Tivoli Security Compliance Manager

Version 5.1.1 rel. 2 – July, 2008

Collector and Message Reference Unix Oracle™ Addendum

Table of Contents

Preface

The *IBM Tivoli Security Compliance Manager Collector and Message Reference Oracle" Addendum* describes the following:

- New collectors that gather Oracle™ database configuration information
- New policy template, Unix Oracle Policy, for monitoring the configuration of Oracle™ databases.

Documentation for previously developed collectors that are used in the new policy template can be found in the *IBM Tivoli Security Compliance Manager Collector and Message Reference* publication.

The information in this book will be added to the *IBM Tivoli Security Compliance Manager Collector and Message Reference* publication the next time that publication is updated.

What this book contains

This document contains the following chapters:

- Chapter 1, Required Configuration
- Chapter 2, Policies

  Provides information on the Unix Oracle Policy.
- Chapter 3, Collectors

  Provides general information on the new collectors.

Chapter 1.Required Configuration

Create Database Tables

Some of the queries in the Unix Oracle Policy template refer to tables that you must create before the queries can be executed. You must first edit the **jac_add.sql** file that was bundled with the policy template to verify the contents are correct for your deployment. The comments in the sql file should be thoroughly reviewed. After you have verified the contents, use DB2 to create the tables in your IBM Tivoli Security Compliance Manager 5.1.1 database, JAC, using the DB2 command, db2 tvf jac_add.sql.

Chapter 2.Policy Templates

This chapter documents the following policy template:

- Unix Oracle Policy

Unix Oracle Policy Template

The Unix Oracle Policy template is a policy for checking compliance of Oracle™ databases running on Unix platforms.

Deployment information for the policy template

The IBM Tivoli Security Compliance Manager Unix Oracle Policy template consists of collectors and compliance queries that can be used to determine if a Oracle™ database complies with specific security requirements.

The collector instances associated with this policy are scheduled to run once a day at random times on each client that has this policy assigned.

See the *IBM Tivoli Security Compliance Manager Administration Guide* for details regarding installing and deploying policies.

Policy overview

Parameters used in the policy:

Parameter Name	Description	Type	Default
`Allowed Grantors`	List of grantor types that have permission to add access to the database.	List of strings	'ORACLE-1', 'IBM'
`DBA Grantees`	List of allowed GRANTEEs for the DBA role.	List of strings	'SYS', 'SYSTEM', 'MWADM', 'TIVADMDB', 'OPS$TIVADM'
`DBA Group Members`	List of userids that are allowed in the DBA group.	List of strings	'root', 'oracle', 'ora', 'mwadm', 'tivadm'
`Disallowed User Names`	Disallowed user names.	List of strings	'TRACESVR', 'MDSYS', 'ORDSYS', 'CTXSYS', 'REPADMIN', 'AURORAORBUNAUTHENTICATED', 'SYS', 'SYSTEM', 'DBSNMP', 'SCOTT', 'PO8', 'OUTLN', 'ADAMS', 'JONES', 'BLAKE', 'CLARK', 'HR', 'OE', 'SH', 'TEST', 'DUMMY', 'GUEST', 'DEMO'

Failed Login Limit	Limit of failed login attempts.	Integer	3
Max Collector Data Age	The maximum acceptable age of collector data in days.	Integer	8 [days]
Minimum Idle Time Limit	The minimum setting allowed as the idle time.	Integer	30
Minimum Password Lock Time	The minimum password lock time.	Integer	8
Password Grace Limit	This is the grace period after the password lifetime limit is exceeded.	Integer	7
Password Lifetime Limit	The minimum setting allowed for the password lifetime.	Integer	83
Password Reuse Limit	The maximium password reuse.	Integer	12
PWD Changing Standard Users	List of standard user ids who must change their default password.	List of strings	'SYS' ,'SYSTEM', 'DBSNMP', 'SCOTT', 'DEMO', 'PO8', 'OUTLN'

The queries included in this policy check the following items:

- Recent collector data exists for the collector instances. These queries ensure that the collector instance data has been returned from each of the clients for the specific collector within the past eight days.
- Informational list of clients scanned
- Auditing – Database Level
  - Profile
  - Role
  - User
- Auditing – System Level
  - Required auditing enabled
  - Audit trail logging enabled
  - Session
  - System audit by access
  - System grant by access
- Encryption / DBLINK_ENCRYPT_LOGIN
- File Permissions
  - Default files
  - Listener.ora file
  - Listener.ora file ownership
  - Mirror control files exist
  - SQL.BSQ

- Identify and Authenticate
  - ALTER SESSION privilege
  - ANY privileges
  - AUDIT privileges
  - DBA Role
  - DBA group
  - Disallowed User Accounts
  - Failed Login Attempts
  - Idle time check minimum setting
  - Idle time resource limit
  - LOCK ANY privilege
  - No DBA Role for disallowed user account
  - Password Grace Time
  - Password Lock Time
  - Password complexity function
  - Privileges
  - Restrict Role Privileges
  - Restrict System Privilege
  - SYSDBA Role
- Privileges Permissions
  - Grants to Public
  - Table Grants to Public
- Protecting OSR Resources
  - $ORACLE_HOME directory file access permissions
  - Archive logging enabled
  - Archive log files
  - Control file access permissions
  - Init<sid>.ORA (initialization file)
  - Listener.ora password access
  - Oracle Program File Access
  - Oracle config file permission
  - Redo Log file ownership
  - Rollback segments
  - Table Space data files
  - Temporary File access permission
  - UTLPWDMG.SQL ownership
  - UTLPWDMG.SQL world access

- Protecting User Resources
  - $ORACLE_HOME files
  - Archive log files ownership
  - Config.ora files
  - Control file ownership
  - Database files
  - Init.ora files
  - Temp files
- Synonyms
  - Synonym ownership
- UTL
  - Utl_file package
  - Utl_file_dir
- User Settings
  - Disallowed user names
  - Password life time
  - Password reuse max
  - Password reuse not limited
  - Password reuse time unlimited
  - Standard user accounts password changed

Configuring this policy for your deployment

To configure the policy for your environment, do the following:

- Remove any queries that are not relevant to your deployment.
- Modify any values or parameters if the defaults used do not match the values required for your deployment.

Compliance queries

The following sections contain additional information on all of the compliance queries contained within the policy.

Application / Userid ‘ORA<sid>.xx (xx=name of tier) or ‘oracle’

This compliance query ensures that Oracle is installed on the system.

Table 1.Application / Userid ORA<sid>.xx (xx=name of tier) or oracle Attributes

Priority	Normal
Collector instance name	OraBinaryFilePermsV1

Violation message: Oracle not on system. (Client id: {0}, Hostname: {1}).

SQL query:

```
SELECT       a.cli_id, a.alias as "Hostname"
FROM         jac_sys.clients a
EXCEPT
SELECT       e.cli_id, f.alias as "Hostname"
FROM         jac_data.unx_ora_oracle_file_v1 e
INNER JOIN   jac_sys.clients f
ON (e.cli_id=f.cli_id AND (upper(e.owner) = 'ORACLE' OR upper(e.owner) LIKE 'ORA%'))
```

Auditing – Database Level / Profile

This compliance query ensures that the PROFILE audit option is set correctly.

Table 2.Auditing Database Level / Profile Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Audit option, PROFILE, is not correct. (Client: {0}, Hostname: {2}, SID={1}).

SQL query:

```
SELECT       a.cli_id,a.sid, a.hostname
FROM         jac_data.unx_ora_version_v1 a
LEFT JOIN    jac_data.unx_ora_audit_option_v1 b
ON           (a.cli_id=b.cli_id AND a.sid=b.sid)
WHERE        upper(value(audit_option, '')) != 'PROFILE'
OR    upper(value(user_name, '')) != ''
OR    upper(value(success, '')) != 'BY ACCESS'
OR    upper(value(failure, '')) != 'BY ACCESS'
```

Auditing – Database Level / Role

This compliance query ensures that the ROLE audit option is set correctly.

Table 3.Auditing Database Level / Role Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: No ROLE audit option for all users. (Client: {0}, Hostname: {2}, SID={1}).

SQL query:

```
SELECT       a.cli_id,a.sid, a.hostname
FROM         jac_data.unx_ora_version_v1 a
LEFT JOIN    jac_data.unx_ora_audit_option_v1 b
ON           (a.cli_id=b.cli_id AND a.sid=b.sid)
WHERE        upper(value(audit_option, '')) != 'ROLE'
OR    upper(value(user_name, '')) != ''
OR    upper(value(success, '')) != 'BY ACCESS'
OR    upper(value(failure, '')) != 'BY ACCESS'
```

Auditing – Database Level / User

This compliance query ensures that the USER audit option is set correctly.

