER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1CAT.hk.standardchartered.com)

STANDARD ACTION YES

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

Previous Status Passed

SCB_AUDIT_DDL_P- CREATE TRIGGER

Evaluation Date 08/04/2024 at 10:09:56 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, audit_option_type, success, failure, enabled_option, and entity_name.								
Expected	matc	hes regular expre	ssion list					
	.*:CRE	ATE TRIGGER:.*:YES:	YES:.*:.*					
	OR, a	any of the selected	d values below:					
	Setting not found							
	Table not found							
				(0117 0500)				
Actual	Last	Updated:08/04/20	24 at 06:01:09 PM (GM1+0530)				
	SCB_A	AUDIT_DDL_POLICY:(CREATE TRIGGER:STA	NDARD ACTION:YES:Y	ES: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 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 POHK1RCT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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

	.*:CRE	ATE TRIGGER:.*:YES:	YES:.*:.*				
	OR, a	ny of the selecte	d values below:				
	Set	ting not found					
	Tal	ole not found					
Actual	Last	Updated:08/04/20	24 at 06:01:09 PM	(GMT+0530)			
	SCB_A	.UDIT_DDL_POLICY:	CREATE TRIGGER:STA	NDARD ACTION	I:YES:YES:BY USER:ALI	L USERS	
Extended Ex	vidend	e:					
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
(1.39) 14361			'ALTER TRIGGER'	privilege (Uni	ified Auditing)(orac	le19:1:1621: Passe	ed MEDIUM
	POH	K1API3)					

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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									
	.*:ALT	ER TRIGGER:.*:YES:YE	S:.*:.*							
	OR, any of the selected values below:									
	Setting not found									
	Table not found									
A = (=1	Locat Handerto di 00/04/2024 et 00:04:00 DM (CMT: 0520)									
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 Ev	/idenc	e:								
POLICY_NAME	3	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCB_AUDIT_DIOLICY	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 POHK1CAT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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.

separatea van	see of policy_name, addit_option, addit_option_type, ouecoos, failure, onabled_option, and ontroy_name.
Expected	matches regular expression list
	.*:ALTER TRIGGER:.*:YES:YES:.*:*
	OR, any of the selected values below:
	Setting not found
	Table not found

(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 10:09:56 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.

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_TYPE SUCCESS AUDIT_OPTION **FAILURE** ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P- ALTER TRIGGER STANDARD ACTION YES YES BY USER ALL USERS

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

(1.40) 14362 Status of auditing for 'DROP TRIGGER' privilege (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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	ues of p	olicy_name, audit_op	tion, audit_option_typ	oe, success, failure, ena	abled_option, and enti	ity_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	Updated:08/04/202	24 at 06:01:09 PM (GMT+0530)				
	SCB_A	AUDIT_DDL_POLICY:I	DROP TRIGGER:STAND	ARD ACTION:YES:YES	S:BY USER:ALL USERS			
Extended E	vidend	ce:						
POLICY_NAM	Ε	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 POHK1CAT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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:							
	Set	tting not found						
	Ta	ble not found						
Actual	Loot	Undeted-09/04/201	24 of 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:I	DROP TRIGGER:STANI	DARD ACTION:YES:YES	S:BY USER:ALL USERS			
Forten de d'E								
Extended E	viaeno	ce:						
POLICY_NAM	AME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME							
SCB_AUDIT_I 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 POHK1RCT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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.

	F	<u>/</u>		-,	,,	/			
Expected	matches regular expression list								
	.*:DROP TRIGGER:.*:YES:YES:.*:.*								
	OR, a	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	AUDIT_DDL_POLICY:I	DROP TRIGGER:STAND	ARD ACTION:YES:YES	S:BY USER:ALL USERS				
Extended E	ممماني								
Extended	videnc	je:							
POLICY_NAM	ME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME								
SCB_AUDIT_D	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:POHK1API3)

(Gradie 13.1.1021.1 Grittan 13)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 PM (GMT+0530)

Oracle_ATOS - 20240806 page 833

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 create procedure, whether successful or unsuccessful, may provide clues and forensic evidences about potential suspicious/unauthorized activities. This logging requirement should be set as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the CREATE PROCEDURE audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name. **Expected** matches regular expression list *:CREATE PROCEDURE:.*:YES:YES:.*:.* OR, any of the selected values below: Setting not found Table not found Actual Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) SCB_AUDIT_DDL_POLICY:CREATE PROCEDURE:STANDARD ACTION:YES:YES:BY USER:ALL USERS **Extended Evidence:** POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS **FAILURE** ENABLED OPTION ENTITY_NAME SCB_AUDIT_DDL_P- CREATE 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

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 PM (GMT+0530)

PROCEDURE

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.

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:** AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME POLICY NAME SCB_AUDIT_DDL_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:POHK1RCT.hk.standardchartered.com)

Passed MEDIUM

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 PM (GMT+0530)

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.

	-	olicy_name, audit_option,				_ 1 ,	_		
-		thes regular expression EATE PROCEDURE:.*:YES:Y							
		any of the selected va							
		tting not found	iues below:						
		tung not found ble not found							
-		Updated:08/04/2024 a AUDIT_DDL_POLICY:CREA	•	•	ΓΙΟΝ:YES:Y	ES:BY USER:ALL US	SERS		
Extended Evi	dend	;e·							
POLICY_NAME	ucii		JDIT_OPTION_TYPE	SUCCESS	1	FAILURE	ENABLED_OPTION	ENTIT	Y_NAME
_	L_P-	CREATE PROCEDURE ST				YES	_	ALL U	_
(1.42) 143	365	Status of auditing for (oracle19:1:1621:POH	'CREATE FUNCT K1API3)	'ION' state	ment (Uni	fied Auditing)	Passe	ed	MEDIUM
Instance		oracle19:1:1621:PO	•						
Previous Sta	atus	Passed							
Evaluation 1	Date	08/04/2024 at 10:0	09:56 PM (GMT+05	30)					
attempts suspiciou	to cı s/ur	defined by PL/SQL coreate function, whether authorized activities. List String value(s) of X and a values of policy_name, and	er successful or This logging red	unsuccess quirement	sful, may should be	provide clues a e set as approp	and forensic evidence riate to the needs of	es abo the b	out potential usiness.
				ption_type, s	success, ran	ure, enabled_optio	n, and endry_name.		
Expected		matches regular expre .*:CREATE FUNCTION:.*:YE							
		OR, any of the selecte							
		Setting not found Table not found	a values scien.						
Actual		Last Updated:08/04/20	24 at 06:01:09 P	M (GMT+05	530)				
		SCB_AUDIT_DDL_POLICY:	CREATE FUNCTION	:STANDARD	ACTION:YE	S:YES:BY USER:ALI	L USERS		
Extende	d Fv	idence:							
POLICY_N			AUDIT_OPTION_T	VPF SLICCESS	3	FAILURE	ENABLED_OPTION	FNTI	ΓY_NAME
		DL_P- CREATE FUNCTION				YES	BY USER		JSERS
(1.42) 143	365	Status of auditing for (oracle19:1:1621:POH	'CREATE FUNCT K1CAT.hk.standa	TION' state: ardchartere	ment (Uni ed.com)	fied Auditing)	Passe	ed	MEDIUM
Instance		oracle19:1:1621:PO	HK1CAT.hk.standaı	dchartered.c	om				
Previous Sta		Passed							
Evaluation 1	Date	08/04/2024 at 10:0	09:56 PM (GMT+05	30)					
database attempts	as o	ase function, which are defined by PL/SQL coreate function, whether authorized activities.	de and SQL sta er successful or	itements c	ontained sful, may	within these ob provide clues a	ojects. Logging and mand forensic evidence	nonito es abo	ring of all out potential
The follow colon sepa	ing I arateo	ist String value(s) of X ind I values of policy_name, au	icates the status of udit_option, audit_o	the CREATE ption_type, s	FUNCTION success, fail	audit option type oure, enabled_option	defined on the database. T n, and entity_name.	he out	put contains
Expected	d	matches regular expre	ession list						
		.*:CREATE FUNCTION:.*:YE	ES:YES:.*:.*						
		OR, any of the selecte	d values below:						
		Setting not found							
		Table not found							

(1.42) 14365 Status of auditing for 'CREATE FUNCTION' 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 10:09:56 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.

•		1 J =	- · · - ·	= J 1		J —				
Expected	matches regular expression list									
	.*:CRE	.*:CREATE FUNCTION: *:YES:YES: *:.*								
	OR, a	OR, any of the selected values below:								
	Set	ting not found								
	Ta	ble not found								
Actual	Lact	Updated:08/04/202	24 at 06:01:00 DM	CMT - 0530\						
Actual	Lasi	Opuateu.00/04/202	24 at 00.01.09 FWI	GIVI 1 +0330)						
	SCB_A	AUDIT_DDL_POLICY:0	REATE FUNCTION:ST	ANDARD ACTION:YES	:YES:BY USER:ALL US	ERS				
Extended E	viden	· • ·								
Exteriaca E	Viacin	.								
POLICY_NAM	AME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME									
SCB_AUDIT_D OLICY	DL_P-	CREATE FUNCTION	STANDARD ACTION	YES	YES	BY USER	ALL USERS			

(1.43) 14366 Status of auditing for 'CREATE PACKAGE' statement (Unified Auditing) Passed (oracle19:1:1621:POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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 separate	ed value	es of policy_name, au	dit_option, audit_opti	on_type, success, failu	re, enabled_option, ar	nd entity_name.		
Expected	matches regular expression list							
	.*:CREATE PACKAGE:.*: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	CREATE PACKAGE:STA	NDARD ACTION:YES:Y	YES:BY USER:ALL USE	RS		
Extended E	Extended Evidence:							
POLICY_NAM	POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME							
SCB_AUDIT_D	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 POHK1CAT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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_TYPE SUCCESS **FAILURE** ENABLED_OPTION ENTITY_NAME AUDIT_OPTION ALL USERS SCB AUDIT DDL P- CREATE PACKAGE STANDARD ACTION YES YES BY USER OLICY

(1.43) 14366 Status of auditing for 'CREATE PACKAGE' statement (Unified Auditing) (oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

MEDIUM Passed

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

Previous Status

Evaluation Date 08/04/2024 at 10:09:56 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 Undated:08/04/2024 at 06:01:09 PM (GMT+0530)

Aotaai	240t Optication 0472024 at 00.01.00 1 in (Oin 1 10000)								
	SCB_AUDIT_DDL_POLICY:CREATE PACKAGE: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-	CREATE PACKAGE	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:POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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 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:POHK1CAT.hk.standardchartered.com)

Passed MEDIUM

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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 U

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- OLICY	CREATE PACKAGE BODY	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

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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 expre	ession list				
·	.*:CREATE PACKAGE BODY					
	OR, any of the selecte	d values below:				
	Setting not found					
	Table not found					
Actual	Last Updated:08/04/20	024 at 06:01:09 PM	(GMT+0530)			
	SCB_AUDIT_DDL_POLICY:	CREATE PACKAGE BO	DY:STANDARD A	CTION:YES:YES:BY USE	R:ALL USERS	
Extended Ev	ridence:					
POLICY_NAME	E AUDIT_OPTION	AUDIT_OPTION_TYPI	E SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DI OLICY	DL_P- CREATE PACKAGE BODY	STANDARD ACTION	YES	YES	BY USER	ALL USERS
	Status of auditing for (oracle19:1:1621:POH		RE' statement	(Unified Auditing)	Passe	ed MEDIUM
nstance	oracle19:1:1621:P0	•				
revious Status	Passed	-				
valuation Date	08/04/2024 at 10:0	09:56 PM (GMT+0530)			
latabase as of the determinant to a	ase procedures, whicl defined by PL/SQL co Iter procedure, whethe picious/unauthorized a	ode and SQL state er successful or ur	ments contair nsuccessful, r	ned within these ob may provide clues a	ojects. Logging and mand forensic evidence	nonitoring of all es about
The following I colon separated	List String value(s) of X ind d values of policy_name, au	licates the status of the udit_option, audit_opti	e ALTER PROCED on_type, success	OURE audit option type , failure, enabled_option	defined on the database. T n, and entity_name.	Γhe output contains
				·		
Expected	matches regular expre	ession list				
	.*:ALTER PROCEDURE:.*:YI	ES:YES:.*:.*				
	.*:ALTER PROCEDURE::*:YI OR, any of the selecte	ES:YES:.*:.*				
	.*:ALTER PROCEDURE:.*:YI	ES:YES:.*:.*				
	:ALTER PROCEDURE:.:YI OR, any of the selecte Setting not found	ES:YES:.*:.* d values below:	(GMT+0530)			
Actual	*:ALTER PROCEDURE:.*:YI OR, any of the selecte Setting not found Table not found	ES:YES:.*:.* d values below: 024 at 06:01:09 PM	•		L USERS	
Actual	*:ALTER PROCEDURE:.*:YI OR, any of the selecte Setting not found Table not found Last Updated:08/04/20 SCB_AUDIT_DDL_POLICY:	ES:YES:.*:.* d values below: 024 at 06:01:09 PM	•		L USERS	
Actual	*:ALTER PROCEDURE*:YI OR, any of the selecte Setting not found Table not found Last Updated:08/04/20 SCB_AUDIT_DDL_POLICY:	ES:YES:.*:.* d values below: 024 at 06:01:09 PM	TANDARD ACTIC		L USERS ENABLED OPTION	ENTITY_NAME
Actual Extended Ev POLICY_NAME SCB_AUDIT_DI	*:ALTER PROCEDURE*:YI OR, any of the selecte Setting not found Table not found Last Updated:08/04/20 SCB_AUDIT_DDL_POLICY:	es:yes:.*:.* d values below: 024 at 06:01:09 PM ALTER PROCEDURE:S	FANDARD ACTIC	N:YES:YES:BY USER:AL		ENTITY_NAME ALL USERS
Actual Extended Ev POLICY_NAME SCB_AUDIT_DI OLICY (1.45) 14368	*:ALTER PROCEDURE:.*:YI OR, any of the selecte Setting not found Table not found Last Updated:08/04/20 SCB_AUDIT_DDL_POLICY: ridence: E AUDIT_OPTION DL_P- ALTER PROCEDURE Status of auditing for (oracle19:1:1621:POH	es:Yes:.*:* Id values below: 124 at 06:01:09 PM ALTER PROCEDURE:S' AUDIT_OPTION_TYPE STANDARD ACTION CALTER PROCEDU K1CAT.hk.standard	E SUCCESS YES RE' statement statement schartered.com	N:YES:YES:BY USER:AL FAILURE YES	ENABLED_OPTION	ALL USERS
Actual Extended Ev POLICY_NAME SCB_AUDIT_DI OLICY 1.45) 14368 Instance	*:ALTER PROCEDURE*:YI OR, any of the selecte Setting not found Table not found Last Updated:08/04/20 SCB_AUDIT_DDL_POLICY: ridence: AUDIT_OPTION DL_P- ALTER PROCEDURE Status of auditing for (oracle19:1:1621:POH oracle19:1:1621:POH	es:Yes:.*:* Id values below: D24 at 06:01:09 PM ALTER PROCEDURE:S AUDIT_OPTION_TYPE STANDARD ACTION	E SUCCESS YES RE' statement statement schartered.com	N:YES:YES:BY USER:AL FAILURE YES	ENABLED_OPTION BY USER	ALL USERS
Actual Extended Ev POLICY_NAME SCB_AUDIT_DI OLICY (1.45) 14368 Instance Previous Status	*:ALTER PROCEDURE*:YI OR, any of the selecte Setting not found Table not found Last Updated:08/04/20 SCB_AUDIT_DDL_POLICY: ridence: AUDIT_OPTION DL_P- ALTER PROCEDURE Status of auditing for (oracle19:1:1621:POH Passed	ES:YES:.*:.* Id values below: 124 at 06:01:09 PM ALTER PROCEDURE:S AUDIT_OPTION_TYPE STANDARD ACTION CALTER PROCEDU K1CAT.hk.standard	E SUCCESS YES RE' statement dichartered.com	N:YES:YES:BY USER:AL FAILURE YES	ENABLED_OPTION BY USER	ALL USERS
Extended Ev POLICY_NAME SCB_AUDIT_DI OLICY (1.45) 14368 Instance Previous Status Evaluation Date Dracle database as a lattempts to a	*:ALTER PROCEDURE*:YI OR, any of the selecte Setting not found Table not found Last Updated:08/04/20 SCB_AUDIT_DDL_POLICY: ridence: AUDIT_OPTION DL_P- ALTER PROCEDURE Status of auditing for (oracle19:1:1621:POH Passed	ES:YES:.*:* Id values below: 124 at 06:01:09 PM ALTER PROCEDURE:S' AUDIT_OPTION_TYPI E STANDARD ACTION I'ALTER PROCEDU K1CAT.hk.standard OHK1CAT.hk.standard	E SUCCESS YES RE' statement dchartered.com hartered.com the database ments contain successful, resuccessful, res	FAILURE YES (Unified Auditing) e, are created to pened within these obnay provide clues a	ENABLED_OPTION BY USER Passe erform business funct jects. Logging and mand forensic evidence	ALL USERS ed MEDIUM tions and access nonitoring of all es about
Extended Ev POLICY_NAME SCB_AUDIT_DI OLICY (1.45) 14368 Instance Previous Status Evaluation Date Dracle database database as eattempts to a potential suspousiness.	*:ALTER PROCEDURE*:YI OR, any of the selecte Setting not found Table not found Last Updated:08/04/20 SCB_AUDIT_DDL_POLICY: Tidence: AUDIT_OPTION DL_P- ALTER PROCEDURE Status of auditing for (oracle19:1:1621:POH oracle19:1:1621:POH Passed 08/04/2024 at 10:00 ase procedures, which defined by PL/SQL coulter procedure, whether procedure, whether procedures are procedured as a second content of the procedure of	ES:YES:.*:* Id values below: 124 at 06:01:09 PM ALTER PROCEDURE:S' AUDIT_OPTION_TYPI E STANDARD ACTION I'ALTER PROCEDU K1CAT.hk.standard OHK1CAT.hk.standard OHK1CAT.hk.standard	E SUCCESS YES RE' statement Ichartered.com hartered.com the database ments contain insuccessful, riging requirem	FAILURE YES (Unified Auditing) a, are created to pened within these ob may provide clues agent should be set a	enabled_option BY USER Passe erform business funct ejects. Logging and mand forensic evidences appropriate to the	ALL USERS ad MEDIUM tions and access nonitoring of all es about needs of the
Actual Extended Ev POLICY_NAME SCB_AUDIT_DI OLICY (1.45) 14368 Instance Previous Status Evaluation Date Dracle database as a lattempts to a potential suspousiness. The following I colon separated	*:ALTER PROCEDURE*:YI OR, any of the selecte Setting not found Table not found Last Updated:08/04/20 SCB_AUDIT_DDL_POLICY: Tidence: AUDIT_OPTION DL_P- ALTER PROCEDURE Status of auditing for (oracle19:1:1621:POH oracle19:1:1621:POH Passed 08/04/2024 at 10:00 ase procedures, which defined by PL/SQL coller procedure, whether	ES:YES:.*:* Id values below: 124 at 06:01:09 PM ALTER PROCEDURE:S: AUDIT_OPTION_TYPE STANDARD ACTION 1'ALTER PROCEDU K1CAT.hk.standard 109:56 PM (GMT+0530) The are stored withing the and SQL state er successful or unactivities. This logging icates the status of the indit_option, audit_opti	E SUCCESS YES RE' statement Ichartered.com hartered.com the database ments contain insuccessful, riging requirem	FAILURE YES (Unified Auditing) a, are created to pened within these ob may provide clues agent should be set a	enabled_option BY USER Passe erform business funct ejects. Logging and mand forensic evidences appropriate to the	ALL USERS ad MEDIUM tions and access nonitoring of all es about needs of the