Table 4.Auditing Database Level / User Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: USER audit option is not correct. SID={1}

SQL query:

```
SELECT       a.cli_id,a.sid, a.hostname
FROM         jac_data.unx_ora_version_v1 a
LEFT JOIN    jac_data.unx_ora_audit_option_v1 b
ON           (a.cli_id=b.cli_id AND a.sid=b.sid)
WHERE        upper(value(audit_option, '')) != 'USER'
OR    upper(value(user_name, '')) != ''
OR    upper(value(success, '')) != 'BY ACCESS'
OR    upper(value(failure, '')) != 'BY ACCESS'
```

Auditing – System Level / AUDIT_SYS_OPERATIONS Not Enabled

This compliance query ensures the AUDIT_SYS_OPERATIONS parameter is set to true. This is only valid for versions of Oracle after 9.2.

Table 5.Auditing System Level / AUDIT_SYS_OPERATIONS Not Enabled Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: {2} is set to {3}. It must be set to TRUE. (Client: {0}, Hostname: {4}, SID={1})

SQL query:

```
SELECT       a.cli_id, a.sid, a.name, a.value, a.hostname
FROM         jac_data.unx_ora_parameter_v1 a
INNER JOIN   jac_data.unx_ora_version_v1 b
ON           (a.cli_id = b.cli_id AND a.sid = b.sid)
WHERE        upper (a.name) = 'AUDIT_SYS_OPERATIONS'
AND          upper (a.value) <>'TRUE'
AND          ((b.level_1 > 9) OR (b.level_1 = 9 AND b.level_2 >= 2))
```

Auditing – System Level / Audit Trail Logging

This compliance query ensures that the AUDIT_TRAIL parameter is set to OS to enable system wide auditing.

Table 6.Auditing System Level / Audit Trail Logging Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: AUDIT_TRAIL parameter is {3}. It must be OS to enable system wide auditing. (Client: {0}, Hostname: {4}, SID={1})

SQL query:

```
SELECT       cli_id, sid, name, value, hostname
FROM         jac_data.unx_ora_parameter_v1
WHERE        upper (value(name, '')) = 'AUDIT_TRAIL'
AND          upper (value(value, '')) <> 'OS'
```

Auditing – System Level / Create Session

This compliance query ensures that audit option CREATE SESSION is set correctly.

Table 7.Auditing System Level / Create Session Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: No Audit CREATE SESSION for all users. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       a.cli_id, a.sid, a.hostname
FROM         jac_data.unx_ora_version_v1 a
LEFT JOIN    jac_data.unx_ora_audit_option_v1 b
ON           (a.cli_id=b.cli_id AND a.sid=b.sid)
WHERE        upper(value(b.audit_option, '')) != 'CREATE SESSION'
OR    upper(value(b.user_name, '')) != ''
OR    upper(value(b.success, '')) != 'BY ACCESS'
OR    upper(value(b.failure, '')) != 'BY ACCESS'
```

Auditing – System Level / System Audit By Access

This compliance query ensures that the SYSTEM AUDIT access is configured properly.

Table 8.Auditing - System Level / System Audit By Access Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: SYSTEM AUDIT access configuration is not correct. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       a.cli_id, a.sid, a.hostname
FROM         jac_data.unx_ora_version_v1 a
LEFT JOIN    jac_data.unx_ora_audit_option_v1 b
ON           (a.cli_id=b.cli_id AND a.sid=b.sid)
WHERE        upper(value(b.audit_option, '')) != 'SYSTEM AUDIT'
OR    upper(value(b.user_name, '')) != ''
OR    upper(value(b.success, '')) != 'BY ACCESS'
OR    upper(value(b.failure, '')) != 'BY ACCESS'
```

Auditing – System Level / System Grant

This compliance query ensures that all defined Oracle Instances (SIDs) have their SYSTEM GRANT audit option set correctly.

Table 9.Auditing System Level / System Grant Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Audit option SYSTEM GRANT must be BY ACCESS for all users. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       a.cli_id,a.sid, a.hostname
FROM         jac_data.unx_ora_version_v1 a
LEFT JOIN    jac_data.unx_ora_audit_option_v1 b
ON           (a.cli_id=b.cli_id AND a.sid=b.sid)
WHERE        upper(value(b.audit_option, '')) != 'SYSTEM GRANT'
OR    upper(value(b.user_name, '')) != ''
OR    upper(value(b.success, '')) != 'BY ACCESS'
OR    upper(value(b.failure, '')) != 'BY ACCESS'
```

Collector Data / OraBinaryFilePermsV1 Data Exists

Verifies the collector used by this policy has run successfully within the allowed time frame. Default is 8 days.

Table 10.Collector Data / OraBinaryFilePermsV1 Attributes

Priority	Normal
Collector instance name	OraBinaryFilePermsV1

Violation message: Required collector data is missing or is too old: unix.any.OraBinaryFilePermsV1. (Client: {0}, Hostname: {1})

SQL query:

```
SELECT       a.cli_id, a.alias as "Hostname"
FROM         jac_sys.clients a
EXCEPT ALL
SELECT       cli_id, hostname as "Hostname"
FROM         jac_data.unx_ora_oracle_file_v1
WHERE logdate > TIMESTAMP(CHAR(CURRENT DATE - $(Max Collector Data Age) DAYS) || '-00.00.00')
```

Collector Data / OraHomeFilePermsV1 Data Exists

Verifies the collector used by this policy has run successfully within the allowed time frame. Default is 8 days.

Table 11.Collector Data / OraHomeFilePermsV1 Attributes

Priority	Normal
Collector instance name	OraHomeFilePermsV1

Violation message: Required collector data is missing or is too old: unix.any.OraHomeFilePermsV1. (Client: {0}, Hostname: {1})

SQL query:

```
SELECT       a.cli_id, a.alias as "Hostname"
FROM         jac_sys.clients a
EXCEPT ALL
SELECT       cli_id, hostname as "Hostname"
FROM         jac_data.unx_ora_oracle_home_files_v1
WHERE logdate > TIMESTAMP(CHAR(CURRENT DATE - $(Max Collector Data Age) DAYS) || '-00.00.00')
```

Collector Data / OraListenerFilePermsV1 Data Exists

Verifies the collector used by this policy has run successfully within the allowed time frame. Default is 8 days.

Table 12.Collector Data / OraListenerFilePermsV1 Data Exists Attributes

Priority	Normal
Collector instance name	OraListenerFilePermsV1

Violation message: Required collector data is missing or is too old: unix.any.OraListenerFilePermsV1. (Client: {0}, Hostname: {1})

SQL query:

```
SELECT       a.cli_id, a.alias as "Hostname"
FROM         jac_sys.clients a
EXCEPT ALL
SELECT       cli_id, hostname as "Hostname"
FROM         jac_data.unx_ora_listener_v2
WHERE logdate > TIMESTAMP(CHAR(CURRENT DATE - $(Max Collector Data Age) DAYS) || '-00.00.00')
```

Collector Data / OraPwdFunctionsV1 Data Exists

Verifies the collector used by this policy has run successfully within the allowed time frame. Default is 8 days.

Table 13.Collector Data / OraPwdFunctionsV1 Attributes

Priority	Normal
Collector instance name	OraPwdFunctionsV1

Violation message: Required collector data is missing or is too old: unix.any.OraPwdFunctionsV1. (Client: {0}, Hostname: {1})

SQL query:

```
SELECT       a.cli_id, a.alias as "Hostname"
FROM         jac_sys.clients a
EXCEPT ALL
SELECT       cli_id, hostname as "Hostname"
FROM         jac_data.unx_ora_pw_function_v1
WHERE logdate > TIMESTAMP(CHAR(CURRENT DATE - $(Max Collector Data Age) DAYS) || '-00.00.00')
```

Collector Data / OracleQueriesV1 Data Exists

Verifies the collector used by this policy has run successfully within the allowed time frame. Default is 8 days.

Table 14.Collector Data / OracleQueriesV1 Data Exists Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Required collector data is missing or is too old: unix.any.OracleQueriesV1. (Client: {0}, Hostname: {1})

SQL query:

```
SELECT       a.cli_id, a.alias as "Hostname"
FROM         jac_sys.clients a
EXCEPT ALL
SELECT        cli_id, hostname as "Hostname"
FROM         jac_data.unx_ora_config_files_v1
WHERE logdate > TIMESTAMP(CHAR(CURRENT DATE - $(Max Collector Data Age) DAYS) || '-00.00.00')
```

Encryption / DBLINK_ENCRYPT_LOGIN

This compliance query ensures that the DBLINK_ENCRYPT_LOGIN parameter is set to TRUE. This check is only valid for versions of Oracle prior to 9.2.

Table 15.Encryption / DBLINK_ENCRYPT_LOGIN Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: {2} is set to {3}. Must be set to TRUE. (Client: {0}, Hostname: {4}, SID={1})

SQL query:

```
SELECT       a.cli_id, a.sid, b.name, b.value, a.hostname
FROM         jac_data.unx_ora_version_v1 a
INNER JOIN   jac_data.unx_ora_parameter_v1 b
ON           (a.cli_id=b.cli_id AND a.sid=b.sid)
WHERE        upper(value(b.name, ''))='DBLINK_ENCRYPT_LOGIN'
AND          upper(value(b.value, '')) <> 'TRUE'
AND          (a.level_1 < 9 OR  (a.level_1 = 9 AND a.level_2 < 2))
```

File Permissions / Default protection of database files

This compliance query ensures that the file ownership and access permissions of database files are correct.

Table 16.File Permissions / Default protection of database files Attributes

Priority	Normal
Collector instance name	OracleQueriesV1, OraBinaryFilePermsV1

Violation message: Database file,{8}, ownership or permissions are incorrect. OWNER={3}\nGROUP={4}\nOWNER Permissions={5}\nGROUP Permissions={6}\nOther users permissions={7}\n(Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT DISTINCT a.cli_id, a.sid, a.hostname, a.owner, a.group, a.mod_owner,a.mod_group,
             a.mod_other, a.file_name
FROM         jac_data.unx_ora_data_files_v2 a
INNER JOIN   jac_data.unx_ora_oracle_file_v1 b
ON           (a.sid = b.sid AND a.cli_id=b.cli_id)
WHERE        (      a.owner <> b.owner
       OR    a.group <> b.group
       OR    a.mod_owner <> 'rw-'
       OR    a.mod_group <> 'r--'
       OR    a.mod_other <> '---')
UNION
SELECT       a.cli_id, a.sid, a.hostname, a.owner, a.group, a.mod_owner,a.mod_group,
             a.mod_other, a.file_name
FROM         jac_data.unx_ora_temp_files_v1 a
INNER JOIN   jac_data.unx_ora_oracle_file_v1 b
ON           (a.sid = b.sid AND a.cli_id=b.cli_id)
WHERE (      a.owner <> b.owner
      OR     a.group <> b.group
      OR     a.mod_owner <> 'rw-'
```

```
      OR      a.mod_group <> 'r--'
      OR      a.mod_other <> '---')
```

File Permissions / Listener.ora access permissions

This compliance query ensures that listener.ora files have the proper access permission settings.

Table 17.File Permissions / Listener.ora access permissions Attributes

Priority	Normal
Collector instance name	OraListenerFilePermsV1

Violation message: File, {7}, has incorrect file permissions. Owner={2}. Group={3}. Owner Permissions={4}. Group Permissions={5}. Other user permissions={6}\n(Client: {0}, Hostname: {2})

SQL query:

```
SELECT DISTINCT cli_id, hostname, owner, group, mod_owner, mod_group, mod_other, file
FROM         jac_data.unx_ora_listener_v2
WHERE        mod_owner <> 'rw-'
OR    mod_group <> 'r--'
OR    mod_other <> '---'
```

File Permissions / Listener.ora correct file ownership

This compliance query ensures that the listener.ora files have proper user and group ownership.

Table 18.File Permissions / Listener.ora correct file ownership Attributes

Priority	Normal
Collector instance name	OraListenerFilePermsV1, OraBinaryFilePermsV1

Violation message: File {4} is owned by user {2} group {3}. Should be owned by user {5} group {6}.\n(Client: {0}, Hostname: {2})

SQL query:

```
SELECT       a.cli_id, a.hostname, a.owner, a.group, a.file, b.owner, b.group
FROM         jac_data.unx_ora_listener_v2 a
INNER JOIN  jac_data.unx_ora_oracle_file_v1 b ON a.cli_id=b.cli_id
WHERE        (a.owner <> b.owner OR a.group <> b.group)
```

File Permissions / Mirror Control Files

This compliance query ensures that a control files have a mirror.

Table 19.File Permissions / Mirror Control Files Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: File {8} has no mirror. Owner={3}. Group={4}. Owner permissions={5}. Group permissions={6}.Other user permissions={7}.\n(Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT DISTINCT cli_id, sid, hostname, owner, group, mod_owner, mod_group, mod_other, value
FROM        jac_data.unx_ora_ctrl_files_v2
GROUP BY    cli_id, sid, hostname, owner, group, mod_owner, mod_group, mod_other, value
HAVING      count(value) > 2
```

File Permissions / SQL.BSQ and CATALOG.BSQ

This compliance query ensures that the SQL.BSQ and CATALOG.BSQ files have not been modified.

Note: This check depends upon the additional server table JAC_ADD.ORACLE_SQL_BSQ_V1 values being set correctly.

Table 20.File Permissions / SQL.BSA and CATALOG.BSQ Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: File, {9}, has been changed. LEVEL 1= {4}\nLEVEL 2= {5}\nLEVEL 3={6}\nLEVEL 4={7}\nLEVEL 5={8}\n\nSUM1={10}\nSUM2={11}\n(Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT      a.cli_id, a.sid, a.hostname, b.os_name, c.level_1, c.level_2, c.level_3,
            c.level_4, c.level_5, a.file_name, c.sum_1, a.sum_2
FROM        jac_data.unx_ora_bsq_file_v1 a
INNER JOIN  jac_sys.clients b ON a.cli_id = b.cli_id
INNER JOIN  jac_add.oracle_sql_bsq_v1 c ON upper(c.bs) = upper(b.os_name)
INNER JOIN  jac_data.unx_ora_version_v1 d ON (c. level_1 = d.level_1
                  AND   c. level_2 = d.level_2
                  AND   c. level_3 = d.level_3
                  AND   c. level_4 = d.level_4
                  AND   c. level_5 = d.level_5
                  AND   (c.sum_1 <>  integer(a.sum_1 ) OR c.sum_2 <> integer(a.sum_2)))
UNION
SELECT DISTINCT a.cli_id, 'N/A', a.hostname, b.os_name, d.level_1, d.level_2, d.level_3,
            d.level_4, d.level_5, a.file_name, 0, 0
FROM        jac_data.unx_ora_bsq_file_v1 a
INNER JOIN  jac_sys.clients b ON a.cli_id = b.cli_id
INNER JOIN  jac_data.unx_ora_version_v1 d ON d.cli_id=a.cli_id
LEFT JOIN   jac_add.oracle_sql_bsq_v1 e ON (upper(b.os_name) != upper(e.bs)
                  AND   d.level_1 != e.level_1
                  AND   d.level_2 != e.level_2
                  AND   d.level_3 != e.level_3
                  AND   d.level_4 != e.level_4
                  AND   d.level_5 != e.level_5)
```

Identify and Authenticate / ALTER SESSION privilege

This compliance query ensures that ALTER SESSION privilege has not been granted incorrectly.

Note: This query uses additional database server tables JAC_ADD.ALLOWED_GRANTOR_TYPES_V1 and JAC_ADD.ORACLE_USERS_V1.

Table 21.Identify and Authenticate / ALTER SESSION privilege Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: ALTER SESSION privilege invalid. GRANTEE={3}\nPRIVILEGE={4}\n(Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       cli_id, sid, hostname, grantee, privilege
FROM         jac_data.UNX_ORA_SYS_PRIVS_V1
WHERE        (UPPER(privilege) = 'ALTER SESSION')
AND   UPPER(grantee)
NOT IN
      (SELECT       y.username
       FROM         jac_add.oracle_users_v1 y
                     INNER JOIN   jac_add.allowed_grantor_types_v1 z
                     ON    y.usertype=z.usertype)
AND   UPPER(grantee)
NOT IN
      (SELECT       role
       FROM         jac_add.oracle_roles_v1)
```

Identify and Authenticate / ANY Privileges

This compliance query checks that no unauthorized user has been granted excessive permissions.

If the permission has been granted by an authorized grantor, no violation is detected.

Table 22.Identify and Authenticate / ANY Privileges Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Grantee {3} must not have privilege {4}.\n(Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       cli_id, sid, hostname, grantee, privilege
FROM         jac_data.UNX_ORA_SYS_PRIVS_V1
WHERE        (UPPER(privilege) LIKE '%ANY%' OR UPPER(privilege) = 'BECOME USER'
             OR     UPPER(privilege) = 'UNLIMITED TABLESPACE')
AND          UPPER(grantee)
NOT IN
      (SELECT       username
       FROM         jac_add.oracle_users_v1 x
       INNER JOIN   jac_add.allowed_grantor_types_v1 y ON x.usertype = y.usertype)
AND   UPPER(grantee)
NOT IN       (SELECT role FROM jac_add.oracle_roles_v1)
```

Identify and Authenticate / AUDIT privileges

This compliance query checks for correct AUDIT privileges.