Oracle_ATOS - 20240806 page 839

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 YES BY USER ALL USERS

(1.45) 14368 Status of auditing for 'ALTER PROCEDURE' statement (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 10:09:56 PM (GMT+0530)

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

The following List String value(s) of X indicates the status of the ALTER PROCEDURE audit option type defined on the database. The output contains colon separated values of policy_name, audit_option, audit_option_type, success, failure, enabled_option, and entity_name. **Expected** matches regular expression list .*:ALTER PROCEDURE:.*:YES:YES:.*:.* OR, any of the selected values below: Setting not found Table not found Actual Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) SCB_AUDIT_DDL_POLICY:ALTER PROCEDURE:STANDARD ACTION:YES:YES:BY USER:ALL USERS **Extended Evidence:** POLICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS **FAILURE** ENABLED_OPTION ENTITY_NAME SCB_AUDIT_DDL_P- ALTER PROCEDURE STANDARD ACTION YES YES BY USER ALL USERS

(1.46) 14369 Status of auditing for 'ALTER FUNCTION' statement (Unified Auditing)(oracle19:1:1621: Passed **MEDIUM** POHK1API3)

oracle19:1:1621:POHK1API3 Instance

Passed Previous Status

Evaluation Date 08/04/2024 at 10:09:56 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 colon separate	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	any of the selected	l values below:						
	Set	ting not found							
	Tal	ble not found							
Actual		•	24 at 06:01:09 PM (LTER FUNCTION:STA		YES:BY USER:ALL USE	RS			
Extended E	Extended Evidence:								
POLICY_NAM	LICY_NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME								
SCB_AUDIT_D OLICY	DIT_DDL_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 10:09:56 PM (GMT+0530)

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

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

Expected matches regular expression list									
		.*:ALTER FUNCTION:.*:YES:YES:.*:.*							
		OR, any of the selected values below:							
		Set	ting not found						
		Tal	ble not found						
	Actual	1	Llm dete d.00/04/20	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:A	ALTER FUNCTION:STA	NDARD ACTION:YES:Y	YES:BY USER:ALL USE	RS		
	Extended Ex	Evidence:							
	POLICY_NAM	AME 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 POHK1RCT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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	ed value	es of policy_name, au	dit_option, audit_optic	on_type, success, failu	ire, enabled_option, a	and entity_name.			
Expected	matches regular expression list								
	.*:ALTER FUNCTION:.*:YES:YES:.*:.*								
	OR, any of the selected values below:								
	Set	ting not found							
	Tab	ole not found							
Actual	Loot	l Indoted .00/04/201	04 at 06:04:00 DM /	CMT. 0E20\					
Actual	Last	Opdated:06/04/202	24 at 06:01:09 PM (GIWI 1 +0530)					
	SCB_A	AUDIT_DDL_POLICY:A	ALTER FUNCTION:STA	NDARD ACTION:YES:	YES:BY USER:ALL US	ERS			
Extended Evidence:									
POLICY_NAMI	AME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME								
SCR AUDIT D	ODE P ALTER FUNCTION STANDARD ACTION VES VES RV LISER ALL LISERS								

(1.47) 14370 Status of auditing for 'ALTER PACKAGE' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

OLĪĒY

Evaluation Date 08/04/2024 at 10:09:56 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	.*:ALTER PACKAGE:.*:YES:YES:.*:									
	OR, any of the selected values below:										
	Set	ting not found									
	Tal	ble not found									
A			04 - 4 00 04 00 DM	OMT OFOO							
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM ((GIVI I +0530)							
	SCB_A	AUDIT_DDL_POLICY:A	ALTER PACKAGE:STAN	DARD ACTION:YES:Y	ES:BY USER:ALL USER	S					
Extended E	ded Evidence:										
POLICY_NAM	NAME AUDIT_OPTION AUDIT_OPTION_TYPE SUCCESS FAILURE ENABLED_OPTION ENTITY_NAME										
SCB_AUDIT_DDL_P- ALTH		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 POHK1CAT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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.

coloii scparati	u varu	es of policy_name, au	art_option, addit_optic	on_type, success, rand	are, chabica_option, a	nd charty_name.		
Expected	matches regular expression list							
	.*:ALT	ALTER PACKAGE:.*:YES:YES:.*:*						
	OR, a	any of the selected	l values below:					
	Setting not found							
	Tal	ole not found						
				(OLIT 0500)				
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_NAM	E	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 POHK1RCT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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_type, success, failure, enabled_option, and entity_name.

colori separated values of policy_name, addit_option, addit_option_type, success, failure, enabled_option, and enaty_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:08/04/202	24 at 06:01:09 PM ((GMT+0530)						
	SCB_A	.UDIT_DDL_POLICY:A	ALTER PACKAGE:STAN	IDARD ACTION:YES:Y	ES:BY USER:ALL USER	S				
Extended E	videnc	e:								
POLICY_NAM	E	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME			
SCB_AUDIT_D OLICY	DIT_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:POHK1API3)

Passed MEDIUM

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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	matc	nes regular expres	ssion list								
	.*:ALT	.*:ALTER PACKAGE BODY:.*:YES:YES:.*:.*									
	OR, a	any of the selected	d values below:								
	Setting 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:A	ALTER PACKAGE BODY	Y:STANDARD ACTION:	YES:YES:BY USER:ALI	LUSERS					
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				

(1.48) 14371 Status of auditing for 'ALTER PACKAGE BODY' 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 10:09:56 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 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 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:POHK1RCT.hk.standardchartered.com)

Passed MEDIUM

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 PM (GMT+0530)

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

(1.49) 14372 Status of auditing for 'DROP PROCEDURE' statement (Unified Auditing) (oracle19:1:1621:POHK1API3)

Passed MEDIUM

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 PM (GMT+0530)

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

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

Expected matches regular expression list

:DROP PROCEDURE:.:YES:YES:.*:.*

OR, any of the selected values below:

Setting not found

Table not found

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

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

Extended Evidence:

POLICY_NAME AU	UDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_P- DROLICY	ROP 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)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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

YES

(1.49) 14372 Status of auditing for 'DROP PROCEDURE' statement (Unified Auditing)

AUDIT_OPTION_TYPE SUCCESS

Passed MEDIUM

ENTITY_NAME

ALL USERS

ENABLED_OPTION

BY USER

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

Previous Status Passed

POLICY_NAME

Evaluation Date 08/04/2024 at 10:09:56 PM (GMT+0530)

AUDIT_OPTION

SCB_AUDIT_DDL_P- DROP PROCEDURE | STANDARD ACTION | YES

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

(1.50) 14373 Status of auditing for 'DROP FUNCTION' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 PM (GMT+0530)

Oracle database function, which are stored within the database, are created to perform business functions and access

Oracle_ATOS - 20240806 page 845

MEDIUM

Passed

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	matc	matches regular expression list									
	.*:DRC	*:DROP FUNCTION:.*:YES:YES:.*:.*									
	OR, a	any of the selected	l values below:								
	Set	tting not found									
	Ta	ble not found									
Actual	Last	Llm dete d.00/04/00	04 -+ 0C-04-00 DM /	OMT - 0520)							
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM (GIVI I +0530)							
	SCB_A	AUDIT_DDL_POLICY:E	ROP FUNCTION:STAN	NDARD ACTION:YES:Y	ES:BY USER:ALL USEF	RS					
Extended E	viden	ce:									
POLICY_NAM	Е	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 POHK1CAT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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	eu vaiue	es of policy_name, au	uit_option, audit_opti	on_type, success, failt	ire, enabied_option, a	па епшу_пате.				
Expected	matc	matches regular expression list								
	.*:DRC	.*:DROP FUNCTION:.*:YES:YES:.*:.*								
	OR, any of the selected values below:									
	Set	ting not found								
	Table not found									
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM ((GMT+0530)						
	SCB_A	AUDIT_DDL_POLICY:I	DROP FUNCTION:STAP	NDARD ACTION:YES:Y	ES:BY USER:ALL USE	RS				
Extended Ex	Extended Evidence:									
POLICY_NAM	NAME 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 POHK1RCT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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.

coloil separat	ou values of policy_name, addit_option_t, pe, success, failure, ondered_option, and only_name.
Expected	matches regular expression list
	.*:DROP FUNCTION:.*:YES:YES:.*:.*

	OR, a	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:I	ROP FUNCTION:STAN	NDARD ACTION:YES:Y	ES:BY USER:ALL USE	RS				
Extended Ev	vidend	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			

(1.51) 14374 Status of auditing for 'DROP PACKAGE' statement (Unified Auditing)(oracle19:1:1621: Passed MEDIUM POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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	l values below:							
	Set	ting not found								
	Tal	ole not found								
Actual	14	Um 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:D	ROP PACKAGE:STANI	DARD ACTION:YES:YE	S:BY USER:ALL USERS)				
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 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 10:09:56 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 vait	ies 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 E	vidence:

POLICY_NAME	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME
SCB_AUDIT_DDL_P- OLICY	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 10:09:56 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							
Actual	Last	Updated:08/04/202	24 at 06:01:09 PM (GMT+0530)					
	SCB_A	SCB_AUDIT_DDL_POLICY:DROP PACKAGE:STANDARD ACTION:YES:YES:BY USER:ALL USERS							
Extended E	vidend	ce:							
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		

(1.52) 14375 Status of auditing for 'DROP PACKAGE BODY' statement (Unified Auditing) Passed (oracle19:1:1621:POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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 separate	ed value	es of policy_name, au	dit_option, audit_option	on_type, success, failu	ire, enabled_option, ai	nd entity_name.	
Expected	matches regular expression list						
	.*DROP PACKAGE BODY:.*:YES:YES:.*:.*						
	OR, any of the selected values below:						
	Set	ting not found					
	Tal	ole not found					
Actual	Last	Undated:08/04/202	24 at 06:01:09 PM ((GMT+0530)			
710100.		_ -			YES:YES:BY USER:ALL	USERS	
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 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:POHK1CAT.hk.standardchartered.com)

Passed MEDIUM

MEDIUM

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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						
	.*DROP PACKAGE BODY:.*:YES:YES::*:.*								
	OR, any of the selected values below:								
	Set	ting not found							
	Tal	ole not found							
Actual	l act		04 at 06:01:00 PM ('CMT+0530\					
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								
			MOT THORNOL BODT	.ormivDriid Norioiv.	TEO.TEO.DT COER.TAEL	COLICO			
Extended Ev	/idenc	e:							
POLICY_NAMI	3	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME		
SCB_AUDIT_D		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:POHK1RCT.hk.standardchartered.com)

Passed MEDIUM

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 PM (GMT+0530)

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	OP PACKAGE BODY:.*:	YES:YES:.*:.*				
	OR,	any of the selecte	d values below:				
	Se	tting not found					
	Ta	Table not found					
			0.4	·			
Actual	Last	Updated:08/04/20	24 at 06:01:09 PM (GM1+0530)			
	SCB_A	AUDIT_DDL_POLICY:	DROP PACKAGE BODY	:STANDARD ACTION:	YES:YES:BY USER:ALL	USERS	
Extended E	viden	ce:					
POLICY_NAM	1E	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

(1.53) 14376 Status of auditing for 'LOGON' action (Unified Auditing)(oracle19:1:1621:POHK1API3) Passed MEDIUM

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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	mato	hes regular expres	ssion list								
	.*:LO0	.*:LOGON:.*:.*:YES:.*:*									
	OR,	any of the selected	I values below:								
	Se	tting not found									
	Ta	ble not found									
Actual	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)										
	SCB_I	LOGON_ALL_FAILURE	S:LOGON:STANDARD	ACTION:NO:YES:BY U	SER:ALL USERS						
	SCB_I	LOGON_LOGOFF_PRI\	USER:LOGON:STAND	ARD ACTION:YES:YES	B:BY USER:ALL USERS						
Extended Ev	/iden	ce:									
POLICY_NAMI	3	AUDIT_OPTION	AUDIT_OPTION_TYPE	SUCCESS	FAILURE	ENABLED_OPTION	ENTITY_NAME				
SCB_LOGON_I FF_PRIVUSER	.OGO-	LOGON	STANDARD ACTION	YES	YES	BY USER	ALL USERS				
SCB_LOGON_A FAILURES	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 10:09:56 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
Cytopded C	

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:POHK1RCT.hk. Passed MEDIUM standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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 I

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

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

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

Extended Evidence:

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

(1.54) 14377 Status of auditing for 'LOGOFF' action (Unified Auditing)(oracle19:1:1621:POHK1API3) Passed MEDIUM

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 PM (GMT+0530)

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

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

Expected matches regular expression list

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

OR, any of the selected values below:

Setting not found
Table not found

Actual

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

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

Extended Evidence:

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

(1.54) 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 10:09:56 PM (GMT+0530)

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

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

Expected matches regular expression list

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

OR, any of the selected values below:

		ting not found 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	.OGON_LOGOFF_PRI\	/USER:LOGOFF:STANI	DARD ACTION:YES:YES	S:BY USER:ALL USERS				
Extended Ex	vidend	ce:							
POLICY_NAM	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 FF PRIVUSER	LOGO-	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 10:09:56 PM (GMT+0530)

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

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

Expected	matches regular expression list								
	.*:LOGOFF:.*:YES:YES:.*:*								
OR, any of the selected values below:									
	Set	ting not found							
	Tal	ole not found							
Actual	Last	Indated:08/04/203	24 at 06:01:09 PM ('CMT+0530\					
Actual		•		•	C.DV HCED.ALL HCEDC				
	2CP_L	OGON_LOGOFF_PRI	USER:LUGUFF:STAINL	DARD ACTION: 1ES: 1E	S:BY USER:ALL USERS				
Extended Ev	/idend	e:							
POLICY_NAM	E	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 POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Failed

Evaluation Date 08/04/2024 at 10:09:56 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	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)
	File not found

tend	ded Evider	nce:				
orma	ation					
not	found, pleas	se verify authentication record file paths.				
0)R					
T	he following	$List \ String \ value (s) \ of \ X \ indicates \ the \ status \ of \ the \ SQLNET. authentication_services \ setting \ defined \ within \ the \ sqlnet. or a \ file.$				
E	xpected	contains regular expression list				
tcps		tcps				
		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)		Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)				
		File not found				
E	xtended E	vidence:				
Ir	nformation					
Fi	ile not found	l, please verify authentication record file paths.				