Note: This query uses additional database server tables

JAC_ADD.ORACLE_ROLES_V1, JAC_ADD.ORACLE_USERS_V1, JAC_ADD.ALLOWED_GRANTOR_TYPES_V1

Table 23.Identify and Authenticate / AUDIT privileges Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Incorrect audit privilege. GRANTEE={3}\nPRIVILEGE={4}\n(Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       cli_id, sid, hostname, grantee, privilege
FROM         jac_data.UNX_ORA_SYS_PRIVS_V1
WHERE        (UPPER(privilege) LIKE 'AUDIT%')
AND          UPPER(grantee)
NOT IN
      (SELECT       username
       FROM         jac_add.oracle_users_v1 x
        INNER JOIN  jac_add.allowed_grantor_types_v1 y
        ON          x.usertype=y.usertype)
AND          UPPER(grantee)
NOT IN
             (SELECT       UPPER(role)
              FROM         jac_add.oracle_roles_v1)
```

Identify and Authenticate / DBA Role

This compliance query ensures that the DBA role is not granted inappropriately.

Table 24.Identify and Authenticate / DBA Role Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Unauthorized user with DBA-Role. User={3}. Role={4}. S\n(Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       cli_id, sid, hostname, grantee, granted_role
FROM         jac_data.unx_ora_role_privs_v1
WHERE        granted_role = 'DBA'
AND          upper(grantee)
NOT IN       ($(DBA Grantees))
```

Identify and Authenticate / DBA Group

This compliance query ensures that oracle files group ownership is limited to acceptable users.

Table 25.Identify and Authenticate / DBA Group Attributes

Priority	Normal
Collector instance name	OraBinaryFilePermsV1

Violation message: Unauthorized user, {4} is a member of group {3} which has group ownership of file {5}. \n(Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       cli_id, sid, hostname, group, owner, value
FROM         jac_data.unx_ora_oracle_file_v1
WHERE        lower(owner) NOT IN ($(DBA Group Members))
```

Identify and Authenticate / Disallowed User Accounts

This compliance query ensures that sample and other disallowed user names are not assigned privileges.

Table 26.Identify and Authenticate / Disallowed User Accounts Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Disallowed user, {3}, has role {4}. \n(Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       a.cli_id, a.hostname, a.sid, a.username, b.granted_role
FROM         jac_data.unx_ora_user_profile_v1 a
LEFT OUTER JOIN     jac_data.unx_ora_role_privs_v1 b
ON           a.username = b.grantee AND a.cli_id=b.cli_id
WHERE        upper(a.username) IN ($(Disallowed User Names))
```

Identify and Authenticate / Failed Login Attempts

This compliance query ensures that the failed login limit is set for all users.

Table 27.Identify and Authenticate / Failed Login Attempts Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: User {3} has {5} set to {6}. Profile={4}.\n(Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       a.cli_id, a.sid, a.hostname, b.username, a.profile, a.resource_name, a.limit
FROM         jac_data.unx_ora_profile_settings_v1 a
INNER JOIN   jac_data.unx_ora_user_profile_v1 b
ON           a.cli_id=b.cli_id AND a.sid=b.sid AND a.profile=b.profile
WHERE        resource_name='FAILED_LOGIN_ATTEMPTS'
AND          (((substr(a.limit,1,1) between '0' AND '9')
```

```
       AND integer(a.limit) > $(Failed Login Limit))
       OR (substr(a.limit,1,1) NOT between '0' AND '9') OR ( a.limit IS NULL ))
```

Identify and Authenticate / Idle Time Check Minimum Setting

This compliance query ensures that the IDLE_TIME is set.

Table 28.Identify and Authenticate / Idle Time Check Minimum Setting Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: User, {3} has {5} set to {6}. Must be less than or equal to {7}. PROFILE={4}.\n(Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       a.cli_id, a.sid, a.hostname, b.username, a.profile, resource_name, a.limit, $
              (Minimum Idle Time Limit)
FROM         jac_data.unx_ora_profile_settings_v1 a
INNER JOIN   jac_data.unx_ora_user_profile_v1 b
ON           a.cli_id=b.cli_id AND a.sid=b.sid AND a.profile=b.profile
WHERE        resource_name = 'IDLE_TIME'
AND ((substr(limit,1,1) between '0' AND '9'  AND integer(limit)>$(Minimum Idle Time Limit))
       OR    (substr(limit,1,1) NOT between '0' AND '9')
       OR    (limit IS NULL))
```

Identify and Authenticate / LOCK ANY privilege

This compliance query ensures that LOCK permissions have not been granted incorrectly.

Table 29.Identify and Authenticate / LOCK ANY privilege Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: LOCK privilege incorrect. GRANTEE={3}\nPRIVILEGE={4}.\n(Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       cli_id, hostname, sid, grantee, privilege
FROM         jac_data.UNX_ORA_SYS_PRIVS_V1
WHERE        (UPPER(privilege) LIKE 'LOCK%')
AND          UPPER(grantee)
NOT IN
      (SELECT DISTINCT username
       FROM         jac_add.oracle_users_v1 x
       WHERE        x.usertype IN ($(Allowed Grantors)))
AND   UPPER(grantee)
NOT IN
      (SELECT       role
       FROM         jac_add.oracle_roles_v1)
```

Identify and Authenticate / No DBA Role For Disallowed User Account

This compliance query ensures that disallowed user names are not assigned the DBA role.

Table 30.Identify and Authenticate / No DBA Role for Disallowed User Account Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: User {3} must not have role {4}. \n(Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       cli_id, sid, hostname, grantee, granted_role
FROM         jac_data.unx_ora_role_privs_v1 a
WHERE        upper(a.grantee) IN ($(Disallowed User Names))
AND          upper (granted_role)  = 'DBA'
```

Identify and Authenticate / Password Grace Time

This compliance query ensures that the PASSWORD_GRACE_TIME setting is correct.

Table 31.Identify and Authenticate / Password Grace Time Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: ORA PROFILE SETTINGS PASSWORD GRACE TIME NOT STANDARD.\nUSERNAME={2}\nPROFILE={3}\nRESOURCE NAME={4}\nLIMIT={5}.\n(Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       a.cli_id, a.sid, a.hostname, username, a.profile, resource_name, limit, $
              (Password Grace Limit)
FROM         jac_data.unx_ora_profile_settings_v1 a
INNER JOIN   jac_data.unx_ora_user_profile_v1 b
ON           a.cli_id=b.cli_id
AND          a.sid=b.sid
AND          a.profile=b.profile
WHERE        resource_name='PASSWORD_GRACE_TIME'
AND   ((substr(limit,1,1) between '0' AND '9' AND  integer(limit)>$(Password Grace Limit)
       OR    (substr(limit,1,1) NOT between '0' AND '9') OR (limit IS NULL)))
```

Identify and Authenticate / Password Lock Time

This compliance query ensures that the minimum password lock time setting is valid.

Table 32.Identify and Authenticate / Password Lock TimeAttributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: User {2} has {4} set to {5}. Should be at least {6}. Profile={3}.\n(Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       a.cli_id, a.sid, a.hostname, username, a.profile, resource_name, limit,
             $(Minimum Password Lock Time)
FROM         jac_data.unx_ora_profile_settings_v1 a
INNER JOIN   jac_data.unx_ora_user_profile_v1 b
ON           a.cli_id=b.cli_id AND a.profile=b.profile
WHERE        resource_name='PASSWORD_LOCK_TIME'
AND (((substr(limit,1,1) between '0' AND '9') AND integer(limit)>$(Minimum Password Lock
Time))
              OR    substr(limit,1,1) NOT between '0' AND '9'
              OR    limit IS NULL)
```

Identify and Authenticate / Password complexity function

The password complexity function must be enabled to enforce the following attributes:

A valid password will have a minimum length of eight (8) characters.

A valid password will contain at least one alpha and one numeric character.

Table 33.Identify and Authenticate / Password complexity function Attributes

Priority	Normal
Collector instance name	OracleQueriesV1, OraPwdFunctionsV1

Violation message: Password complexity invalid for user {3}: profile "{4}" "{5}" "{6}" "(7)". (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT        u.cli_id, u.sid, u.hostname, u.username, u.profile, p.limit, p.hc_id,
             p.hc_description
FROM         jac_data.unx_ora_user_profile_v1 u
INNER JOIN   jac_data.unx_ora_pw_function_v1 p
ON           (u.cli_id = p.cli_id AND u.sid = p.sid AND u.profile=p.profile)
WHERE        (p.limit is NULL OR p.hc_id is NOT  NULL)
```

Identify and Authenticate / Privileges

It is recommended that privileges be assigned to users indirectly. Privileges should be granted to roles only.

Table 34.Identify and Authenticate / Privileges Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: User {3} has privilege granted directly.\n(Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       cli_id, sid, hostname, grantee
FROM         jac_data.unx_ora_tab_privs_v1
WHERE        grantee
NOT IN
      (SELECT       role
       FROM         jac_data.unx_ora_roles_v1 )
AND          upper( grantee )
NOT IN       ($(Allowed Grantors))
```

Identify and Authenticate / Resource Limit

This compliance query ensures that the RESOURCE_LIMIT configuration parameter is not set to false.

Table 35. Identify and Authenticate / Resource Limit Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Configuration parameter {3} is incorrectly set to {4}. \n(Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       cli_id, hostname, sid,name, value
FROM         jac_data.unx_ora_parameter_v1
WHERE        upper(name) = 'RESOURCE_LIMIT'
AND          (upper(value) IN ('FALSE','NONE') OR value IS NULL)
```

Identify and Authenticate / Restrict Role Privileges

Roles containing %ANY%,%ADMINISTER%,%ALTER%,%USER%,%DROP%,or %AUDIT%

must be restricted to administrative users.

Table 36.Identify and Authenticate / Restrict Role Privileges Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: user "{3}" with role "{4}" with privs not allowed. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       a.cli_id, a.sid, a.hostname, a.grantee, a.granted_role
FROM         jac_data.unx_ora_role_privs_v1 a
WHERE        a.granted_role
IN
      (SELECT DISTINCT grantee
       FROM         jac_data.UNX_ORA_SYS_PRIVS_V1
       WHERE        grantee
       IN
             (SELECT       role
              FROM         jac_data.UNX_ORA_ROLES_V1 )
      AND    (privilege LIKE '%ANY%'
             OR     privilege LIKE '%ADMINISTER%'
             OR     privilege LIKE '%ALTER%'
             OR     privilege LIKE '%USER%'
             OR     privilege LIKE '%DROP%'
             OR     privilege LIKE '%AUDIT%'))
AND          a.grantee
NOT IN       ($(Allowed Grantors))
```

Identify and Authenticate / Restrict System Privileges

System privileges, FORCE TRANSACTION, MANAGE TABLESPACE, RESTRICTED SESSION, and GLOBAL QUERY REWRITE,

must be restricted to system administrators.

Table 37.Identify and Authenticate / Restrict System Privileges Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: grantee "{3}" has privilege "{4}". (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       cli_id, sid, hostname, grantee, privilege
FROM         jac_data.unx_ora_sys_privs_v1
WHERE        privilege
IN    ('FORCE TRANSACTION','MANAGE TABLESPACE','RESTRICTED SESSION','GLOBAL QUERY REWRITE')
AND          grantee NOT IN ($(Allowed Grantors))
```

Identify and Authenticate / SYSDBA Role

This compliance query checks that no users other than SYS and SYSTEM gave access to pwfile

Table 38.Identify and Authenticate / SYSDBA Role Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: User {3} can connect as sysdba/sysoper. SYSDBA={4}. SYSOPER={5}. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT      cli_id, sid, hostname, username, sysdba, sysoper
FROM        jac_data.unx_ora_pwfile_users_v1
WHERE       upper(username) NOT IN  ($(DBA Grantees))
```

Privileges Permissions / Grants to Public

This compliance query ensures that system roles and privileges are not granted to PUBLIC.

Table 39.Privileges Permissions / Grants to Public Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: {3}, {5}, granted to PUBLIC. GRANTEE={4}. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT      cli_id, sid, hostname, 'ROLE' , GRANTEE, GRANTED_ROLE
FROM        jac_data.UNX_ORA_ROLE_PRIVS_V1
WHERE       GRANTEE = 'PUBLIC'
UNION
SELECT      cli_id, sid, hostname, 'SYSTEM' , GRANTEE, PRIVILEGE
FROM        jac_data.UNX_ORA_SYS_PRIVS_V1
WHERE       GRANTEE = 'PUBLIC'
```

Privileges Permissions / Table Grants to Public

This compliance query ensures that public table access is not incorrectly granted.

Table 40.Privileges Permissions / Table Grants to Public Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Public granted access to tables. Grantee={3}. Grantor={4}. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT      cli_id, sid, hostname, GRANTEE, grantor
FROM        jac_data.UNX_ORA_TAB_PRIVS_V1
WHERE       upper(GRANTEE) = 'PUBLIC'
AND         grantor
```

```
NOT IN
      (SELECT       username
       FROM         jac_add.oracle_users_v1 a
       INNER JOIN   jac_add.allowed_grantor_types_v1 b ON a.usertype=b.usertype)
```

Protecting OSR Resources / $ORACLE_HOME directory file access permissions

This compliance query ensures that files in the $ORACLE_HOME directory have proper world access permissions.

Table 41.Protecting OSR Resources / $ORACLE_HOME directory file access permissions Attributes

Priority	Normal
Collector instance name	OraHomeFilePermsV1

Violation message: File {8} has incorrect world access permissions {7}. Owner={3}. Group={4}. Owner permissions={5}. Group permissions={6}.\n(Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       cli_id, sid, hostname, owner, group, mod_owner, mod_group, mod_other, value
FROM         jac_data.unx_ora_oracle_home_files_v1
WHERE        mod_other NOT LIKE '_-_'
```

Protecting OSR Resources / Archive Logging Enabled

This compliance query ensures that archive log mode is enabled.

Table 42.Protecting OSR Resources / Archive Logging Enabled Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Archive log mode is not enabled. Database logmode={2}\nAutomatic archival={3}.\n(Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       cli_id, sid, hostname, database_logmode, automatic_archival
FROM         jac_data.unx_ora_archive_v1
WHERE        upper (DATABASE_LOGMODE) = 'NO ARCHIVE MODE'
OR           upper (AUTOMATIC_ARCHIVAL) = 'DISABLED'
```

Protecting OSR Resources / Archive log files

This compliance query ensures that Oracle archive log files do not have world access permission.

Table 43.Protecting OSR Resources / Archive log files Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Archive log file,{8}, has incorrect access permission. OWNER={3}\nGROUP={4}\nOWNER Permissions={5}\nGROUP Permissions={6}\nOTHER Users Permissions={7}.\n(Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT      cli_id, sid, hostname, owner, group, mod_owner,mod_group, mod_other, value
FROM        jac_data.unx_ora_archive_files_v1
WHERE       mod_other NOT LIKE '--_'
```

Protecting OSR Resources / Control file access permission

This compliance query ensures that Oracle control files do not have world access.

Table 44.Protecting OSR Resources / Control file access permission Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Oracle database control file has incorrect file access permissions.OWNER={3}, GROUP={4}, MOD_OWNER={5}, MOD_GROUP={6}, MOD_OTHER={7}, VALUE={8}, (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT DISTINCT cli_id, sid, hostname, owner, group, mod_owner, mod_group, mod_other, value
FROM        jac_data.unx_ora_ctrl_files_v2
WHERE       mod_other NOT LIKE '--_'
```

Protecting OSR Resources / Init <database sid>.ORA(initialization file)

This compliance query ensures that the init files do not have world access.

Table 45.Protecting OSR Resources / Init<database.sid>.ORA(initialization file) Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: File {8} has incorrect world access permissions={7}. Onwer={3}. Group={4}. Owner permissions={5}. Group permissions={6}. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT      cli_id, sid, hostname, owner, group, mod_owner, mod_group, mod_other, file_name
FROM        jac_data.unx_ora_sid_files_v2
WHERE       mod_other NOT LIKE '--_'
```

Protecting OSR Resources / Listener.ora password access

This compliance query ensures that the password keyword is not included in the listener.ora files.

Table 46.Protecting OSR Resources / Listener.ora password access Attributes

Priority	Normal
Collector instance name	OraListenerFilePermsV1

Violation message: File, {2}, may contain password information. CONTENT={3},COMMENT={4}.\n(Client: {0}, Hostname: {1})

SQL query:

```
SELECT      cli_id, hostname, file, content, comment
FROM        jac_data.unx_ora_listener_v2
WHERE       content IS NULL
OR          (content IS NOT NULL AND upper(comment) = 'TRUE')
```

Protecting OSR Resources / Oracle Program File Access

This compliance query ensures that Oracle Program files have the correct access permissions for the file owner and group.

Table 47.Protecting OSR Resources / Oracle Program File Access Attributes

Priority	Normal
Collector instance name	OraBinaryFilePermsV1

Violation message: File {8} has incorrect access permissions. Owner={3}. Group={4}. Owner permissions={5}. Group permissions={6}. Other user permissions={7}. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT      cli_id, sid, hostname, owner, group, mod_owner, mod_group, mod_other, value
FROM        jac_data.unx_ora_oracle_file_v1
WHERE       mod_group NOT LIKE '__s'
OR          mod_owner NOT LIKE '__s'
```

Protecting OSR Resources / Oracle config file permission

This compliance query ensures that the Oracle config files have valid world access permission.