(1.55) 24264 Status of ENCRYPTION_SERVER and AUTHENTICATION_SERVICES(oracle19:1:1621: Passed MEDIUM POHK1CAT.hk.standardchartered.com)

 $In stance \qquad \qquad oracle 19:1:1621: POHK1CAT. hk. standard chartered. com$

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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 se	et for the SQLNET.ENCRYPTION_SERVE	R 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 E	Evidence:					
File name		Setting	Value			
/u01/app/or ora	racle/local/network/admin/sqlnet.	sqlnet.encryption_server	REQUESTED			
OR						
The following	g List String value(s) of X indicates	he status of the SQLNET.authentication	_services setting defined within the sqlnet.c	ora file.		
Expected	contains regular expression list					
	tcps					
	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)					
	Setting not found					
Extended E	Evidence:					
File name		Setting	Value			

(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 10:09:56 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.

Expected	regular expression match					
, poo	REQUESTED					
	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)				
	File not found					
Extended I	Evidence:					
File name		Setting	Value			
/u01/app/gi sqlnet.ora	rid/product/12cR2/network/admin/	sqlnet.encryption_server				
OR						
	g List String value(s) of X indicates th	ne status of the SQLNET.authentication_s	ervices setting defined within the s	sqlnet.ora file.		
The followin	g List String value(s) of X indicates the contains regular expression		ervices setting defined within the s	sqlnet.ora file.		
The followin			ervices setting defined within the s	sqlnet.ora file.		
The followin	contains regular expression	list	ervices setting defined within the s	sqlnet.ora file.		
OR The followin Expected	contains regular expression tcps OR, any of the selected value Setting not found	list	ervices setting defined within the s	sqlnet.ora file.		
Γhe followin	contains regular expression tcps OR, any of the selected value	list	ervices setting defined within the s	sqlnet.ora file.		
The followin	contains regular expression tcps OR, any of the selected value Setting not found	list es below:	ervices setting defined within the s	sqlnet.ora file.		
The followin	contains regular expression tcps OR, any of the selected value Setting not found File not found	list es below:	ervices setting defined within the s	sqlnet.ora file.		
The followin	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	list es below:	ervices setting defined within the s	sqlnet.ora file.		
The followin Expected Actual	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	list es below:	ervices setting defined within the s	sqlnet.ora file.		

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 PM (GMT+0530)

Disallow Factory or Vendor Default accounts in Production

Disallow Factory or Vendor Default accounts in Production

Scan Parameters:

DBQUERY: select username from dba_users

Expected does not contain regular expression list

DB Column Name: USERNAME

^SH\$
^SCOTT\$
^PM\$
^OE\$
^IX\$
^HR\$
^BI\$

OR, any of the selected values below:

Set status to PASS if no data found

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

USERNAME SYS SYSTEM XSSNULL OUTHN SYSSUMF DESNMY APPOOSSYS DESPWUSER GGSYS ANONYMOUS CTXSYS DVF CSMADMIN_INTERNAL MOSYS OLAIRYS XIB WMSYS GAMACIUSER CSSCS GAMACIUSER CSS. CAAN MDATA SYSBACKUP REMOTE_SCHEDULER_AGENT ORARO GAMEDI SYSSRAC GSMKOOTUSER GRAMED GRAMED AUDOYS DIP ORARO GRAMED G	Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530)
SYSTEM SYSSULL OLYMSYS LEACSYS OUTLIN SYSSUMF DESNMP APPOOSSYS DESHWUSER GCSYS ANONYMOUS CTXSYS DVF SMADMIN_INTERNAL MDSYS OLAFSYS XDB WMSYS GSMADMIN_INTERNAL MDSYS OLAFSYS XDB WMSYS GSMCATUSER CSC, SCAN MDDATA SYSBACKUP REMOTE SCHEDULER AGENT ORANO SEB LINK GSMUSER SYSBAC GSMLINK GSMUSER SYSSAC GEMROOTUSER ORANDE DEAD DEAD DEAD SYSSAC GEMROOTUSER ORANDE ORANDE DEAD ORANDE SYSKAC GRAMCOTUSER ORANDE ORANDE SYSKAC GRAMCOTUSER ORANDE ORANDE ORANDE ORANDE SYSKAC GRAMCOTUSER ORANDE O	JSERNAME
SYSTEM SYSSULL OLYMSYS LEACSYS OUTLIN SYSSUMF DESNMP APPOOSSYS DESHWUSER GCSYS ANONYMOUS CTXSYS DVF SMADMIN_INTERNAL MDSYS OLAFSYS XDB WMSYS GSMADMIN_INTERNAL MDSYS OLAFSYS XDB WMSYS GSMCATUSER CSC, SCAN MDDATA SYSBACKUP REMOTE SCHEDULER AGENT ORANO SEB LINK GSMUSER SYSBAC GSMLINK GSMUSER SYSSAC GEMROOTUSER ORANDE DEAD DEAD DEAD SYSSAC GEMROOTUSER ORANDE ORANDE DEAD ORANDE SYSKAC GRAMCOTUSER ORANDE ORANDE SYSKAC GRAMCOTUSER ORANDE ORANDE ORANDE ORANDE SYSKAC GRAMCOTUSER ORANDE O	SYS
XSSMUIL OLIVIN SYSTEMACY OUTEN SYSSUMF DESMIP DESMIP DESMIP DESWIP DESWIP DESWIP OCTOR OCT	
DIVMSYS LEBECSYS	
LBACSYS OUTLN SYSSUMF DBSMMP APPOORSYS DBSFWUSER CCSYS ARONYMOUS CTXSYS DVSYS DVSYS DVSYS DVSYS OVALIBRIAN OF ANOLOGY CSMADMIN_INTERNAL MOSYS OLAPSYS XDB WMSYS CSMADMIN_INTERNAL MOSYS CLEASE CSMACTUSER CCS, SCAN MIDDATA SYSBACKUP REMOTE SCHEDULER AGENT ORARO SCB LINK CSMUSER SYSEAC SCB LINK CSMOSTER CSMOSTER CSMOTUSER ORARODUSER	
OUTLN SYSSUMF DESNMP APPOOSSYS DESPWUSER CCSYS ANONYMOUS CTASYS DVSYS DVF GSMADMIN_INTERNAL MDSYS OLAPSYS ADB WMSYS CSMCATUSER CSSCAN MDDATA SYSBACKUP REMOTE SCHEDULER_AGENT ORARO SCB_LINK CSSMCATUSER CSCB_LINK CSCB_LINK CSCB_LINK CSCB_LINK CSCB_LINK CSCB_LINK CSCB_LINK CSMCATUSER CSCB_LINK CSMCATUSER CDEAN ADD ADD ADD ADD ADD ADD ADD ADD ADD A	
SYSSUMF DBSNMP APPQOSSYS DBSIPWUSER GCSYS ANONYMOUS CTXSYS DVSYS DVF CSMADMIN_INTERNAL MDSYS OLAPSYS XDB WMSYS GSMCATUSER CCS_SCAN MDDATA SYSSACKUP REMOTE_SCHEDULER_AGENT ORARD SCB_LINK GSMSOTUSER CS.BLINK GSMCSTUSER CS.BLINK GSMCSTUSER CS.BLINK GSMCSTUSER CS.BLINK GSMUSER SYSSACKUP REMOTE_SCHEDULER_AGENT ORARD SCB_LINK GSMUSER SYSSACKUP SYSKAC CSMROTUSER ORARD SCB_LINK GSMUSER SYSKAC CSMROTUSER ORARD SCB_LINK GSMUSER SYSKAC CSMROTUSER ORARD SCB_LINK GSMUSER SYSKAC CSMROTUSER ORARD STYSKAC ORARD STY	
DBSNMP APPQOSSYS DBSFWUSER GCSYS ANONYMOUS CTXSYS DVSY DVF CSMADMIN_INTERNAL MDSYS OLAPSYS BASILITATION OLAPSYS SMED WMSYS GSMCATUSER CCS, SCAN MDDATA SYSBACKUP REMOTE, SCHEDULER, AGENT ORANG GSMUSER SCS, LINK GSMUSER GRAMEDI	
APPQOSSYS DBSPWUSER GCSYS ANONYMOUS CTXSYS DVSYS DVF GSMADMIN_INTERNAL MDSYS OLAPSYS XDB WMSYS GSMATUSER CCS, SCAN MDDATA SYSBACKUP REMOTE, SCHEDULER_AGENT ORARO SCBLINK GSMLOYSER CSMLOYSER CSMROOTUSER CSMROOTUSER CORAMED2 SL INFORMIN_SCHEMA DBBARO AUDSYS DIP ORDPLICINS DBBADDM SYSKM ORDPLICINS DBADDM SYSKM ORDPLICINS DBADDM SYSKM ORDDATA AOGEMS ORACEL OCM OREMUSER SYSDG ORDSYS ORAMED1 PUPPETAM	
DBSFWUSER CGSYS ANONYMOUS CTXSYS DVSYS DVSYS DVSYS DWSYS GSMADMIN_INTERNAL MDSYS CLAPSYS XDB WMSYS SCBMCATUSER CCS_SCAN MDDATA SYSBACKUP REMOTE_SCHEDULER_AGENT ORARO SCB_LINK GSMUSER SYSBACKUP STSBAC SCB_LINK GSMUSER SYSRAC SOB_LINK GSMUSER SYSRAC SOB_LINK GSMUSER SYSRAC SOB_LINK GSMUSER SYSRAC SOB_LINK GSMUSER SYSRAC GRAMEDIZ LINFORMIN_SCHEMA DBARO AUDSYS DIP ORRPPLUGINS DBARO AUDSYS DIP ORRPPLUGINS DBARO AUDSYS ORRDOATA AOGEMS ORROLL CCM ORRDATA AOGEMS ORROLL CCM ORROLL	
GGSYS ANONYMOUS CTXSYS DVSYS DVF GSMADMIN_INTERNAL MDSYS OLAPSYS XDB WMSYS GSMCATUSER CCS_SCAN MDDATA SYSBACKUP REMOTE_SCHEDULER_AGENT ORARD SCB_LINK GSMCOTUSER CSMROOTUSER CSMROOTUSER ORARD SCB_LINK GSMIN_SYSSEAC GSMROOTUSER ORARD SCB_LINK GSMUSER SYSISAC GSMROOTUSER ORARD	
ANONYMOUS CTXSYS DVF CSMADMIN_INTERNAL MDSYS OLAPSYS XDB WMSYS SCMCATUSER CCS SCAN MDDATA SYSBACKUP REMOTE SCHEDULER AGENT ORARO SCB_LINK CSMUSER SYSBAC SCB_LINK CSMCATUSER CSMCOTUSER ORAMEDI SLINK CSMINSER SYSRAC SCMCOTUSER ORAMEDI SLINK CSMINSER SYSRAC SCMINSER SYSRAC	
CTXSYS DVSYS DVSYS DVF GSMADMIN_INTERNAL MDSYS OLAPSYS XDB WMSYS GSMCATUSER CCS, SCAN MDDATA SYSBACKUP REMOTE SCHEDULER AGENT ORARO SCB_LINK GSMCOTUSER CSMCMADDER SYSRAC SSMCOTUSER SYSRAC SMROTUSER SYSIRAC SMROTUSER SYSIRAC SMROTUSER SYSIRAC GSMYDER SIL INFORMTN_SCHEMA DBARO AUDSYS DIP ORDPLUCINS DBADDM SYSKM ORDDATA AGGEMS ORBOLL ORACL OR	
DVSYS DVF GSMADMIN_INTERNAL MDSYS OLAPSYS XDB WMSYS GSMCATUSER CCS_SCAN MDDATA SYSBACKUP REMOTE_SCHEDULER_AGENT ORARO SGB_LINK GSMUSER SYSRAC GSMROOTUSER ORAMED2 SI_INFORMTN_SCHEMA DBAD JBAPD UGINS DBADDM SYSKM ORDATA AGCEMS ORACLE_OCM OEMUSER SYSDG ORBOSYS ORBASYS ORAMED1 PUPPETAM	
DVF CSMADMIN_INTERNAL MDSYS OLAPSYS XDB WMSYS CSMCATUSER CCS_SCAN MDDATA SYSBACKUP REMOTE_SCHEDULER_AGENT ORARO SCB_LINK CSMUSSER SYSPRAC GSMROOTUSER ORAMED2 SI_INFORMTN_SCHEMA DBARO AUDSYS DIP ORDPLUGINS DBADDM SYSKM ORDADATA AOGENS ORACLE_OCM ORMUSER SYSDC ORMUSER SYSDC ORDSYS ORAMED1	
GSMADMIN_INTERNAL MDSYS OLAPSYS XDB WMSYS GSMCATUSER CCS_SCAN MDDATA SYSBACKUP REMOTE_SCHEDULER_AGENT ORARO SCB_LINK GSMUSER SYSRAC GSMROOTUSER ORAMED2 SI_INFORNTIN_SCHEMA DBARO AUDSYS DIIP ORDPLUGINS DBADD SYSKM ORDDATA AUDSYS DIIP ORDPLUGINS DBADDM SYSKM ORDDATA AOGEMS ORADELE OCM OEMUSER SYSSM ORADELE OCM OEMUSER SYSSM ORADELE OCM OEMUSER SYSSM ORADELE OCM OEMUSER SYSOG ORADELE OCM ORAMED1 PUPPETAM	
MDSYS 0LAPSYS WMSYS GSMCATUSER CCS_SCAN MDDATA SYSBACKUP REMOTE_SCHEDULER_AGENT ORARO SCB_LINK GSMUSER SYSRAC GSMROOTUSER ORAMED2 SI_NFORMTN_SCHEMA DBARO AUDSYS DIP OROPPLUGINS DBADDM SYSKM ORDDATA AOGEMS ORACLE_OCM ORACLE_OCM ORACLE_OCM ORRDSYS ORRDSYS ORAMED1	
OLAPSYS XDB WMSYS GSMCATUSER CCS_SCAN MDDATA SYSBACKUP REMOTE_SCHEDULER_AGENT ORARO SCB_LINK GSMUSER SYSRAC GSMROOTUSER ORAMED2 SI_INFORNTN_SCHEMA DBABRO AUDSYS DIP ORDPLUGINS DBADDM SYSKM ORDDATA AOGEMS ORACLE_OCM OEMUSER SYSDG ORAMED1 PUPPETAM	
XDB WMSYS CS SCAN MDDATA SYSBACKUP REMOTE_SCHEDULER_AGENT ORARO SCE_LINK GSMUSER SYSRAC GSMROOTUSER ORAMED2 SI_INFORNTN_SCHEMA DBARO AUDSYS DIP ORDPLUGINS DBADDM SYSKM ORDDATA AGCEMS ORACLE_OCM ORACLE_OCM ORACLE_OCM ORMSER SYSDG ORAMED I PUPPETAM	
WMSYS CS. SCAN MDDATA SYSBACKUP REMOTE_SCHEDULER_AGENT ORARO SCB_LINK GSMUSER SYSRAC GSMROOTUSER ORAMED2 SI_INFORMTN_SCHEMA DBARO AUDSYS DIP ORDPLUGINS DBADM SYSKM ORDDATA AGGEMS ORACLE_OCM OEMUSER SYSDG ORAWED1 PUPPETAM	
GSMCATUSER CCS. SCAN MDDATA SYSBACKUP REMOTE SCHEDULER_AGENT ORARO SCB_LINK GSMUSER SYSRAC GSMROOTUSER ORAMED2 SI_INFORMTN_SCHEMA DBARO AUBONYS DIP ORDPLUGINS DBADDM SYSKM ORDDATA AGGEMS ORADATA AGGEMS ORACLE_OCM OEMUSER SYSDG ORDSYS ORDSYS ORDSYS ORDSYS ORDSYS ORDDATA AGGEMS ORACLE_OCM OEMUSER SYSSCB ORAMED1 PUPPETAM	
CCS_SCAN MDDATA SYSBACKUP REMOTE_SCHEDULER_AGENT ORARO SCB_LINK GSMUSER SYSRAC GSMROOTUSER ORAMED2 SI_INFORMTN_SCHEMA DBAARO AUDSYS DIP ORDPLUGINS DBADDM SYSKAM ORDPLUGINS DBADDM SYSKM ORDDATA AOGEMS ORACLE_OCM OEMUSER SYSKD ORDSYS ORACLE_OCM OEMUSER SYSDG ORDSYS ORAMED1 PUPPETAM	
MDDATA SYSBACKUP REMOTE_SCHEDULER_AGENT ORARO SCB_LINK CSMUSER SYSRAC GSMUSER SYSRAC GSMROOTUSER ORAMED2 SI_INFORMTN_SCHEMA DBARO AUDSYS DIP ORDPLUGINS DIP ORDPLUGINS DBADDM SYSKM ORDDATA AOGEMS ORDDATA AOGEMS ORACLE_OCM OEMUSER ORACLE_OCM OEMUSER ORDSYS ORACLE_OCM OEMUSER SYSCM ORDSYS ORAMED1	
SYSBACKUP REMOTE_SCHEDULER_AGENT ORARO SCB_LINK SCB_LINK SSMUSER SYSRAC GSMROOTUSER ORAMED2 SL_INFORMTN_SCHEMA DBARO AUDSYS DIP ORDPLUGINS DBADDM SYSKM ORDDATA AOGEMS ORACLE_OCM OEMUSER ORACLE_OCM OEMUSER ORACLE_OCM ORDSYS ORAMED1 PUPPETAM	
ORARO SCB_LINK GSMUSER SYSRAC GSMROOTUSER ORAMED2 SI_INFORMTN_SCHEMA DBARO AUDSYS DIP ORDPLUGINS DBADDM SYSKM ORDDATA AOGEMS ORACLE_OCM OEMUSER SYSDG ORDSYS ORDSYS ORAMEDI PUPPETAM	
ORARO SCB_LINK GSMUSER SYSRAC GSMROOTUSER ORAMED2 SI_INFORMTN_SCHEMA DBARO AUDSYS DIP ORDPLUGINS DBADDM SYSKM ORDDATA AOGEMS ORACLE_OCM OEMUSER SYSDG ORDSYS ORDSYS ORAMEDI PUPPETAM	
GSMUSER SYSRAC GSMROOTUSER ORAMED2 SI_INFORMTN_SCHEMA DBARO AUDSYS DIP ORDPLUGINS DBADDM SYSKM ORDDATA AOGEMS ORDDATA AOGEMS ORACLE_OCM OEMUSER SYSDG ORDSYS ORDSYS ORDSYS ORDSYS ORDSYS ORDSYS ORDMS ORDSYS ORDMS ORDMS ORDMS ORDMS ORDMS ORDMS ORDMS ORDMS ORACLE_OCM OEMUSER SYSDG ORDMS ORDM	
GSMUSER SYSRAC GSMROOTUSER ORAMED2 SI_INFORMTN_SCHEMA DBARO AUDSYS DIP ORDPLUGINS DBADDM SYSKM ORDDATA AOGEMS ORDDATA AOGEMS ORACLE_OCM OEMUSER SYSDG ORDSYS ORDSYS ORDSYS ORDSYS ORDSYS ORDSYS ORDMS ORDSYS ORDMS ORDMS ORDMS ORDMS ORDMS ORDMS ORDMS ORDMS ORACLE_OCM OEMUSER SYSDG ORDMS ORDM	SCB_LINK
GSMROOTUSER ORAMED2 SI_INFORMTN_SCHEMA DBARO AUDSYS DIP ORDPLUGINS DBADDM SYSKM ORDDATA AOGEMS ORACLE_OCM OEMUSER SYSDG ORDSYS ORDSYS ORDSYS ORDSYS ORDSYS ORDSYS ORACLE_OCM OEMUSER	GSMUSER
GSMROOTUSER ORAMED2 SI_INFORMTN_SCHEMA DBARO AUDSYS DIP ORDPLUGINS DBADDM SYSKM ORDDATA AOGEMS ORACLE_OCM OEMUSER SYSDG ORDSYS ORDSYS ORDSYS ORDSYS ORDSYS ORDSYS ORACLE_OCM OEMUSER	
SI_INFORMTN_SCHEMA DBARO AUDSYS DIP ORDPLUGINS DBADDM SYSKM ORDDATA AOGEMS ORACLE_OCM OEMUSER SYSDG ORDSYS ORDSYS ORDSYS ORAMED1 PUPPETAM	
DBARO AUDSYS DIP ORDPLUGINS DBADDM SYSKM ORDDATA AOGEMS ORACLE_OCM OEMUSER SYSDG ORDSYS ORACLE_OCM ORDSYS ORACLE_OCM OEMUSER SYSDG ORDSYS ORACLE_OCM ORDSYS	DRAMED2
AUDSYS DIP ORDPLUGINS DBADDM SYSKM ORDDATA AOGEMS ORACLE_OCM OEMUSER SYSDG ORDSYS ORACLE_OCH ORDSYS ORAMED1 PUPPETAM	SI_INFORMTN_SCHEMA
DIP ORDPLUGINS DBADDM SYSKM ORDDATA AOGEMS ORACLE_OCM OEMUSER SYSDG ORDSYS ORACLE_OCH OUDDETAM	
ORDPLUGINS DBADDM SYSKM ORDDATA AOGEMS ORACLE_OCM OEMUSER SYSDG ORDSYS ORAMED 1 PUPPETAM	AUDSYS
DBADDM SYSKM ORDDATA AOGEMS ORACLE_OCM OEMUSER SYSDG ORDSYS ORAMED 1 PUPPETAM	DIP
SYSKM ORDDATA AOGEMS ORACLE_OCM OEMUSER SYSDG ORDSYS ORAMED 1 PUPPETAM	ORDPLUGINS
ORDDATA AOGEMS ORACLE_OCM OEMUSER SYSDG ORDSYS ORAMED 1 PUPPETAM	DBADDM
AOGEMS ORACLE_OCM OEMUSER SYSDG ORDSYS ORAMED1 PUPPETAM	SYSKM
ORACLE_OCM OEMUSER SYSDG ORDSYS ORAMED1 PUPPETAM	DRDDATA
OEMUSER SYSDG ORDSYS ORAMED 1 PUPPETAM	
SYSDG ORDSYS ORAMED 1 PUPPETAM	DRACLE_OCM
SYSDG ORDSYS ORAMED 1 PUPPETAM	
ORAMED1 PUPPETAM	
PUPPETAM	DRDSYS
PUPPETAM	
	PUPPETAM
	CC_ITRS

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 POHK1CAT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 PM (GMT+0530)

Disallow Factory or Vendor Default accounts in Production

Disallow Factory or Vendor Default accounts in Production

Scan Parameters:

DBQUERY: select username from dba_users

Expected does not contain regular expression list

DB Column Name: USERNAME

^SH\$
^SCOTT\$
^PM\$
^OE\$
^IX\$
^HR\$

^BI\$

OR, any of the selected values below:

Set status to PASS if no data found

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

USERNAME
SYS
SYSTEM
XS\$NULL
OJVMSYS
LBACSYS
OUTLN
SYS\$UMF
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
PUPPETAM
ORAMED1
CCS_SCAN
SCB_LINK
DBARO
DBADDM DBARO2
AOGEMS
SCB_REMOTE_CLONE
OEMUSER
SECADMIN SECONDARY SECONDA
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 POHK1API3)

Instance oracle19:1:1621:POHK1API3

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

Extended Evidence:

Statistics:

Query returned 47 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 Passed

Evaluation Date 08/04/2024 at 10:09:56 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

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. **Passed** HIGH standardchartered.com)

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

Previous Status

Evaluation Date 08/04/2024 at 10:09:56 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

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:POHK1API3) **Passed** HIGH

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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

(1.58) 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 10:09:56 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'

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:POHK1CAT. Passed **HIGH** hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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** POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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') Passed HIGH (IAM-400,CIS-26,CIS-9)(oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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
3	DEFAULT	SCB_19C_PWD_VERIFY_FUNCT	ION NO
3	ORA_STIG_PROFILE	SCB_19C_PWD_VERIFY_FUNCT	ION NO
1	DEFAULT	SCB_19C_PWD_VERIFY_FUNCT	ION NO
1	ORA_STIG_PROFILE	SCB_19C_PWD_VERIFY_FUNCT	ION NO
1	SCB_STATIC_APP	SCB_19C_PWD_VERIFY_FUNCT	ION YES
3	SCB SUPP	SCB 19C PWD VERIFY FUNCT	ON NO

Extended Evidence:

Statistics:

Query returned 6 rows

(1.59) 101070 Status of Database user password complexity('PASSWORD_VERIFY_FUNCTION') Passed HIGH (IAM-400,CIS-26,CIS-9)(oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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
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') **Passed HIGH** (IAM-400,CIS-26,CIS-9)(oracle19:1:1621:POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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
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
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
4	SCB_SUPP	SCB_19C_PWD_VERIFY_FUNCTION NO
3	SCB_STATIC_APP_ATX	SCB_19C_PWD_VERIFY_FUNCTION NO
3	DEFAULT	SCB_19C_PWD_VERIFY_FUNCTION NO
1	ORA STIG PROFILE	SCB 19C PWD VERIEY FUNCTION NO

Extended Evidence:

Statistics:

Instance

Query returned 14 rows

(1.60) 101075 Status of the IDLE-TIME resource parameter set for Oracle profiles (IAM-450)

Failed MEDIUM

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

Previous Status

Evaluation Date 08/04/2024 at 10:09:56 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

Instance

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

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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=

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:

Query returned 2 rows

(1.60) 101075 Status of the IDLE-TIME resource parameter set for Oracle profiles (IAM-450) (oracle19:1:1621:POHK1API3)

Passed MEDIUM

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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

(1.61) 101101 Ensure 'EXECUTE_CATALOG_ROLE' Is Revoked from Unauthorized 'GRANTEE' (CIS-62)(oracle19:1:1621:POHK1RCT.hk.standardchartered.com) oracle19:1:1621:POHK1RCT.hk.standardchartered.com

Passed

HIGH

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:57 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:POHK1CAT.hk.standardchartered.com)

Passed

HIGH

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:57 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')

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

(1.61) 101101 Ensure 'EXECUTE CATALOG ROLE' Is Revoked from Unauthorized 'GRANTEE' **HIGH Passed** (CIS-62)(oracle19:1:1621:POHK1API3)

oracle19:1:1621:POHK1API3 Instance

Previous Status

08/04/2024 at 10:09:56 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

(1.62) 101103 Ensure 'SELECT_CATALOG_ROLE' Is Revoked from Unauthorized 'GRANTEE'(CIS-61) 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 10:09:57 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 GRANTEE, GRANTEE, SELECT_CATALOG_ROLE 'I RIV'S
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

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

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:POHK1CAT.hk.standardchartered.com)

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

Previous Status Passed

08/04/2024 at 10:09:57 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 GRANTEE, GRANTEE, SELECT_CATALOG_ROLE 'I RIV'S
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:POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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%'

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

Previous Status

08/04/2024 at 10:09:57 PM (GMT+0530) **Evaluation Date**

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) **Passed**

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

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

Previous Status

Evaluation Date 08/04/2024 at 10:09:57 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:

Ouery returned 0 rows

(1.63) 101107 Ensure 'CREATE LIBRARY' Is Revoked from Unauthorized 'GRANTEE'(CIS-57)

Passed HIGH

HIGH

(oracle19:1:1621:POHK1API3)

oracle19:1:1621:POHK1API3 Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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) **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 10:09:57 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:

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) HIGH Passed (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

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

Previous Status

Evaluation Date 08/04/2024 at 10:09:57 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

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:POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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) **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 10:09:57 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:

DBOUERY: 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) **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 10:09:57 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:

Query returned 0 rows

(1.65) 101109 Ensure 'ALTER SYSTEM' Is Revoked from Unauthorized 'GRANTEE'(CIS-55)

Passed HIGH

(oracle19:1:1621:POHK1API3)

Instance oracle19:1:1621:POHK1API3 Previous Status

Evaluation Date 08/04/2024 at 10:09:57 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

(1.66) 101110 Ensure 'BECOME USER' Is Revoked from Unauthorized 'GRANTEE'(CIS-53)

Passed HIGH

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

Previous Status Passed

08/04/2024 at 10:09:57 PM (GMT+0530) **Evaluation Date**

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

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

Scan Parameters:

DBOUERY: 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:

Previous Status

Query returned 0 rows

(1.66) 101110 Ensure 'BECOME USER' Is Revoked from Unauthorized 'GRANTEE'(CIS-53)

Passed

HIGH

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

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

Evaluation Date 08/04/2024 at 10:09:57 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) (oracle19:1:1621:POHK1API3)

Passed

HIGH

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:57 PM (GMT+0530)

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

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

Scan Parameters:

DBQUERY:

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

Expected any of the selected values below:

Set status to PASS if no data found

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.67) 101112 Ensure 'AUDIT SYSTEM' Is Revoked from Unauthorized 'GRANTEE'(CIS-51)

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 10:09:57 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

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

Previous Status Passed

08/04/2024 at 10:09:57 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:POHK1API3)

Passed HIGH

oracle19:1:1621:POHK1API3 Instance

Previous Status Passed

08/04/2024 at 10:09:57 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

(1.68) 101113 Ensure 'SELECT ANY DICTIONARY' Is Revoked from Unauthorized 'GRANTEE'(cis-49) **MEDIUM** Passed (oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:57 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 '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%'

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 10:09:57 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 'GCDC' 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:

Query returned 0 rows

(1.68) 101113 Ensure 'SELECT ANY DICTIONARY' Is Revoked from Unauthorized 'GRANTEE'(cis-49) Failed **MEDIUM** (oracle19:1:1621:POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Failed

Evaluation Date 08/04/2024 at 10:09:57 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

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

> **GRANTEE PRIVILEGE** CC ITRS SELECT ANY DICTIONARY

Extended Evidence:

Statistics:

Instance

Query returned 1 rows

(1.69) 101115 Ensure 'ALL' Is Revoked from Unauthorized 'GRANTEE' on 'AUD\$'(CIS-42) (oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

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

HIGH Passed

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:57 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)

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 10:09:57 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');

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

(1.69) 101115 Ensure 'ALL' Is Revoked from Unauthorized 'GRANTEE' on 'AUD\$'(CIS-42)

HIGH **Passed**

(oracle19:1:1621:POHK1API3)

oracle19:1:1621:POHK1API3

Previous Status Passed

08/04/2024 at 10:09:57 PM (GMT+0530) **Evaluation Date**

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

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

Scan Parameters:

DBOUERY:

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:

Query returned 0 rows

(1.70) 101140 Status of the 'REMOTE_LISTENER' setting via SQL query (CIS-8)(oracle19:1:1621: **Passed HIGH** POHK1API3)

oracle19:1:1621:POHK1API3 Instance

Previous Status

Evaluation Date 08/04/2024 at 10:09:56 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

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

(1.70) 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 Passed

Evaluation Date 08/04/2024 at 10:09:56 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

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

(1.70) 101140 Status of the 'REMOTE_LISTENER' setting via SQL query (CIS-8)(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 10:09:56 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

(1.71) 101149 Status of the existence of the sys.user\$mig table(CIS-33)(oracle19:1:1621:POHK1API3) Passed **HIGH**

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:57 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 10:09:57 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 10:09:57 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 POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:57 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 POHK1RCT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:57 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 oracle 19:1:1621:POHK1CAT.hk.standardchartered.com

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:57 PM (GMT+0530)

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

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

Scan Parameters:

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

Expected any of the selected values below:

Set status to PASS if no data found

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(1.73) 1051 Status of the 'os_roles=' setting in init.ora(oracle19:1:1621:POHK1API3) Passed HIGH

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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 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 10:09:56 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 E	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:POHK1RCT.hk. standardchartered.com)

Passed HIGH

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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)

Extended Evidence:

NAME	VALUE
os_roles	FALSE
os_roles	FALSE
os_roles	FALSE

(1.74) 101064 Status of instance configuration (alter database / alter system) are captured in the security events(oracle19:1:1621:POHK1API3)

HIGH Passed

HIGH

oracle19:1:1621:POHK1API3 Instance

Previous Status

08/04/2024 at 10:09:56 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

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** security events(oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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:POHK1CAT.hk.standardchartered.com)

Passed

HIGH

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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
SCB_AUDIT_DDL_POLICY	ALTER SYSTEM	STANDARD ACTION

Extended Evidence:

Statistics:

Query returned 3 rows

2. TIP 3.0

(2.1) 101311 Ensure all Users are authenticated before access to an information System(IAM-340) Passed MEDIUM (oracle19:1:1621:POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 PM (GMT+0530)

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

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

Scan Parameters:

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

'PUPPETAM')

Expected is contained in regular expression list

DB Column Name: AUTHENTICATION_TYPE

^PASSWORD\$

OR, any of the selected values below: Set status to PASS if no data found Actual Last Updated:08/04/2024 at 06:01:09 PM (GMT+0530) **AUTHENTICATION_TYPE** PASSWORD **Extended Evidence:** Statistics: Query returned 1 rows

(2.1) 101311 Ensure all Users are authenticated before access to an information System(IAM-340) **Failed MEDIUM** (oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

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

Previous Status

Evaluation Date 08/04/2024 at 10:09:56 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

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:

Additional values found in failed controls: Unexpected values

EXTERNAL

(2.1) 101311 Ensure all Users are authenticated before access to an information System(IAM-340) **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 10:09:56 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', 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

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

AUTHENTICATION_TYPE

PASSWORD

Extended Evidence:

Statistics:

Query returned 1 rows

(2.2) 101319 Status of 'DBA_%' granted to grantees (direct and indirect grants)(CIS-43) (oracle19:1:1621:POHK1API3) **Passed**

oracle19:1:1621:POHK1API3 Instance

Passed Previous Status

Evaluation Date 08/04/2024 at 10:09:57 PM (GMT+0530)

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

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

Scan Parameters:

DBQUERY: SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS A WHERE TABLE_NAME LIKE 'DBA_%' AND OWNER = 'SYS' AND GRANTEE

NOT IN (SELECT USERNAME FROM DBA_USERS WHERE ORACLE_MAINTAINED='Y') AND GRANTEE NOT IN (SELECT ROLE FROM DBA_ROLES WHERE ORACLE_MAINTAINED='Y') AND GRANTEE NOT IN (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%'

HIGH

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

(2.2) 101319 Status of 'DBA_%' granted to grantees (direct and indirect grants)(CIS-43) HIGH **Passed** (oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

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

Previous Status

Evaluation Date 08/04/2024 at 10:09:57 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:POHK1CAT.hk.standardchartered.com)