Table 48.Protecting OSR Resources / Oracle config file permission Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Config file {8} has invalid access permissions. Owner={3}. Group={4}. Owner permissions={5}. Group permissions={6}. Other user permissions={7}. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT      cli_id, sid, hostname, owner, group, mod_owner, mod_group, mod_other, value
FROM        jac_data.unx_ora_config_files_v1
WHERE       mod_other NOT LIKE '--_'
```

Protecting OSR Resources / Redo Log file ownership

This compliance query checks the redo log files for proper file ownership.

Table 49.Protecting OSR Resources/ Redo Log file ownership Attributes

Priority	Normal
Collector instance name	OracleQueriesV1, OraBinaryFilePermsV1

Violation message: Redo log file, is owned by user {3} and group {4}. It should be owned by {8} and group {9}. User permissions={5}. Group permissions={6}. Other user permissions={7}. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       a.cli_id, a.sid, a.hostname, a.owner, a.group, a.mod_owner, a.mod_group,
              a.mod_other, a.member, b.owner as REQ_OWN, b.group as REQ_GROUP
FROM         jac_data.unx_ora_redo_files_v1 a
INNER JOIN   jac_data.unx_ora_oracle_file_v1 b
ON           (a.sid = b.sid AND a.cli_id=b.cli_id)
WHERE        (a.owner <> b.owner OR a.group <> b.group)
```

Protecting OSR Resources / Redo log files access permissions

This compliance query ensures that the redo log files are not world readable or world writable.

Table 50.Protecting OSR Resources / Redo log files access permissions Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Redo log file, has incorrect access permissions. Owner={3}. Group={4}. Owner permissions={5}. Group permissions={6}. Other users permissions={7}. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       cli_id, sid, hostname, owner, group, mod_owner, mod_group, mod_other, member
FROM         jac_data.unx_ora_redo_files_v1
WHERE        mod_other NOT LIKE '--_'
```

Protecting OSR Resources / Rollback Segments

This compliance query ensuers that the Oracle rollback files have correct ownership and access permissions.

Table 51.Protecting OSR Resources / Rollback Segments Attributes

Priority	Normal
Collector instance name	OracleQueriesV1, OraBinaryFilePermsV1

Violation message: Rollback file, {8} has incorrect ownership or access permission. OWNER={3}, GROUP={4}, Owner Permissions={5}, GROUP Permissions={6}, OTHER Users Permissions={7}, (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       a.cli_id, a.sid, a.hostname, a.owner, a.group, a.mod_owner, a.mod_group,
              a.mod_other, a.file_name
FROM         jac_data.unx_ora_rollback_files_v1 a
INNER JOIN   jac_data.unx_ora_oracle_file_v1 b ON (a.sid = b.sid AND a.cli_id = b.cli_id)
WHERE        (a.owner <> b.owner OR a.group <> b.group OR a.mod_other NOT LIKE '--_')
```

Protecting OSR Resources / Table Space Data Files

This compliance query ensures that table space data files do not have world access.

Table 52.Protecting OSR Resources / Table Space Data Files Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Table space data file,{8}, has world access permission={7}. Owner={3}, Group={4}, Owner Permissions={5}, Group Permissions={6}. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       cli_id, sid, hostname, owner, group, mod_owner,mod_group, mod_other, file_name
FROM         jac_data.unx_ora_data_files_v2
WHERE        mod_other NOT LIKE '--_'
```

Protecting OSR Resources / Temporary File Access Permission

This compliance query ensures that the temporary file access permissions are acceptable.

Table 53.Protecting OSR Resources / Temporary File Access Permission Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Temporary file {8} has incorrect access permissions. Owner={3}. Group={4}. Owner permissions={5}. Group Permissions={6}. Other User Permissions={7}. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       cli_id, sid, hostname, owner, group, mod_owner, mod_group, mod_other, file_name
FROM         jac_data.unx_ora_temp_files_v1
```

```
WHERE       mod_other NOT LIKE '--_'
```

Protecting OSR Resources / UTLPWDMG.SQL ownership

This compliance query ensures that Oracle file, utlpwdmg.sql, has the same owner and group owner as the files in the Oracle installation directory.

Table 54.Protecting OSR Resources / UTLPWDMG.SQL ownership Attributes

Priority	Normal
Collector instance name	OracleQueriesV1, OraBinaryFilePermsV1

Violation message: Oracle file, UTLPWDMG.SQL, file owner or group is incorrect. OWNER={2}, GROUP={3}, Owner Permissions={4},Group Permissions={5},Other Users Permissions={6},File={7}. (Client: {0}, Hostname:{1})

SQL query:

```
SELECT      a.cli_id, a.hostname, a.owner, a.group, a.mod_owner,a.mod_group, a.mod_other,
             a.value
FROM        jac_data.unx_ora_utlpwd_file_v1 a
INNER JOIN  jac_data.unx_ora_oracle_file_v1 b
ON          a.sid=b.sid AND a.cli_id=b.cli_id
WHERE       (a.owner <> b.owner OR a.group <> b.group)
```

Protecting OSR Resources / UTLPWDMG.SQL world access

This compliance query ensures that the Oracle file, utlpwdmg.sql, has the correct file access. Only the owner and group members should have access to this file..

Table 55.Protecting OSR Resources / UTLPWDMG.SQL world access Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Oracle utlpwdmg.sql file has incorrect access permissions. OWNER={2}, GROUP={3}, OWNER PERMISSIONS={4}, GROUP PERMISSIONS={5}, OTHER USER PERMISSIONS={6}, FILE NAME={7}. (Client: {0}, Hostname: {1})

SQL query:

```
SELECT      cli_id, hostname, owner, group, mod_owner,mod_group, mod_other, value
FROM        jac_data.unx_ora_utlpwd_file_v1
WHERE       mod_other NOT LIKE '--_'
```

Protecting User Resources / $ORACLE_HOME files

This compliance query ensures that files in the $ORACLE_HOME directory have proper user and group ownership.

Table 56.Protecting User Resources / $ORACLE_HOME files Attributes

Priority	Normal
Collector instance name	OraBinaryFilePermsV1, OraHomeFilePermsV1

Violation message: File {8} is owned by user {3} group {4}. Should be owned by user {9} group {10}. Owner permissions={5}\nGroup permissions={6}\nOther user permissions={7}. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       a.cli_id, a.sid, a.hostname, a.owner, a.group, a.mod_owner, a.mod_group,
              a.mod_other, a.value, b.owner, b.group
FROM         jac_data.unx_ora_oracle_home_files_v1 a
INNER JOIN   jac_data.unx_ora_oracle_file_v1 b ON (a.sid = b.sid AND a.cli_id=b.cli_id)
WHERE        (a.owner <> b.owner OR a.group <> b.group)
```

Protecting User Resources / Archive Log files ownership

This compliance query ensures that the archive log files have the correct owner.

Table 57.Protecting User Resources / Archive Log files ownership Attributes

Priority	Normal
Collector instance name	OracleQueriesV1, OraBinaryFilePermsV1

Violation message: Archive file {8} is owned by user {3} group {4}. It should be owned by user {9} group {10}. Owner permissions={5}.Group permissions={6}.Other user permissions={7}. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       a.cli_id, a.sid, a.hostname, a.owner, a.group, a.mod_owner, a.mod_group,
              a.mod_other, a.value, b.owner, b.group
FROM         jac_data.unx_ora_archive_files_v1 a
INNER JOIN   jac_data.unx_ora_oracle_file_v1 b ON (a.sid = b.sid AND a.cli_id=b.cli_id)
WHERE        (a.owner <> b.owner OR a.group <> b.group)
```

Protecting User Resources / Config.ora files

This compliance query ensures that instance configuration files have the correct file ownership.