Passed

HIGH

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

Previous Status Passed

08/04/2024 at 10:09:57 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 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', 'INFA_META_02', 'PUPPETAM', 'ORDS_ADMIN', 'ORDS_METADATA') AND GRANTEE NOT INFA_META_01', 'INFA_META_01', 'INFA_ 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

(2.3) 101322 Ensure 'DBA_SYS_PRIVS.%' Is Revoked from Unauthorized 'GRANTEE' with 'ADMIN_OPTION'(CIS-46)(oracle19:1:1621:POHK1API3)

Passed HIGH

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

08/04/2024 at 10:09:57 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:POHK1RCT.hk.standardchartered.com)

Passed HIGH

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

Previous Status Passed

08/04/2024 at 10:09:57 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:POHK1CAT.hk.standardchartered.com)

HIGH **Passed**

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:57 PM (GMT+0530)

Ensure 'DBA SYS PRIVS.%' Is Revoked from Unauthorized 'GRANTEE' with 'ADMIN OPTION'(CIS-46)

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

Scan Parameters:

DBQUERY: SELECT GRANTEE, PRIVILEGE, CON_ID

FROM CDB_SYS_PRIVS A WHERE ADMIN_OPTION='YES'
AND GRANTEE NOT IN (SELECT USERNAME FROM CDB_USERS WHERE ORACLE_MAINTAINED='Y')

AND GRANTEE NOT IN (SELECT ROLE FROM CDB_ROLES WHERE ORACLE_MAINTAINED='Y')
AND GRANTEE NOT IN ('CCS_SCAN','SECADMIN','ORAMED1','GGADMIN','SCB_ADMIN','AOGEMS','DBAID','DBADDM','OEMUSER',
'SCB_LINK', 'ORACLE', 'ORAMED2', 'PATROL','PUPPETAM','ORDS_ADMIN')

Expected any of the selected values below:

Set status to PASS if no data found

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.4) 101323 Ensure 'EXEMPT ACCESS POLICY' Is Revoked from Unauthorized 'GRANTEE'(CIS-52) HIGH (oracle19:1:1621:POHK1API3)

oracle19:1:1621:POHK1API3 Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:57 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

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:POHK1RCT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:57 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:

SELECT GRANTEE, PRIVILEGE, CON_ID DBQUERY:

SELECT GRANTEE, FRIVILEGE, COIN_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')

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

(2.4) 101323 Ensure 'EXEMPT ACCESS POLICY' Is Revoked from Unauthorized 'GRANTEE'(CIS-52) **Passed HIGH** (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

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

Previous Status

08/04/2024 at 10:09:57 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

(2.5) 101325 Status of '%ANY%' system privilege granted to grantees (direct and indirect grants) **Failed HIGH** (CIS-45)(oracle19:1:1621:POHK1API3)

oracle19:1:1621:POHK1API3 Instance

Previous Status Failed

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
'%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

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

GRANTEE	PRIVILEGE
CC_ITRS	SELECT ANY DICTIONARY

Extended Evidence:

Statistics:

Query returned 1 rows

(2.5) 101325 Status of '%ANY%' system privilege granted to grantees (direct and indirect grants) (CIS-45)(oracle19:1:1621:POHK1RCT.hk.standardchartered.com) **Passed** HIGH

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

Previous Status Passed

08/04/2024 at 10:09:57 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:

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')
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%'

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) HIGH Passed (CIS-45)(oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:57 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')

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_PERFSTATM' and GRANTEE not like 'SPLEX%' and GRANTEE

TOTAL INDEX OF THE NOTICE OF

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

(2.6) 101326 Status of username and account status granted SELECT ANY TABLE privilege(CIS-50) Passed **HIGH** (oracle19:1:1621:POHK1API3)

oracle19:1:1621:POHK1API3 Instance

Previous Status Passed

08/04/2024 at 10:09:57 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 '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'
'AOGEM'' '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:POHK1RCT.hk.standardchartered.com)

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

Passed Previous Status

Evaluation Date 08/04/2024 at 10:09:57 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:

DBOUERY:

SVS_PRVS
AND CRANTEE NOT IN (SELECT USERNAME FROM DBA_USERS WHERE
AND CRANTEE NOT IN (SELECT DAY DBA_USER) WHERE ORACLE MANTAINED=*)
NOT IN (SELECT BOLE FROM DBA_ROLES WHERE ORACLE MANTAINED=*)
DIANT, DBARO, DBAROZ, CRANEDT (CARADMY, SCB_LINK), SCB_LINK, 'ORACLE, 'ORAMED2', "PATROL', "PUPPETAM, 'ORDS_ADMIN') and GRANTEE not like "SCDC%" and GRANTEE not like "ACCEMIN" and GRANTEE not like "SCLINK" and GRANTEE not like "SCLI

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:POHK1CAT.hk.standardchartered.com) HIGH

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

Previous Status Passed

08/04/2024 at 10:09:57 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 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 'PATROLM' and GRANTEE not like 'APEXM' and GRANTEE not like 'GGMONM' and GRANTEE not like 'PATROLM' and GRANTEE not like 'SCB_PERFSTATM' and GRANTEE not like 'SPLEXM' and GRANTEE not like 'SQLTM' and GRANTEE not like 'AOGEMM'

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 POHK1API3)

oracle19:1:1621:POHK1API3 Instance

Previous Status

08/04/2024 at 10:09:57 PM (GMT+0530) **Evaluation Date**

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

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

Scan Parameters:

DBOUERY: 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

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

POHK1RCT.hk.standardchartered.com)

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

Previous Status

Evaluation Date 08/04/2024 at 10:09:57 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: **Passed HIGH** POHK1CAT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:57 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

(2.8) 101332 Status of the FAILED LOGIN ATTEMPTS resource parameter set in all Oracle profiles **HIGH Passed** (oracle19:1:1621:POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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 SUPP:3

SCB_STATIC_APP:UNLIMITED

SCB_INFRA_APP:UNLIMITED

ORA_STIG_PROFILE:6

SCB_STATIC_APP_PSS:UNLIMITED

SCB_STATIC_APP_ATX:UNLIMITED

DEFAULT:UNLIMITED

SCB_INFRA_SUPP:3

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:POHK1RCT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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:UNLIMITED

SCB_SUPP:3

DEFAULT:UNLIMITED

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 **HIGH Passed** (oracle19:1:1621:POHK1CAT.hk.standardchartered.com)

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

Previous Status

Evaluation Date 08/04/2024 at 10:09:56 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

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

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

(2.9) 101336 Status of the login & logoff security events for administrators_SLM-010 (oracle19:1:1621:POHK1API3)

Passed

HIGH

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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

•				
Л	ct		2	
_	L	u	a	

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	OB IECT ACTION

Extended Evidence:

Statistics:

Query returned 60 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 10:09:56 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	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

OCD ALIDIT DDI DOLLOV	DDOD DDOGEDLIDE	OTTANDA DD. A OTTONI
SCB_AUDIT_DDL_POLICY	DROP PROCEDURE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	CREATE TYPE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	DROP TYPE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	ALTER ROLE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	ALTER TYPE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	ALTER VIEW	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	CREATE FUNCTION	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	ALTER FUNCTION	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	DROP FUNCTION	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	CREATE PACKAGE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	ALTER PACKAGE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	DROP PACKAGE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	CREATE PACKAGE BODY	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	ALTER PACKAGE BODY	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	DROP PACKAGE BODY	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	CREATE DIRECTORY	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	DROP DIRECTORY	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	CHANGE PASSWORD	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	ALTER SYNONYM	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	ALTER DATABASE LINK	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	CREATE PLUGGABLE DATABASE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	ALTER PLUGGABLE DATABASE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	DROP PLUGGABLE DATABASE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	CREATE LOCKDOWN PROFILE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	DROP LOCKDOWN PROFILE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	ALTER LOCKDOWN PROFILE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	GRANT	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	REVOKE	STANDARD ACTION
SCB_AUDIT_DROP_POLICY	DROP TABLE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	ALL	OBJECT ACTION

Extended Evidence:

Statistics:

Query returned 60 rows

(2.9) 101336 Status of the login & logoff security events for administrators_SLM-010 (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 10:09:56 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	DROP PROFILE	SYSTEM PRIVILEGE
SCB_AUDIT_DDL_POLICY	ALTER PROFILE	SYSTEM PRIVILEGE
SCB_AUDIT_DDL_POLICY	CREATE PROFILE	SYSTEM PRIVILEGE

NER AUDIT DOL, POLICY CREATE NIJE SER AUDIT DOL, POLICY CREATE INTRABASE LINK SYSTEM PRIVILEGE SER AUDIT DOL, POLICY ALTER USER SYSTEM PRIVILEGE SER AUDIT DOL, POLICY CREATE INDEX SER AUDIT DOL, POLICY CREATE INDEX STANDARD ACTION SER AUDIT DOL, POLICY ALTER SEQUENCE STANDARD ACTION SER AUDIT DOL, POLICY BEOP SYNONYM STANDARD ACTION SER AUDIT DOL, POLICY DEOP SYNONYM STANDARD ACTION STANDARD ACTION STANDARD ACTION STANDARD ACTION STANDARD ACTION S	SCB_AUDIT_DDL_POLICY	ALTER DATABASE	SYSTEM PRIVILEGE
SCR_AUDT_DOL_POLICY CREATE DATABASE_LINK SYSTEM PRIVILEGE SCR_AUDT_DOL_POLICY CREATE USER SYSTEM PRIVILEGE SCR_AUDT_DOL_POLICY CREATE USER SYSTEM PRIVILEGE SCR_AUDT_DOL_POLICY CREATE USER SYSTEM PRIVILEGE SCR_AUDT_DOL_POLICY CREATE TABLE STANABAD_ACTION SCR_AUDT_DOL_POLICY CREATE TABLE STANABAD ACTION SCR_AUDT_DOL_POLICY CREATE SPOUNCE SCR_AUDT_DOL_POLICY CREATE SPOUNCE SCR_AUDT_DOL_POLICY CREATE SPOUNCE SCR_AUDT_DOL_POLICY CREATE SPOUNCE SCR_AUDT_DOL_POLICY ALTER SEQUENCE STANABAD ACTION SCR_AUDT_DOL_POLICY ALTER TABLE STANABAD ACTION SCR_AUDT_DOL_POLICY ALTER SEQUENCE STANABAD ACTION SCR_AUDT_DOL_POLICY ALTER TABLE STANABAD ACTION SCR_AUDT_DOL_POLICY CREATE SYNONYM STANABAD ACTION STANABAD ACTION SCR_AUDT_DOL_POLICY CREATE SYNONYM STANABAD ACTION STANABAD ACTION STANABAD ACTION STANABAD ACTION STANABAD ACTION S			
SCE AUDIT DDI. POLICY SCE AUDIT DDI. POLICY ALTER USER SYSTEM REVULECE SCE AUDIT DDI. POLICY ALTER SYSTEM SYSTEM PRIVILECE SCE AUDIT DDI. POLICY ALTER SYSTEM SYSTEM PRIVILECE SCE AUDIT DDI. POLICY CREATE INDE SCE AUDIT DDI. POLICY CREATE INDE SCE AUDIT DDI. POLICY CREATE INDEX STANDARD ACTION SCE AUDIT DDI. POLICY CREATE ROBEX STANDARD ACTION SCE AUDIT DDI. POLICY ALTER SEQUENCE STANDARD ACTION SCE AUDIT DDI. POLICY BROP SEQUENCE STANDARD ACTION SCE AUDIT DDI. POLICY BROP SEQUENCE STANDARD ACTION SCE AUDIT DDI. POLICY BROP SYNONYM STANDARD ACTION SCE AUDIT DDI. POLICY CREATE PROCEDURE STANDARD ACTION STANDARD ACTION SCE AUDIT DDI. POLICY CREATE PROCEDURE STA			
SCR AUDIT DDL. POLICY CREATE USER SYSTEM PRIVILEGE SCR AUDIT DDL. POLICY CREATE TABLE STANDARD ACTION SCR AUDIT DDL. POLICY CREATE TABLE STANDARD ACTION SCR AUDIT DDL. POLICY CREATE RIDEX STANDARD ACTION SCR AUDIT DDL. POLICY CREATE SEQUENCE STANDARD ACTION SCR AUDIT DDL. POLICY ALTER SEQUENCE STANDARD ACTION SCR AUDIT DDL. POLICY CREATE SYNONYM STANDARD ACTION SCR AUDIT DDL. POLICY CREATE SPROCHURE STANDARD ACTION SCR AUDIT DDL. POLICY CREATE SPROCHURE STANDARD ACTION SCR AUDIT DDL. POLICY CREATE SPROCHURE STANDARD ACTION SCR AUDIT DDL. POLICY CREATE SEQUENCE STANDARD ACTION SCR AUDIT DDL. POLICY ALTER SECUENCE STANDARD ACTION SCR AUDIT DDL. POLICY ALTER SYSTEM STANDARD ACTION SCR AUDIT DDL. POLICY CREATE TIME SYSTEM STANDARD ACTION SCR AUDIT DDL. POLICY CREATE TIME SYSTEM STANDARD ACTION SCR AUDIT DDL. POLICY CREATE TIME SYSTEM STANDARD ACTION SCR AUDIT DDL. POLICY CREATE TIME SYSTEM STANDARD ACTION SCR AUDIT DDL. POLICY CREATE TIME SYS			
SCR AUDT DOL, POLICY KER AUDT DOL, POLICY CREATE TABLE SCR AUDT DOL, POLICY CREATE TABLE SCR AUDT DOL, POLICY CREATE TABLE STANDARD ACTION SCR AUDT DOL, POLICY CREATE TABLE STANDARD ACTION SCR AUDT DOL, POLICY ALTER NIDEX STANDARD ACTION SCR AUDT DOL, POLICY ALTER NIDEX STANDARD ACTION SCR AUDT DOL, POLICY ALTER NIDEX STANDARD ACTION SCR AUDT DOL, POLICY ALTER SEQUENCE STANDARD ACTION SCR AUDT DOL, POLICY DROP STRONYM STANDARD ACTION SCR AUDT DOL, POLICY DROP STRONYM STANDARD ACTION SCR AUDT DOL, POLICY CREATE SYNONYM STANDARD ACTION SCR AUDT DOL, POLICY CREATE SYNONYM STANDARD ACTION SCR AUDT DOL, POLICY CREATE SYNONYM STANDARD ACTION SCR AUDT DOL, POLICY CREATE PROCEDURE STANDARD ACTION SCR AUDT DOL, POLICY CREATE BOATABASE LINK STANDARD ACTION SCR AUDT DOL, POLICY ALTER PROCEDURE STANDARD ACTION SCR AUDT DOL, POLICY CREATE BOATABASE LINK STANDARD ACTION SCR AUDT DOL, POLICY ALTER SYSTEM STANDARD ACTION STANDARD ACTION SCR AUDT DOL, POLICY AL			
SCR_AUDT DEL_POLICY ESCR_AUDT DEL_POLICY CREATE INDEX STANDARD ACTION SCR_AUDT DEL_POLICY CREATE SEQUENCE STANDARD ACTION SCR_AUDT DEL_POLICY ALTER SEQUENCE STANDARD ACTION SCR_AUDT DEL_POLICY SCR_AUDT DEL_POLICY CREATE STANDARD ACTION SCR_AUDT DEL_POLICY SCR_AUDT DEL_POLICY GREATE STANDARD ACTION SCR_AUDT DEL_POLICY SCR_AUDT DEL_POLICY CREATE STANDARD ACTION SCR_AUDT DEL_POLICY SCR_AUDT DEL_POLICY CREATE STANDARD ACTION SCR_AUDT DEL_POLICY CREATE FROCEDURE STANDARD ACTION SCR_AUDT DEL_POLICY CREATE FROCEDURE STANDARD ACTION SCR_AUDT DEL_POLICY ALTER SCR_SCR_SCR_SCR_SCR_SCR_SCR_SCR_SCR_SCR_			
SCR_AUDT_DDL_POLICY CREATE TABLE STANDARD ACTION SCR_AUDT_DDL_POLICY CREATE STANDARD ACTION SCR_AUDT_DDL_POLICY SCR_AUDT_DDL_POLICY ATTER NDFEX STANDARD ACTION SCR_AUDT_DDL_POLICY ATTER SEQUENCE STANDARD ACTION SCR_AUDT_DDL_POLICY DROP SEQUENCE STANDARD ACTION SCR_AUDT_DDL_POLICY DROP SEQUENCE STANDARD ACTION SCR_AUDT_DDL_POLICY SCR_AUDT_DDL_POLICY DROP SEQUENCE STANDARD ACTION SCR_AUDT_DDL_POLICY CREATE PROCEDURE STANDARD ACTION SCR_AUDT_DDL_POLICY CREATE DATABASE LINK STANDARD ACTION SCR_AUDT_DDL_POLICY CREATE DATABASE LINK STANDARD ACTION SCR_AUDT_DDL_POLICY CREATE SYSTEM STANDARD ACTION SCR_AUDT_DDL_POLICY ATTER USER STANDARD ACTION SCR_AUDT_DDL_POLICY ATTER SYSTEM STANDARD ACTION SCR_AUDT_DDL_POLICY ATTER SYSTEM STANDARD ACTION SCR_AUDT_DDL_POLICY ATTER SYSTEM STANDARD ACTION SCR_AUDT_DDL_POLICY CREATE SYSTEM STANDARD ACTION SCR_AUDT_DDL_POLICY CREATE ROSE STANDARD ACTION STAN			
SCB_AUDIT_DOL_POLICY CREATE NDEX STANDARD ACTION SCB_AUDIT_DOL_POLICY ALTER INDEX STANDARD ACTION SCB_AUDIT_DOL_POLICY ALTER INDEX STANDARD ACTION SCB_AUDIT_DOL_POLICY ALTER TENDEX STANDARD ACTION SCB_AUDIT_DOL_POLICY ALTER TENDEX STANDARD ACTION SCB_AUDIT_DOL_POLICY ALTER TABLE STANDARD ACTION SCB_AUDIT_DOL_POLICY DROP SEQUENCE STANDARD ACTION SCB_AUDIT_DOL_POLICY SCB_AUDIT_DOL_POLICY DROP SEQUENCE STANDARD ACTION SCB_AUDIT_DOL_POLICY ALTER PROCEDURE STANDARD ACTION SCB_AUDIT_DOL_POLICY ALTER SCB_AUDIT_DOL_POLICY SCB_AUDIT_DOL_POLICY ALTER SCB_AUDIT_DOL_POLICY SCB_AUDIT_DOL_POLICY ALTER SCB_AUDIT_DOL_POLICY SCB_AUDIT_DOL_POLICY ALTER SCB_AUDIT_DOL_POLICY CREATE BCB_BCB_BCB_BCB_BCB_BCB_BCB_BCB_BCB_BCB			
SCR ALDIT DDL. POLICY CREATE SPOUENCE STANDARD ACTION SCR ALDIT DDL. POLICY ALTER INDEX STANDARD ACTION SCR ALDIT DDL. POLICY ALTER SEQUENCE STANDARD ACTION SCR ALDIT DDL. POLICY DROP SEQUENCE STANDARD ACTION SCR ALDIT DDL. POLICY DROP SEQUENCE STANDARD ACTION SCR ALDIT DDL. POLICY DROP SEQUENCE STANDARD ACTION SCR ALDIT DDL. POLICY SCR ALDIT DDL. POLICY DROP SYNONYM STANDARD ACTION SCR ALDIT DDL. POLICY SCR ALDIT DDL. POLICY DROP VIEW STANDARD ACTION SCR ALDIT DDL. POLICY SCR ALDIT DDL. POLICY CREATE PROCEDURE STANDARD ACTION SCR ALDIT DDL. POLICY CREATE PROCEDURE STANDARD ACTION SCR ALDIT DDL. POLICY CREATE PROCEDURE STANDARD ACTION SCR ALDIT DDL. POLICY CREATE DATABASS LINK STANDARD ACTION SCR ALDIT DDL. POLICY CREATE DATABASS LINK STANDARD ACTION SCR ALDIT DDL. POLICY ALTER SYSTEM STANDARD ACTION SCR ALDIT DDL. POLICY CREATE BROWN SCR ALDIT DDL. POLICY CREATE ROCE STANDARD ACTION SCR ALDIT DDL. POLICY DROP DATABASE LINK STANDARD ACTION SCR ALDIT DDL. POLICY CREATE ROCE STANDARD ACTION SCR ALDIT DDL. POLICY CREATE ROCE STANDARD ACTION SCR ALDIT DDL. POLICY SCR ALDIT DDL. POLICY CREATE ROCE STANDARD ACTION SCR ALDIT DDL. POLICY SCR ALDIT DDL. POLICY CREATE ROCE STANDARD ACTION STANDARD ACTION SCR AL			
SCB AUDIT DDL, POLICY SCB AUDIT DDL, POLICY ATTER SEQUENCE STANDARD ACTION SCB AUDIT DDL, POLICY DROP SEQUENCE STANDARD ACTION SCB AUDIT DDL, POLICY CREATE SYNONYM STANDARD ACTION SCB AUDIT DDL, POLICY SCB AUDIT DDL, POLICY CREATE PROCEDURE STANDARD ACTION SCB AUDIT DDL, POLICY ATTER PROCEDURE STANDARD ACTION SCB AUDIT DDL, POLICY ATTER PROCEDURE STANDARD ACTION SCB AUDIT DDL, POLICY ATTER SYNONYM SCB AUDIT DDL, POLICY ATTER SYNONYM SCB AUDIT DDL, POLICY ATTER STANDARD ACTION SCB AUDIT DDL, POLICY ATTER STANDARD ACTION SCB AUDIT DDL, POLICY ATTER SYNONYM SCB AUDIT DDL, POLICY CREATE USER STANDARD ACTION SCB AUDIT DDL, POLICY CREATE TURGER STANDARD ACTION SCB AUDIT DDL, POLICY CREATE USER STANDARD ACTION STANDARD ACTION STANDARD ACTION STANDARD ACTION STANDA			
SCB ALDIT DDL. POLICY CREATE SEQUENCE STANDARD ACTION SCB ALDIT DDL. POLICY ALTER REQUENCE STANDARD ACTION SCB ALDIT DDL. POLICY ALTER TABLE STANDARD ACTION SCB ALDIT DDL. POLICY SCB ALDIT DDL. POLICY CREATE SYNONYM STANDARD ACTION SCB ALDIT DDL. POLICY CREATE PROCEDURE STANDARD ACTION SCB ALDIT DDL. POLICY CREATE PROCEDURE STANDARD ACTION SCB ALDIT DDL. POLICY CREATE PROCEDURE STANDARD ACTION SCB ALDIT DDL. POLICY CREATE ATTARASE LINK STANDARD ACTION SCB ALDIT DDL. POLICY CREATE ATTARASE LINK STANDARD ACTION SCB ALDIT DDL. POLICY CREATE ATTARASE LINK STANDARD ACTION SCB ALDIT DDL. POLICY ALTER USER STANDARD ACTION SCB ALDIT DDL. POLICY ALTER SYSTEM STANDARD ACTION SCB ALDIT DDL. POLICY ALTER SYSTEM STANDARD ACTION SCB ALDIT DDL. POLICY CREATE RICK SCB ALDIT DDL. POLICY CREATE RICK STANDARD ACTION SCB ALDIT D			
SCB AUDIT DDL POLICY ALTER SPQUENCE STANDARD ACTION SCB AUDIT DDL POLICY ALTER TABLE STANDARD ACTION SCB AUDIT DDL POLICY ALTER SCB			
SCB AUDIT DDL POLICY SCB AUDIT DDL POLICY SCB AUDIT DDL POLICY SCB AUDIT DDL POLICY CREATE SYNONYM STANDARD ACTION SCB AUDIT DDL POLICY ATTER PROCEDURE STANDARD ACTION SCB AUDIT DDL POLICY SCB AUDIT DDL POLICY ATTER PROCEDURE STANDARD ACTION SCB AUDIT DDL POLICY ATTER PROCEDURE STANDARD ACTION SCB AUDIT DDL POLICY ATTER PROCEDURE STANDARD ACTION SCB AUDIT DDL POLICY ATTER SCB STANDARD ACTION SCB AUDIT DDL POLICY ATTER STANDARD ACTION SCB AUDIT DDL POLICY ATTER SCB STANDARD ACTION SCB AUDIT DDL POLICY ATTER SCB STANDARD ACTION SCB AUDIT DDL POLICY ATTER STANDARD ACTION SCB AUDIT DDL POLICY CREATE USER STANDARD ACTION SCB AUDIT DDL POLICY ATTER SCB SCB AUDIT DDL POLICY SCB AUDIT DDL		-	
SCB AUDIT_DDL_POLICY ALTER USER STANDARD ACTION SCB AUDIT_DDL_POLICY CREATE USER STANDARD ACTION SCB AUDIT_DDL_POLICY CREATE USER STANDARD ACTION SCB AUDIT_DDL_POLICY CREATE ROSE STANDARD ACTION SCB AUDIT_DDL_POLICY ALTER TRIGGER STANDARD ACTION SCB AUDIT_DDL_POLICY SCB AUDIT_DDL_POLICY ALTER ROSE STANDARD ACTION STANDARD ACTION SCB AUDIT_DDL_POLICY ALTER ROSE STANDARD ACTION STANDARD ACTION SCB AUDIT_DDL_P		-	
SCB AUDIT DDL POLICY ALTER SYSTEM STANDARD ACTION SCB AUDIT DDL POLICY SCB AUDIT DDL			
SCB AUDIT DDL POLICY ALTER PROCEDURE STANDARD ACTION SCB AUDIT DDL POLICY SCB AUDIT DDL POLICY ALTER STANDARD ACTION SCB AUDIT DDL POLICY ALTER STANDARD ACTION SCB AUDIT DDL POLICY ALTER STANDARD ACTION SCB AUDIT DDL POLICY SCB AUD			
SCB. AUDIT DDL. POLICY ALTER PROCEDURE STANDARD ACTION SCB. AUDIT DDL. POLICY ALTER USER STANDARD ACTION SCB. AUDIT DDL. POLICY SCB. AUDIT DDL. POLICY CREATE USER STANDARD ACTION SCB. AUDIT DDL. POLICY SCB. AUDIT DDL. POLICY DROP USER STANDARD ACTION SCB. AUDIT DDL. POLICY SCB. AUDIT DDL. POLICY DROP USER STANDARD ACTION SCB. AUDIT DDL. POLICY SCB. AUDIT DDL. POLICY DROP USER STANDARD ACTION SCB. AUDIT DDL. POLICY SCB. AUDIT DDL. POLICY DROP USER STANDARD ACTION SCB. AUDIT DDL. POLICY SCB. AUDIT DDL. POLICY SCB. AUDIT DDL. POLICY SCB. AUDIT DDL. POLICY ALTER TRIGGER STANDARD ACTION SCB. AUDIT DDL. POLICY SCB. AUDIT DDL. POLICY ALTER TRIGGER STANDARD ACTION SCB. AUDIT DDL. POLICY SCB. AUDIT DDL. POLICY CREATE PROPILE STANDARD ACTION SCB. AUDIT DDL. POLICY SCB. AUDIT DDL. POLICY CREATE PROPILE STANDARD ACTION SCB. AUDIT DDL. POLICY SCB. AUDIT DDL. POLICY CREATE PROPILE STANDARD ACTION SCB. AUDIT DDL. POLICY SCB. AUDIT DDL. POLICY CREATE PROPILE STANDARD ACTION SCB. AUDIT DDL. POLICY SCB. AUDIT DDL. POLICY CREATE PROPILE STANDARD ACTION SCB. AUDIT DDL. POLICY SCB. AUDIT DDL. POLICY CREATE TYPE STANDARD ACTION SCB. AUDIT DDL. POLICY SCB. AUDIT DDL. POLICY CREATE TYPE STANDARD ACTION SCB. AUDIT DDL. POLICY SCB. AUDIT DDL. POLICY CREATE TYPE STANDARD ACTION SCB. AUDIT DDL. POLICY SCB. AUDIT DDL. POLICY CREATE TYPE STANDARD ACTION SCB. AUDIT DDL. POLICY ALTER ROLE STANDARD ACTION SCB. AUDIT DDL. POLICY CREATE TYPE STANDARD ACTION SCB. AUDIT DDL. POLICY ALTER ROLE STANDARD ACTION SCB. AUDIT DDL. POLICY CREATE TYPE STANDARD ACTION 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 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 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 DROP PROPILE STANDARD ACTION SCB AUDIT DDL POLICY ALTER PROPILE STANDARD ACTION SCB AUDIT DDL POLICY ALTER PROPILE STANDARD ACTION SCB AUDIT DDL POLICY CREATE TYPE STANDARD ACTION SCB AUDIT DDL POLICY SCB AUDIT DDL POLICY ALTER PROPILE STANDARD ACTION SCB AUDIT DDL POLICY ALTER PROPILE STANDARD ACTION SCB AUDIT DDL POLICY ALTER TYPE STANDARD ACTION STANDARD ACTION SCB AUDIT DDL POLICY ALTER TYPE STANDARD ACTION STANDARD ACTION STANDARD ACTION SCB AUDIT DDL POLICY ALTER PROPILE STANDARD ACTION STANDARD ACTION STANDARD ACTION STANDARD ACTION SCB AUDIT DDL POLICY ALTER PROPILE STANDARD ACTION STANDARD ACTION STANDARD ACTION STANDARD ACTION STANDARD ACTION SCB AU			
SCB AUDIT DDL POLICY ATTER USER STANDARD ACTION SCB AUDIT DDL POLICY SCB AUDIT DDL POLICY CREATE USER STANDARD ACTION SCB AUDIT DDL POLICY SCB AUDIT DDL POLICY CREATE USER STANDARD ACTION SCB AUDIT DDL POLICY SCB AUDIT DDL POLICY DROP BOLE SCB AUDIT DDL POLICY SCB AUDIT DDL POLICY SCB AUDIT DDL POLICY CREATE RIGGER STANDARD ACTION SCB AUDIT DDL POLICY SCB AUDIT DDL POLICY CREATE RIGGER STANDARD ACTION SCB AUDIT DDL POLICY ATTER TRIGGER STANDARD ACTION SCB AUDIT DDL POLICY ATTER TRIGGER STANDARD ACTION SCB AUDIT DDL POLICY CREATE PROPILE STANDARD ACTION SCB AUDIT DDL POLICY DROP PROPILE STANDARD ACTION SCB AUDIT DDL POLICY DROP PROPILE STANDARD ACTION SCB AUDIT DDL POLICY CREATE PROPILE STANDARD ACTION SCB AUDIT DDL POLICY DROP PROCEDURE STANDARD ACTION SCB AUDIT DDL POLICY CREATE PROPILE STANDARD ACTION SCB AUDIT DDL POLICY CREATE TYPE STANDARD ACTION SCB AUDIT DDL POLICY ALTER PROFILE STANDARD ACTION SCB AUDIT DDL POLICY CREATE TYPE STANDARD ACTION SCB AUDIT DDL POLICY CREATE TYPE STANDARD ACTION SCB AUDIT DDL POLICY CREATE TYPE STANDARD ACTION SCB AUDIT DDL POLICY ALTER PROFILE STANDARD ACTION STANDARD ACTION SCB AUDIT			
SCB AUDIT_DDL_POLICY CREATE DATABASE LINK 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 USER STANDARD ACTION SCB AUDIT_DDL_POLICY CREATE ROLE STANDARD ACTION SCB AUDIT_DDL_POLICY DROP USER STANDARD ACTION SCB AUDIT_DDL_POLICY DROP USER STANDARD ACTION SCB AUDIT_DDL_POLICY CREATE TRIGGER STANDARD ACTION SCB AUDIT_DDL_POLICY CREATE TRIGGER STANDARD ACTION SCB AUDIT_DDL_POLICY ALTER TRIGGER STANDARD ACTION SCB AUDIT_DDL_POLICY CREATE PROFILE STANDARD ACTION SCB AUDIT_DDL_POLICY CREATE TYPE STANDARD ACTION STANDARD ACTION SCB AUDIT_DDL_POLICY ALTER FUNCTION STANDARD ACTION STANDARD ACTION SCB AUDIT_DDL_POLICY ALTER FUNCTION STANDARD ACTION STANDARD ACTION SCB AUDIT_DDL_POLICY ALTER FUNCTION STANDARD ACTION SCB AUDIT_DDL_POLICY ALTER PUNCTION STANDARD ACTION STANDARD ACTION SCB AUDIT_DDL_POLICY CREATE PACK			
SCE AUDIT DDL POLICY CREATE DATABASE LINK STANDARD ACTION SCE AUDIT DDL POLICY ALTER USER STANDARD ACTION SCE AUDIT DDL POLICY ALTER USER STANDARD ACTION SCE AUDIT DDL POLICY CREATE USER STANDARD ACTION SCE AUDIT DDL POLICY CREATE USER STANDARD ACTION SCE AUDIT DDL POLICY CREATE ROLE STANDARD ACTION SCE AUDIT DDL POLICY CREATE ROLE STANDARD ACTION SCE AUDIT DDL POLICY SCE AUDIT DDL POLICY DROP USER STANDARD ACTION SCE AUDIT DDL POLICY SCE AUDIT DDL POLICY CREATE TRIGGER STANDARD ACTION SCE AUDIT DDL POLICY DROP PROFILE STANDARD ACTION SCE AUDIT DDL POLICY CREATE TRIGGER STANDARD ACTION SCE AUDIT DDL POLICY CREATE TYPE STANDARD ACTION SCE AUDIT DDL POLICY CREATE TYPE STANDARD ACTION SCE AUDIT DDL POLICY CREATE TYPE STANDARD ACTION SCE AUDIT DDL POLICY ALTER FUNCTION STANDARD ACTION SCE AUDIT DDL POLICY ALTER FUNCTION STANDARD ACTION SCE AUDIT DDL POLICY ALTER PACKAGE STANDARD ACTION SCE AUDIT DDL POLICY CREATE			
SCE AUDIT DDL. POLICY SCE AUDIT DDL. POLICY ALTER USER STANDARD ACTION SCE AUDIT DDL. POLICY ALTER USER STANDARD ACTION SCE AUDIT DDL. POLICY CREATE USER STANDARD ACTION SCE AUDIT DDL. POLICY CREATE ROLE STANDARD ACTION SCE AUDIT DDL. POLICY DROP USER STANDARD ACTION SCE AUDIT DDL. POLICY DROP USER STANDARD ACTION SCE AUDIT DDL. POLICY SCE AUDIT DDL. POLICY DROP USER STANDARD ACTION SCE AUDIT DDL. POLICY SCE AUDIT DDL. POLICY SCE AUDIT DDL. POLICY CREATE TRIGGER STANDARD ACTION SCE AUDIT DDL. POLICY ALTER TRIGGER STANDARD ACTION SCE AUDIT DDL. POLICY ALTER ROLE STANDARD ACTION SCE AUDIT DDL. POLICY SCE AUDIT DDL. POLICY ALTER TYPE STANDARD ACTION SCE AUDIT DDL. POLICY SCE AUDIT DDL. POLICY ALTER TYPE STANDARD ACTION SCE AUDIT DDL. POLICY SCE AUDIT DDL. POLICY ALTER TYPE STANDARD ACTION SCE AUDIT DDL. POLICY SCE AUDIT DDL. POLICY ALTER FUNCTION STANDARD ACTION SCE AUDIT DDL. POLICY SCE AUDIT DDL. POLICY ALTER FUNCTION STANDARD ACTION SCE AUDIT DDL. POLICY SCE AUDIT DDL. POLICY ALTER PACKAGE STANDARD ACTION SCE AUDIT DDL. POLICY SCE AUDIT DDL. POLICY ALTER PACKAGE STANDARD ACTION SCE AUDIT DDL. POLICY SCE AUDIT DDL. POLICY ALTER PACKAGE BODY STANDARD ACTION SCE AUDIT DDL. POLICY SCE AUDIT DDL. POLICY SCE AUDIT DDL. POLICY SCE AUDIT			
SCB AUDIT DDL, POLICY SCB AUDIT DDL, POLICY SCB AUDIT DDL, POLICY CREATE USER STANDARD ACTION SCB AUDIT DDL, POLICY SCB AUDIT DDL, P			
SCB_AUDIT_DDL_POLICY CREATE USER STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE ROLE STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE ROLE STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP USER STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP USER STANDARD ACTION SCB_AUDIT_DDL_POLICY 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 CREATE PRIGGER STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE PROFILE STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE PROFILE STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP PROFILE STANDARD ACTION SCB_AUDIT_DDL_POLICY SCB_AUDIT_DDL_POLICY DROP PROFILE STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE TYPE STANDARD ACTION SCB_AUDIT_DDL_POLICY SCB_AUDIT_DDL_POLICY CREATE TYPE STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE TYPE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER ROLE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER ROLE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER TYPE STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE FUNCTION STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER FUNCTION STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE PACKAGE STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE			