Table 58.Protecting User Resources / Config.ora files Attributes

Priority	Normal
Collector instance name	OracleQueriesV1, OraBinaryFilePermsV1

Violation message: Config file, {8} has incorrect user ({3}) or group ({4}) ownership. User should be {9}. Group should be {10}. Owner permissions={5}. Group permissions={6}. Other user permissions={7}. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       a.cli_id, a.sid, a.hostname, a.owner, a.group, a.mod_owner, a.mod_group,
              a.mod_other, a.value, b.owner, b.group
FROM         jac_data.unx_ora_config_files_v1 a
INNER JOIN   jac_data.unx_ora_oracle_file_v1 b ON (a.sid = b.sid AND a.cli_id = b.cli_id)
WHERE        (a.owner <> b.owner OR a.group <> b.group)
```

Protecting User Resources / Control file ownership

This compliance query checks the file ownership of list control files.

Table 59.Protecting User Resources / Control file ownership Attributes

Priority	Normal
Collector instance name	OracleQueriesV1, OraBinaryFilePermsV1

Violation message: File {8} has owner {3}, group {4}. Should be owned by {9} group {10}.Owner permissiosn={5}\nGroup permissions={6}\nOther user permissions={7}. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       a.cli_id, a.sid, a.hostname, a.owner, a.group, a.mod_owner, a.mod_group,
              a.mod_other, a.value, b.owner, b.group
FROM         jac_data.unx_ora_ctrl_files_v2 a
INNER JOIN   jac_data.unx_ora_oracle_file_v1 b ON (a.sid = b.sid AND a.cli_id=b.cli_id)
WHERE        (a.owner <> b.owner OR a.group <> b.group)
```

Protecting User Resources / Database files

This compliance query ensures that the database files have the correct owner.

Table 60.Protecting User Resources / Database files Attributes

Priority	Normal
Collector instance name	OracleQueriesV1, OraBinaryFilePermsV1

Violation message: File {8} is owned by user {3} and group {4}. It should be owned by user {9} and group {10}. Owner permissions={5}.Group permissions={6}.Other users permissions={7}.(Client: {0}, Hostname: {2},SID={1})

SQL query:

```
SELECT       a.cli_id, a.sid, a.hostname, a.owner, a.group, a.mod_owner, a.mod_group,
              a.mod_other, a.file_name, b.owner, b.group
FROM         jac_data.unx_ora_data_files_v2 a
INNER JOIN   jac_data.unx_ora_oracle_file_v1 b ON (a.sid = b.sid AND a.cli_id=b.cli_id)
WHERE        (a.owner <> b.owner OR a.group <> b.group)
```

Protecting User Resources / Init.ora files

This compliance query ensures that the SID files have the proper ownership.

Table 61.Protecting User Resources / Init.ora files Attributes

Priority	Normal
Collector instance name	OracleQueriesV1, OraBinaryFilePermsV1

Violation message: File {8} is owned by user {3} and group {4}. It should be owned by user {9} and group {10}. Owner permissions={5}.Group permissions={6}.Other users permissions={7}.(Client: {0}, Hostname: {2},SID={1})

SQL query:

```
SELECT       a.cli_id, a.sid, a.hostname, a.owner, a.group, a.mod_owner, a.mod_group,
              a.mod_other, a.file_name, b.owner, b.group
FROM         jac_data.unx_ora_sid_files_v2 a
INNER JOIN   jac_data.unx_ora_oracle_file_v1 b ON (a.sid = b.sid AND a.cli_id=b.cli_id)
```

```
WHERE        (a.owner <> b.owner OR a.group <> b.group)
```

Protecting User Resources / Temp files

This compilance query ensures that temp files have correct ownership and access permissions.

Table 62.Protecting User Resources / Temp files Attributes

Priority	Normal
Collector instance name	OracleQueriesV1, OraBinaryFilePermsV1

Violation message: Temp file, {8}, has incorrect ownership or access permissions. OWNER={3}, GROUP={4}, OWNER Permissions={5}, GROUP Permissions={6}, OTHER Users Permissions={7}. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       a.cli_id, a.sid, a.hostname, a.owner, a.group, a.mod_owner, a.mod_group,
              a.mod_other, a.file_name
FROM         jac_data.unx_ora_temp_files_v1 a
INNER JOIN   jac_data.unx_ora_oracle_file_v1 b ON (a.sid = b.sid AND a.cli_id = b.cli_id)
WHERE        (a.owner <> b.owner OR a.group <> b.group)
```

Roles, Views, and Access Control / Host Command

This compliance query ensures that the HOST command is disabled.

Table 63.Roles, Views, and Access Control / Host Command Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Host command not disabled. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       cli_id, sid, hostname
FROM         jac_data.unx_ora_version_v1
WHERE        (cli_id, sid, hostname)
NOT IN
      (SELECT       cli_id, sid, hostname
       FROM         jac_data.UNX_ORA_CLP_PRODUCT_PROFILE_V1
       WHERE        upper(product) = 'SQL*PLUS'
       AND          userid = '%'
       AND          char_value = 'DISABLED'
       AND          attribute = 'HOST' )
```

Roles, Views, and Access Control / Network listeners for SQL*NET clients

Network listeners for SQL*NET should be password protected.

*Table 64.Roles, Views, and Access Control / Network listeners for SQL*NET clients Attributes*

Priority	Normal
Collector instance name	OraListenerFilePermsV1

Violation message: file listener "{2}" password is missing.(Client: {0}, Hostname: {1})

SQL query:

```
SELECT       cli_id, hostname, file, content, comment
FROM         jac_data.unx_ora_listener_v2
WHERE        content is NULL
OR           (content is NOT NULL AND upper(comment) = 'TRUE')
```

Roles, Views, and Access Control / Oracle default role

This compliance query ensures that roles are assigned appropriately.

Table 65.Roles, Views, and Access Control / Oracle default role Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: User,{3}, has been granted role, {4}. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       cli_id, sid, hostname, grantee, granted_role
FROM         jac_data.UNX_ORA_ROLE_PRIVS_V1
WHERE        UPPER(grantee)
NOT IN
      (SELECT       username
       FROM         jac_add.oracle_users_v1
       WHERE        usertype
       IN           ($(Allowed Grantors))
       AND          UPPER(grantee)
       NOT IN
             (SELECT       role
              FROM         jac_add.oracle_roles_v1)
       AND          granted_role
       IN
             (SELECT       role
              FROM         jac_add.oracle_roles_v1))
```

Roles, Views, and Access Control / Set Role Privilege

This compliance query ensures that the SET ROLE and SET attributes are disabled for the SQL*PLUS product.

Table 66.Roles, Views, and Access Control / Set Role Privilege Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: SET ROLE or SET command not disabled. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       cli_id, sid, hostname
FROM         jac_data.unx_ora_version_v1
WHERE        (cli_id, sid, hostname)
NOT IN
      (SELECT       cli_id, sid, hostname
       FROM         jac_data.UNX_ORA_CLP_PRODUCT_PROFILE_V1
       WHERE        upper(product) = 'SQL*PLUS'
       AND          userid = '%'
       AND          char_value = 'DISABLED'
       AND          (attribute = 'SET ROLE'  OR attribute = 'SET'))
```

Snapshot Info / Clients

Lists the clients contained in the snapshot.

Table 67.Snapshot Info / Clients Attributes

Priority	Informational
Collector instance name	None

Violation message: Client Snapshot Successful: (Client: {0}, Hostname: {1})

SQL query:

```
SELECT       cli_id,alias
FROM         jac_sys.clients
```

Synonyms / Synonym ownership

This compliance query ensures that synonym tables have acceptable ownership.

Table 68.Synonyms / Synonym ownership Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Incorrect ownership of synonym, {3}. Table owner={4}. Table name={5}. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       cli_id, sid, hostname, SYNONYM_NAME, TABLE_OWNER, TABLE_NAME
FROM         jac_data.UNX_ORA_SYNONYM_V1
```

```
WHERE               UPPER(table_owner)
NOT IN
             (SELECT       UPPER(username)
              FROM         jac_add.oracle_users_v1 x
              WHERE        x.usertype IN ($(Allowed Grantors)))
```

UTL / Utl_file package

This compliance query ensures that the UTL_FILE table does not have EXECUTE privilege granted to PUBLIC.

Table 69.UTL / Utl_file package Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: {3} is public. Privilege={4}.\n(Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       cli_id, sid, hostname, table_name, privilege
FROM         jac_data.UNX_ORA_UTL_PRIVS_V1
WHERE        table_name = 'UTL_FILE'
AND          privilege = 'EXECUTE'
AND          grantee= 'PUBLIC'
```

UTL / Utl_file_dir

This compliance query ensures that the Oracle UTL_FILE_DIR parameter is not set to *.