SCB_AUDIT_DDL_POLICY CREATE ROLE STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP USER STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP USER 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 DROP PROCEDER STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE PROFILE STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP PROFILE STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP PROFILE STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP PROCEDURE STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP PROCEDURE STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP PROCEDURE STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP TROPE STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP TRYPE STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP TRYPE STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP TYPE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER ROLE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER RUNCTION STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER FUNCTION STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE FUNCTION STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER FUNCTION STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP FUNCTION SCB_AUDIT_DDL_POLICY CREATE FUNCTION STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE FUNCTI			
SCB AUDIT DDL POLICY DROP POLE SCB AUDIT DDL POLICY DROP DROP USER STANDARD ACTION SCB AUDIT DDL POLICY DROP POLE STANDARD ACTION SCB AUDIT DDL POLICY CREATE TRIGGER STANDARD ACTION SCB AUDIT DDL POLICY ALTER TRIGGER STANDARD ACTION SCB AUDIT DDL POLICY DROP PROFILE STANDARD ACTION SCB AUDIT DDL POLICY DROP PROCEDURE STANDARD ACTION SCB AUDIT DDL POLICY DROP PROCEDURE STANDARD ACTION SCB AUDIT DDL POLICY DROP PROCEDURE STANDARD ACTION SCB AUDIT DDL POLICY DROP TYPE STANDARD ACTION SCB AUDIT DDL POLICY DROP TYPE STANDARD ACTION SCB AUDIT DDL POLICY ALTER PUNCTION SCB AUDIT DDL POLICY CREATE FUNCTION SCB AUDIT DDL POLICY ALTER PUNCTION SCB AUDIT DDL POLICY ALTER PUNCTION SCB AUDIT DDL POLICY DROP FUNCTION SCB AUDIT DDL POLICY ALTER PUNCTION SCB AUDIT DDL POLICY ALTER PUNCTION SCB AUDIT DDL POLICY CREATE PUNCTION SCB AUDIT DDL POLICY CREATE PACKAGE STANDARD ACTION SCB AUDI			
SCB AUDIT DDL POLICY DROP USER STANDARD ACTION SCB AUDIT DDL POLICY DROP ROLE STANDARD ACTION SCB AUDIT DDL POLICY ALTER TRIGGER STANDARD ACTION SCB AUDIT DDL POLICY ALTER TRIGGER STANDARD ACTION SCB AUDIT DDL POLICY DROP TRIGGER STANDARD ACTION SCB AUDIT DDL POLICY DROP TRIGGER STANDARD ACTION SCB AUDIT DDL POLICY DROP PROFILE STANDARD ACTION SCB AUDIT DDL POLICY DROP PROCEDURE STANDARD ACTION SCB AUDIT DDL POLICY DROP PROCEDURE STANDARD ACTION SCB AUDIT DDL POLICY DROP PROCEDURE STANDARD ACTION SCB AUDIT DDL POLICY DROP 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 PROFILE STANDARD ACTION SCB AUDIT DDL POLICY ALTER FUNCTION STANDARD ACTION SCB AUDIT DDL POLICY ALTER FUNCTION STANDARD ACTION SCB AUDIT DDL POLICY CREATE FUNCTION STANDARD ACTION SCB AUDIT DDL POLICY DROP FUNCTION STANDARD ACTION SCB AUDIT DDL POLICY CREATE PACKAGE STANDARD ACTION SCB AUDIT DDL POLICY CREATE PACKAGE STANDARD ACTION SCB AUDIT DDL POLICY DROP PACKAGE STANDARD ACTION SCB AUDIT DDL POLICY CREATE PACKAGE BODY STANDARD ACTION SCB AUDIT DDL POLICY CREATE PACKAGE BODY STANDARD ACTION SCB AUDIT DDL POLICY CREATE PACKAGE BODY STANDARD ACTION SCB AUDIT DDL POLICY CREATE DROP PACKAGE BODY STANDARD ACTION SCB AUDIT DDL POLICY CREATE DROP PACKAGE BODY STANDARD ACTION SCB AUDIT DDL POLICY CREATE DRAGAGE BODY STANDARD AC			
SCB_AUDIT_DDL_POLICY 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 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 ALTER PROFILE STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP PROFILE STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP PROFILE STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP PROFILE 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 TYPE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER TYPE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER VIEW STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER FUNCTION STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER FUNCTION STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER FUNCTION STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PACKAGE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PACKAGE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PACKAGE STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PACKAGE BODY STANDAR			
SCB_AUDIT_DDL_POLICY 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 ALTER 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 ALTER ROLE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER ROLE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER VIEW STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER VIEW STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER VIEW STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER FUNCTION SCB_AUDIT_DDL_POLICY ALTER FUNCTION SCB_AUDIT_DDL_POLICY ALTER FUNCTION STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PACKAGE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER 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 DROP PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PACKAGE BODY STANDARD ACTION SCB_AUDIT			
SCB_AUDIT_DDL_POLICY SCB_AUDIT_DDL_POLICY DROP TRIGGER STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE PROFILE STANDARD ACTION SCB_AUDIT_DDL_POLICY SCB_AUDIT_DDL_POLICY 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 ROLE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER TYPE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER TYPE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER VIEW STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER FUNCTION 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 DROP PACKAGE STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP PACKAGE STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PACKAGE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER P			
SCB_AUDIT_DDL_POLICY SCB_AUDIT_DDL_POLICY SCB_AUDIT_DDL_POLICY SCB_AUDIT_DDL_POLICY SCB_AUDIT_DDL_POLICY DROP PROFILE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PROFILE STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP PROFILE STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP PROCEDURE STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP PROCEDURE 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 FUNCTION STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER FUNCTION STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP 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 ALTER PACKAGE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PACKAGE STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP PACKAGE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER 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 ALTER PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER SYNONYM STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER SYNONYM STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER SYNONYM STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER P			
SCB_AUDIT_DDL_POLICY CREATE PROFILE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER 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 TYPE 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 ALTER FUNCTION STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE PACKAGE STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE PACKAGE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PACKAGE STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE 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 CREATE PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE DACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE DACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER SYNONYM STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PLUGGABLE DATABASE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER			
SCB_AUDIT_DDL_POLICY 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 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 SCB_AUDIT_DDL_POLICY ALTER 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 DROP PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE DACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE DACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER SYNONYM STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER SYNONYM STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER DATABASE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PLUGGABLE DATABASE STANDARD ACTION			
SCB_AUDIT_DDL_POLICY SCB_AUDIT_DDL_POLICY SCB_AUDIT_DDL_POLICY CREATE TYPE 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 TYPE 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 BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE DIRECTORY STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER SYNONYM STANDARD ACTION			
SCB_AUDIT_DDL_POLICY CREATE TYPE STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP 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 TYPE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER TYPE 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 ALTER PACKAGE STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE PACKAGE STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE 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 ALTER PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE DIRECTORY STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER SYNONYM STANDARD ACTION SCB_AUDIT_DDL_POLICY CHANGE PASSWORD STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER SYNONYM STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER DATABASE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PLUGGABLE DATABASE 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 PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE DIRECTORY STAND			
SCB_AUDIT_DDL_POLICY 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 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 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 ALTER PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE 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 ALTER DATABASE LINK STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER DATABASE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PLUGGABLE DATABASE 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 SCB_AUDIT_DDL_POLICY ALTER FUNCTION SCB_AUDIT_DDL_POLICY ALTER FUNCTION SCB_AUDIT_DDL_POLICY DROP FUNCTION SCB_AUDIT_DDL_POLICY CREATE PACKAGE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PACKAGE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PACKAGE STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE PACKAGE STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE 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 CREATE DIRECTORY STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER SYNONYM STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER DATABASE LINK STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER DATABASE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PLUGGABLE DATABASE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PLUGGABLE DATABASE STANDARD ACTION			
SCB_AUDIT_DDL_POLICY ALTER TYPE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER VIEW STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE FUNCTION SCB_AUDIT_DDL_POLICY ALTER FUNCTION SCB_AUDIT_DDL_POLICY ALTER FUNCTION SCB_AUDIT_DDL_POLICY DROP FUNCTION 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 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 ALTER PACKAGE BODY STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE DIRECTORY STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER SYNONYM STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER DATABASE LINK STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER DATABASE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PLUGGABLE DATABASE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PLUGGABLE DATABASE STANDARD ACTION			
SCB_AUDIT_DDL_POLICY SCB_AUDIT_DDL_POLICY SCB_AUDIT_DDL_POLICY SCB_AUDIT_DDL_POLICY SCB_AUDIT_DDL_POLICY SCB_AUDIT_DDL_POLICY ALTER FUNCTION STANDARD ACTION STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP FUNCTION STANDARD ACTION SCB_AUDIT_DDL_POLICY SCB_AUDIT_DDL_POLICY ALTER PACKAGE STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP 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 DROP 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 SYNONYM STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER DATABASE LINK STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER DATABASE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PLUGGABLE DATABASE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PLUGGABLE DATABASE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PLUGGABLE DATABASE STANDARD ACTION			
SCB_AUDIT_DDL_POLICY 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 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 CREATE DIRECTORY STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE DIRECTORY STANDARD ACTION SCB_AUDIT_DDL_POLICY CHANGE PASSWORD STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER SYNONYM STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER SYNONYM STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER DATABASE LINK STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PACKAGE 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 ALTER FUNCTION STANDARD ACTION SCB_AUDIT_DDL_POLICY CREATE PACKAGE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER 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 SYNONYM STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER DATABASE LINK STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER DATABASE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER DATABASE STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER PLUGGABLE DATABASE STANDARD ACTION			
SCB_AUDIT_DDL_POLICY 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 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 SYNONYM STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER DATABASE LINK STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER DATABASE LINK STANDARD ACTION SCB_AUDIT_DDL_POLICY ALTER 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 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 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 SCB_AUDIT_DDL_POLICY ALTER PLUGGABLE DATABASE STANDARD ACTION SCB_AUDIT_DDL_POLICY SCB_AUDI			
SCB_AUDIT_DDL_POLICY ALTER SYNONYM STANDARD ACTION SCB_AUDIT_DDL_POLICY SCB_AUDIT_DDL_POLICY SCB_AUDIT_DDL_POLICY ALTER DATABASE LINK STANDARD ACTION SCB_AUDIT_DDL_POLICY SCB_AU			
SCB_AUDIT_DDL_POLICYDROP PACKAGESTANDARD ACTIONSCB_AUDIT_DDL_POLICYCREATE PACKAGE BODYSTANDARD ACTIONSCB_AUDIT_DDL_POLICYALTER PACKAGE BODYSTANDARD ACTIONSCB_AUDIT_DDL_POLICYDROP PACKAGE BODYSTANDARD ACTIONSCB_AUDIT_DDL_POLICYCREATE DIRECTORYSTANDARD ACTIONSCB_AUDIT_DDL_POLICYDROP DIRECTORYSTANDARD ACTIONSCB_AUDIT_DDL_POLICYCHANGE PASSWORDSTANDARD ACTIONSCB_AUDIT_DDL_POLICYALTER SYNONYMSTANDARD ACTIONSCB_AUDIT_DDL_POLICYALTER DATABASE LINKSTANDARD ACTIONSCB_AUDIT_DDL_POLICYCREATE PLUGGABLE DATABASESTANDARD ACTIONSCB_AUDIT_DDL_POLICYALTER PLUGGABLE DATABASESTANDARD ACTIONSCB_AUDIT_DDL_POLICYALTER PLUGGABLE DATABASESTANDARD ACTIONSCB_AUDIT_DDL_POLICYDROP PLUGGABLE DATABASESTANDARD ACTION			
SCB_AUDIT_DDL_POLICYCREATE PACKAGE BODYSTANDARD ACTIONSCB_AUDIT_DDL_POLICYALTER PACKAGE BODYSTANDARD ACTIONSCB_AUDIT_DDL_POLICYDROP PACKAGE BODYSTANDARD ACTIONSCB_AUDIT_DDL_POLICYCREATE DIRECTORYSTANDARD ACTIONSCB_AUDIT_DDL_POLICYDROP DIRECTORYSTANDARD ACTIONSCB_AUDIT_DDL_POLICYCHANGE PASSWORDSTANDARD ACTIONSCB_AUDIT_DDL_POLICYALTER SYNONYMSTANDARD ACTIONSCB_AUDIT_DDL_POLICYALTER DATABASE LINKSTANDARD ACTIONSCB_AUDIT_DDL_POLICYCREATE PLUGGABLE DATABASESTANDARD ACTIONSCB_AUDIT_DDL_POLICYALTER PLUGGABLE DATABASESTANDARD ACTIONSCB_AUDIT_DDL_POLICYDROP PLUGGABLE DATABASESTANDARD ACTION			
SCB_AUDIT_DDL_POLICYALTER PACKAGE BODYSTANDARD ACTIONSCB_AUDIT_DDL_POLICYDROP PACKAGE BODYSTANDARD ACTIONSCB_AUDIT_DDL_POLICYCREATE DIRECTORYSTANDARD ACTIONSCB_AUDIT_DDL_POLICYDROP DIRECTORYSTANDARD ACTIONSCB_AUDIT_DDL_POLICYCHANGE PASSWORDSTANDARD ACTIONSCB_AUDIT_DDL_POLICYALTER SYNONYMSTANDARD ACTIONSCB_AUDIT_DDL_POLICYALTER DATABASE LINKSTANDARD ACTIONSCB_AUDIT_DDL_POLICYCREATE PLUGGABLE DATABASESTANDARD ACTIONSCB_AUDIT_DDL_POLICYALTER PLUGGABLE DATABASESTANDARD ACTIONSCB_AUDIT_DDL_POLICYDROP PLUGGABLE DATABASESTANDARD ACTION			
SCB_AUDIT_DDL_POLICYDROP PACKAGE BODYSTANDARD ACTIONSCB_AUDIT_DDL_POLICYCREATE DIRECTORYSTANDARD ACTIONSCB_AUDIT_DDL_POLICYDROP DIRECTORYSTANDARD ACTIONSCB_AUDIT_DDL_POLICYCHANGE PASSWORDSTANDARD ACTIONSCB_AUDIT_DDL_POLICYALTER SYNONYMSTANDARD ACTIONSCB_AUDIT_DDL_POLICYALTER DATABASE LINKSTANDARD ACTIONSCB_AUDIT_DDL_POLICYCREATE PLUGGABLE DATABASESTANDARD ACTIONSCB_AUDIT_DDL_POLICYALTER PLUGGABLE DATABASESTANDARD ACTIONSCB_AUDIT_DDL_POLICYDROP PLUGGABLE DATABASESTANDARD ACTION			
SCB_AUDIT_DDL_POLICYCREATE DIRECTORYSTANDARD ACTIONSCB_AUDIT_DDL_POLICYDROP DIRECTORYSTANDARD ACTIONSCB_AUDIT_DDL_POLICYCHANGE PASSWORDSTANDARD ACTIONSCB_AUDIT_DDL_POLICYALTER SYNONYMSTANDARD ACTIONSCB_AUDIT_DDL_POLICYALTER DATABASE LINKSTANDARD ACTIONSCB_AUDIT_DDL_POLICYCREATE PLUGGABLE DATABASESTANDARD ACTIONSCB_AUDIT_DDL_POLICYALTER PLUGGABLE DATABASESTANDARD ACTIONSCB_AUDIT_DDL_POLICYDROP PLUGGABLE DATABASESTANDARD 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 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 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 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 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 ALTER PLUGGABLE DATABASE STANDARD ACTION SCB_AUDIT_DDL_POLICY DROP PLUGGABLE DATABASE STANDARD ACTION			
SCB_AUDIT_DDL_POLICY DROP PLUGGABLE DATABASE STANDARD ACTION			
		DROP PLUGGABLE DATABASE	STANDARD ACTION
	SCB_AUDIT_DDL_POLICY	CREATE LOCKDOWN PROFILE	STANDARD ACTION

SCB_AUDIT_DDL_POLICY	DROP LOCKDOWN PROFILE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	ALTER LOCKDOWN PROFILE	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	GRANT	STANDARD ACTION
SCB_AUDIT_DDL_POLICY	REVOKE	STANDARD ACTION
SCB_AUDIT_DROP_POLICY	DROP TABLE	STANDARD ACTION
SCB AUDIT DDL POLICY	ALL	OBJECT ACTION

Extended Evidence:

Statistics:

Query returned 69 rows

(2.10) 101339 Status of the PASSWORD_LOCK_TIME resource parameter set in all Oracle profiles Passed HIGH (oracle19:1:1621:POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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:UNLIMITED
SCB_INFRA_APP:UNLIMITED
SCB_SUPP:UNLIMITED
SCB_STATIC_APP_PSS:UNLIMITED
SCB_INFRA_SUPP:UNLIMITED
ORA_STIG_PROFILE:UNLIMITED
SCB_STATIC_APP_ATX:UNLIMITED
DEFAULT: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:POHK1RCT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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:UNLIMITED

DEFAULT:UNLIMITED

ORA_STIG_PROFILE: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 10:09:56 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)

ROFILE ':' LIMIT	
CB_SUPP:UNLIMITED	
EFAULT:UNLIMITED	
CB_INFRA_SUPP:UNLIMITED	
RA_STIG_PROFILE:UNLIMITED	
CB_STATIC_APP:UNLIMITED	
CB_STATIC_APP_ATX:UNLIMITED	
CB_INFRA_APP:UNLIMITED	
CB_STATIC_APP_CCS:UNLIMITED	
CB_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:POHK1RCT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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:UNLIMITED

DEFAULT: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 10:09:56 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_ATX:UNLIMITED
SCB_INFRA_APP:UNLIMITED

SCB_STATIC_APP_CCS:UNLIMITED

SCB_STATIC_APP_ATX_IDLE30:UNLIMITED

Extended Evidence:

Statistics:

Query returned 9 rows

(2.11) 101340 Status of the PASSWORD_LIFE_TIME resource parameter set in all Oracle profiles Passed HIGH (oracle19:1:1621:POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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_INFRA_APP:UNLIMITED SCB_INFRA_SUPP:83 SCB_SUPP:83 SCB_SUPP:83 SCB_STATIC_APP_PSS:UNLIMITED SCB_STATIC_APP_ATX:UNLIMITED DEFAULT: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:POHK1RCT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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\$

SCD_STATIC_APP. :UNLIMI

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
ORA_STIG_PROFILE:20

SCB_SUPP:20

DEFAULT:UNLIMITED

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 10:09:56 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:POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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_SUPP:20 SCB_STATIC_APP_PSS:UNLIMITED SCB_STATIC_APP_ATX:UNLIMITED SCB_INFRA_SUPP:20 SCB_INFRA_SUPP:20 SCB_STATIC_APP:UNLIMITED SCB_INFRA_APP:UNLIMITED DEFAULT: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:POHK1RCT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 PM (GMT+0530)

ORA_STIG_PROFILE:20

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:UNLIMITED

DEFAULT:UNLIMITED

ORA_STIG_PROFILE: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 10:09:56 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

DEFAULT:UNLIMITED

SCB_INFRA_SUPP:UNLIMITED

ORA_STIG_PROFILE:UNLIMITED

SCB_STATIC_APP:UNLIMITED

SCB_STATIC_APP_ATX:UNLIMITED

SCB_INFRA_APP:UNLIMITED

SCB_INFRA_APP:UNLIMITED

SCB_STATIC_APP_CCS:UNLIMITED

SCB_STATIC_APP_ATX_IDLE30:UNLIMITED

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:POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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_INFRA_APP:UNLIMITED SCB_SUPP:UNLIMITED SCB_STATIC_APP_PSS:UNLIMITED SCB_INFRA_SUPP:UNLIMITED ORA_STIG_PROFILE:UNLIMITED SCB_STATIC_APP_ATX:UNLIMITED

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:POHK1RCT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 PM (GMT+0530)

DEFAULT: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:

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:7
ORA_STIG_PROFILE: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:POHK1CAT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 PM (GMT+0530)

Status of the PASSWORD_GRACE_TIME resource parameter set in all Oracle profiles

Status of the PASSWORD_GRACE_TIME resource parameter set in all Oracle profiles

Scan Parameters:

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

Expected is contained in regular expression list

DB Column Name: PROFILE||':'||LIMIT

DEFAULT:7\$

ORA_STIG_PROFILE:7\$
SCB_INFRA_APP.*:7\$
SCB_INFRA_SUPP.*:7\$
SCB_STATIC_APP.*:7\$
SCB_SUPP.*:7\$

MGMT_ADMIN_USER_PROFILE:7\$

MGMT_INTERNAL_USER_PROFILE:UNLIMITED\$

OR, any of the selected values below:

Set status to PASS if no data found

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

PROFILE||':'||LIMIT

SCB_INFRA_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:POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 PM (GMT+0530)

Status of the PASSWORD_GRACE_TIME resource parameter set in all Oracle profiles

Status of the PASSWORD_GRACE_TIME resource parameter set in all Oracle profiles

Scan Parameters:

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

Expected is contained in regular expression list

DB Column Name: PROFILE||':'||LIMIT

DEFAULT:7\$

ORA_STIG_PROFILE:7\$
SCB_INFRA_APP.*:7\$
SCB_INFRA_SUPP.*:7\$
SCB_STATIC_APP.*:7\$
SCB_SUPP.*:7\$

MGMT_ADMIN_USER_PROFILE:7\$

MGMT_INTERNAL_USER_PROFILE:UNLIMITED\$

OR, any of the selected values below:

Set status to PASS if no data found

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

Extended Evidence:

Statistics:

Query returned 8 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

Evaluation Date 08/04/2024 at 10:09:57 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
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

HIGH (2.15) 101344 Ensure No Users Are Assigned the 'DEFAULT' Profile_(CIS-32)(oracle19:1:1621: **Failed** POHK1CAT.hk.standardchartered.com)

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

Previous Status

Evaluation Date 08/04/2024 at 10:09:57 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
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** POHK1API3)

oracle19:1:1621:POHK1API3 Instance

Previous Status Failed

Evaluation Date 08/04/2024 at 10:09:57 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 DBQUERY:

A.ACCOUNT_STATUS='OPEN' AND A.ORACLE_MAINTAINED = 'N' and CON_ID<>2

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
D42ULADM	4
D42ULADM	3

Extended Evidence:

Statistics:

Query returned 2 rows

(2.16) 101345 Ensure 'GRANT ANY OBJECT PRIVILEGE' Is Revoked from Unauthorized 'GRANTEE' **Passed** HIGH (CIS-58)(oracle19:1:1621:POHK1RCT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:57 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')

Oracle_ATOS - 20240806 page 909

Expected

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:POHK1CAT.hk.standardchartered.com)

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

Previous Status

Evaluation Date 08/04/2024 at 10:09:57 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_USERS WHERE ORACLE_MAINTAINED='Y') 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', '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' HIGH **Passed** (CIS-58)(oracle19:1:1621:POHK1API3)

oracle19:1:1621:POHK1API3 Instance

Previous Status

Evaluation Date 08/04/2024 at 10:09:57 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

(2.17) 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 10:09:57 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:POHK1CAT.hk.standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:57 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

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:POHK1API3)

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

08/04/2024 at 10:09:57 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')

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

(2.18) 101352 Ensure '_trace_files_public'ls Set to 'FALSE'(oracle19:1:1621:POHK1RCT.hk. standardchartered.com)

Passed HIGH

HIGH

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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

(2.18) 101352 Ensure '_trace_files_public'ls Set to 'FALSE'(oracle19:1:1621:POHK1CAT.hk. **Passed** standardchartered.com)

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

Previous Status

Evaluation Date 08/04/2024 at 10:09:56 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:POHK1API3)

Passed HIGH

oracle19:1:1621:POHK1API3 Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 PM (GMT+0530)

Ensure ' trace files public'Is Set to 'FALSE'

Ensure '_trace_files_public'Is Set to 'FALSE'

Scan Parameters:

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

Expected matches regular expression list

DB Column Name: VALUE

FALSE

OR, any of the selected values below:

Set status to PASS if no data found

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.19) 101354 Ensure password complexity as per standards(oracle19:1:1621:POHK1API3) **Passed** HIGH

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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:POHK1CAT.hk. **Passed HIGH** standardchartered.com)

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

Previous Status

Evaluation Date 08/04/2024 at 10:09:56 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)'))

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:POHK1RCT.hk. **Passed** standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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')

HIGH

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:POHK1API3) **HIGH Passed**

oracle19:1:1621:POHK1API3 Instance

Previous Status Passed

08/04/2024 at 10:09:57 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', UNION COLLECT 'IN COLLECT '

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:POHK1CAT.hk. Passed HIGH standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:57 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:POHK1RCT.hk. Passed HIGH standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:57 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

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:POHK1API3)

HIGH

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

08/04/2024 at 10:09:57 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

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

No data found

Extended Evidence:

Statistics:

Instance

Query returned 0 rows

(2.21) 101361 Ensure 'GRANT ANY ROLE' Is Revoked from Unauthorized 'GRANTEE'(CIS-59)

Passed HIGH

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

Previous Status

Evaluation Date 08/04/2024 at 10:09:57 PM (GMT+0530)

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

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

Scan Parameters:

DBQUERY: SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS

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

'HCVPWDMANID_ROOT','HCVPWDMANID')

Expected any of the selected values below:

Set status to PASS if no data found

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

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.21) 101361 Ensure 'GRANT ANY ROLE' Is Revoked from Unauthorized 'GRANTEE'(CIS-59)

Passed HIGH

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

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

Previous Status Passed

08/04/2024 at 10:09:57 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:

DBOUERY: SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS

WHERE PRIVILEGE='CRANT 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 (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','HCVPWĎMANĪD')

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

(2.22) 101367 Ensure 'ALL' Is Revoked on 'Sensitive' Tables(CIS-44)(oracle19:1:1621:POHK1API3) **Failed HIGH**

oracle19:1:1621:POHK1API3 Instance

Previous Status Failed

Evaluation Date 08/04/2024 at 10:09:57 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')

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. Passed **HIGH** standardchartered.com)

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

Previous Status

Evaluation Date 08/04/2024 at 10:09:57 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

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:POHK1RCT.hk. Passed HIGH standardchartered.com)

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

Previous Status

Evaluation Date 08/04/2024 at 10:09:57 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)

No data found

Extended Evidence:

Statistics:

Query returned 0 rows

(2.23) 101337 Status of DB admin audit options_SLM-010(oracle19:1:1621:POHK1API3) **Passed MEDIUM**

oracle19:1:1621:POHK1API3 Instance

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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:POHK1CAT.hk. Passed MEDIUM standardchartered.com)

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

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 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 10:09:56 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:POHK1API3) Passed MEDIUM

Instance oracle19:1:1621:POHK1API3

Previous Status Passed

Evaluation Date 08/04/2024 at 10:09:56 PM (GMT+0530)

Ensure secure encryption standards are configured

Ensure secure encryption standards are configured

Scan Parameters:

DBQUERY: select network_service_banner from v\$session_connect_info where sid=(select sid from v\$mystat where rownum = 1) and

network_service_banner like '%AES256%'

Expected contains regular expression list

DB Column Name: NETWORK_SERVICE_BANNER

AES256

OR, any of the selected values below:

Set status to PASS if no data found

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

NETWORK_SERVICE_BANNER

AES256 Encryption service adapter for Linux: Version 19.0.1.0.0 - Production

Extended Evidence:

Statistics:

Query returned 1 rows

(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 10:09:56 PM (GMT+0530)

Ensure secure encryption standards are configured

Ensure secure encryption standards are configured

Scan Parameters:

DBQUERY: select network_service_banner from v\$session_connect_info where sid=(select sid from v\$mystat where rownum = 1) and

network_service_banner like '%AES256%'

Expected contains regular expression list

DB Column Name: NETWORK_SERVICE_BANNER

AES256

OR, any of the selected values below:

Set status to PASS if no data found

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

NETWORK_SERVICE_BANNER

AES256 Encryption service adapter for Linux: Version 19.0.1.0.0 - Production

Extended Evidence:

Statistics:

Query returned 1 rows

(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 10:09:56 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:

Query returned 1 rows

10.21.199.150 (hklpdss2b002.hk.standardchartered.com)

cpe:/o:redhat:

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

Asset Tags

ALL ASSET GROUPS, Vulnerability Management, Engineering Build, Internal Asset, CLOUD POC, SUBNET-HONG KONG, Oracle PC - AG, Policy Compliance - OS SAT/CCM, ICV-Scan-OS- HK1, Production Support, AG_SelfService, SVLM, Metrics Internal Facing IPs, ESC ATM, Test CCM Scan Key update - UNIX, ZINT-SERVER-INVENTORY-ALL, ALL_STATUS_HONG_KONG_PROD, 2021 Q1 Validation Internal, ICV-OS-Red Hat Enterprise Linux, RBI DB Cindy 2021, SGF total IP scanned of the month, MAP_HK 2/3, temp-all-server2, 2021 Q4 Validation Internal,

Dec_2021_CDC_GDC_NC_Scanned, Jan_2022_CDC_GDC_NC_Scanned, Feb_2022_CDC_GDC_NC_Scanned, 2022 Q1 Validation Internal, Total IP scanned for the month of Feb 2022, Mar_2022_CDC_GDC_NC_Scanned, SGF IP not scanned of the month, Apr_2022_CDC_GDC_NC_Scanned,

May_2022_GDC_CDC_NC_scanned, 2022 Q2 Validation Internal, Jun_2022_GDC_CDC_NC_scanned, Jul_2022_GDC_CDC_NC_scanned, 2022 Q3 Validation Internal, Aug_2022_GDC_CDC_NC_scanned, Sep_2022_GDC_CDC_NC_scanned, OpenSSL-Asia-Prod, Nov_2022_GDC_CDC_NC_scanned, 2022 Q4 Validation Internal, Purge Activity, Jan_2023_CDC_GDC_NC_Scanned, Feb_2023_CDC_GDC_NC_Scanned, Self_Service_AG_UM, 2023 Q1 Validation Internal, Mar_2023_CDC_GDC_NC_Scanned, Agr_2023_CDC_GDC_NC_Scanned, AG-ICV Scans-OS_Web [HK - Begins with 10.21.1], Database_Group, May_2023_CDC_GDC_NC_Scanned, 2023 Q2 Validation Internal, Jun_2023_CDC_GDC_NC_Scanned, Sep_2023_CDC_GDC_NC_Scanned,

Oct_2023_CDC_GDC_NC_Scanned, 2023 Q4 Validation Internal, Nov_2023_CDC_GDC_NC_Scanned, JAN_2024_GDC_EAST, Jan_2024_CDC_GDC_NC_Scanned, FEB_2024_GDC_EAST, Feb_2024_CDC_GDC_NC_Scanned, MAR_2024_GDC_EAST, 2024 Q1 Validation Internal, Mar_2024_CDC_GDC_NC_Scanned, APR_2024_GDC_EAST, April_2024_CDC_GDC_NC_Scanned, MAY_2024_GDC_EAST, May_2024_CDC_GDC_NC_Scanned, 2024 Q2 Validation Internal, JUN_2024_GDC_EAST, Jun_2024_CDC_GDC_NC_Scanned, JUL_2024_GDC_EAST, July_2024_CDC_GDC_NC_Scanned

Oracle 19c

1. Database Controls

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

oracle19:1:1621:POHK1API_DG2 Instance