Table 70.UTL / Utl_file_dirAttributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: UTL_FILE_DIR parameter incorrect. NAME={3}\nVALUE={4}. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       cli_id, sid, hostname, name, value
FROM         jac_data.unx_ora_parameter_v1
WHERE        upper (name) = 'UTL_FILE_DIR'
AND          value = '*'
```

User Settings / Disallowed User Names

This compliance query ensures that disallowed usernames are not active.

Table 71.User Settings / Disallowed User Names Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Disallowed user name, {3}, is active. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT      cli_id, sid, hostname, username
FROM        jac_data.unx_ora_user_profile_v1
WHERE       username IN ($(Disallowed User Names))
```

User Settings / Password Life Time

This compliance query ensures that the PASSWORD_LIFE_TIME setting in the user profile is correct.

Table 72.User Settings / Password Life TimeAttributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: User {3} has {5} set to {6}. Must be less than or equal to {7}. PROFILE={4}. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT      a.cli_id, a.sid, a.hostname, b.username, a.profile, a.resource_name, a.limit, $
             (Password Lifetime Limit)
FROM        jac_data.unx_ora_profile_settings_v1 a
INNER JOIN  jac_data.unx_ora_user_profile_v1 b
ON          (a.cli_id=b.cli_id AND a.profile=b.profile AND a.sid=b.sid)
WHERE       a.resource_name='PASSWORD_LIFE_TIME'
AND   ((substr(limit,1,1) between '0' AND '9' AND integer(limit)>$(Password Lifetime Limit))
      OR    substr(limit,1,1) NOT between '0' AND '9' OR limit IS NULL)
```

User Settings / Password Reuse Max

This compliance query ensures that the user profile password reuse maximum is set appropriately.

Table 73.User Settings / Password Reuse Max Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: User, {3}, {5} is set to {6}. Must be at least {7}. Profile={4}.\n(Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       u.cli_id, u.sid, u.hostname, u.username, p.profile, p.resource_name, p.limit,
             $(Password Reuse Limit) as required_setting
FROM         jac_data.unx_ora_profile_settings_v1 p
INNER JOIN   jac_data.unx_ora_user_profile_v1 u
ON           (p.cli_id=u.cli_id AND u.sid=p.sid AND u.profile=p.profile)
WHERE        resource_name='PASSWORD_REUSE_MAX'
AND   (((substr(p.limit,1,1) between '0' AND '9') AND integer(p.limit) < $(Password Reuse
Limit))
             OR     (p.profile='DEFAULT' AND p.limit='UNLIMITED')
             OR     (p.limit IS NULL))
```

User Settings / Password Reuse Not Limited

This compliance query checks the PASSWORD_REUSE_TIME profile setting.

Table 74.User Settings / Password Reuse Not Limited Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: User, {3}, has {5} set to {6}. Profile={4}. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT        a.cli_id, a.sid, a.hostname, b.username, a.profile, a.resource_name, a.limit
FROM         jac_data.unx_ora_profile_settings_v1 a
INNER JOIN   jac_data.unx_ora_user_profile_V1 b
ON           a.cli_id=b.cli_id AND a.sid=b.sid AND a.profile=b.profile
WHERE        resource_name='PASSWORD_REUSE_TIME'
AND          upper(limit) NOT IN ('UNLIMITED','DEFAULT')
```

User Settings / Password Reuse Time Unlimited

Users with default system profile must have unlimited password reuse time.

Table 75.User Settings / Password Reuse Time Unlimited Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: User,{3}, profile, {4}, has {5} set to {6}. Must be set to UNLIMITED. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       a.cli_id, a.sid, a.hostname, b.username, b.profile, a.resource_name, a.limit
FROM         jac_data.unx_ora_profile_settings_v1 a
INNER JOIN   jac_data.unx_ora_user_profile_v1 b
ON           a.profile=b.profile AND a.cli_id=b.cli_id AND a.sid=b.sid
WHERE        a.resource_name='PASSWORD_REUSE_TIME'
AND          b.profile='DEFAULT' AND  a.limit <> 'UNLIMITED'
```

User Settings / Standard User Accounts Password Changed

This compliance query checks that the standard Oracle users do not have their original default passwords.

Table 76.User Settings / Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Standard user, {3}, password has not been changed. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       cli_id, sid, hostname, username
FROM         jac_data.unx_ora_strd_users_v2
WHERE        username IN ($(PWD Changing Standard Users))
```

Collector Instances and Parameters

The table below associates each collector instance with a specific collector and lists any parameters it has and the values for those parameters. Each collector instance is scheduled to run once a day at a random time.

Table 77.Collector instances and parameters for Unix Oracle Policy template

Instance name	Collector name	Parameter name	Parameter value
OraBinaryFilePermsV1	unix.any.OraBinaryFilePermsV1	None	None
OraHomeFilePermsV1	unix.any.OraHomeFilePermsV1	PERM	???????w?
OraHomeFilePermsV1	unix.any.OraHomeFilePermsV1	SEARCH_PATH	No value specified
OraListenerFilePermsV1	unix.any.OraListenerFilePermsV1	SEARCH_PATH	No value specified
OracleQueriesV1	unix.any.OracleQueriesV1	None	None
OraPwdFunctionsV1	unix.any.OraPwdFunctionsV1	None	None

Chapter 3.Collectors

This chapter documents new collectors that were developed for use in the policy. Documentation for previously developed collectors that are used in the policy template can be found in the *IBM Tivoli Security Compliance Manager Collector and Message Reference* publication.

unix.any.OraBinaryFilePermsV1.jar

This collector provides information about the file permissions of the Oracle™ main application files located in $ORACLE_HOME/bin/oracle

Platforms: AIX, SUNOS, LINUX

Oracle Releases: 8.04, 8.1, 9.2, 10

Tables

UNX_ORA_ORACLE_FILE_V1

Table 78.Column information for UNX_ORA_ORACLE_FILE_V1

Column Name	Description	Type (size)
SID	The Oracle SID	VARCHAR(64)
VALUE	The value	VARCHAR(128)
MOD_OWNER	Owner file access permissions	VARCHAR(64)
MOD_GROUP	Group file access permissions	VARCHAR(64)
MOD_OTHER	Global access permissions of the file	VARCHAR(64)
OWNER	File owner user name	VARCHAR(64)
GROUP	Group name	VARCHAR(64)

Parameters

None.

unix.any.OraHomeFilePermsV1.jar

This collector gathers file access permissions for files in the $ORACLE_HOME directory.

Platforms: AIX, SUNOS, LINUX

Oracle Releases: 8.04, 8.1, 9.2, 10

Tables

UNX_ORA_ORACLE_HOME_FILES_V1

Table 79.Column information for UNX_ORA_ORACLE_HOME_FILES_V1

Column Name	Description	Type (size)
SID	The Oracle SID	VARCHAR(64)
VALUE	The file name	VARCHAR(128)
MOD_OWNER	Owner file access permissions	VARCHAR(64)
MOD_GROUP	Group file access permissions	VARCHAR(64)
MOD_OTHER	Global access permissions of the file	VARCHAR(64)
OWNER	File owner user name	VARCHAR(64)
GROUP	Group name	VARCHAR(64)

Parameters

Table 80.Parameters for unix.any.OraHomeFilePermsV1.jar

Parameter	Description	Required	Default
PERMS	Regular expression (regex) pattern for permission matching. Only files with permissions matching this string are included in the output.	No	Match all permissions
SEARCH_PATH	Directories scanned by the collector.	No	Scan through entire $ORACLE_HOME

unix.any.OraListenerFilePermsV1.jar

This collector returns access right permissions for file, listener.ora.

Tables

UNX_ORA_LISTENER_V2

Table 81.Column information for UNX_ORA_LISTENER_V2

Column Name	Description	Type (size)
FILE	File name	VARCHAR(512)
CONTENT	Content associated with the keywords, PASSWORDS_ and	VARCHAR(512)

	passwords_	
COMMENT	Line is commented. Null if not a comment line.	VARCHAR(4)
MOD_OWNER	Owner file access permissions	VARCHAR(4)
MOD_GROUP	Group file access permissions	VARCHAR(4)
MOD_OTHER	Global access permissions of the file	VARCHAR(4)
OWNER	File owner user name	VARCHAR(64)
GROUP	Group name	VARCHAR(64)

Parameters

Table 82.Parameters for unix.any.OraListenerFilePermsV1.jar.

Parameter	Description	Required	Default
SEARCH_PATH	The directories to include when searching for listener.ora files.	No	/home/oracle /oracle /applications

unix.any.OraPwdFunctionsV1.jar

This collector verifies Oracle password functions by creating temporary new profile users that have weak passwords that violate security controls.

Tables

UNX_ORA_PW_FUNCTION_V1

Table 83.Column information for UNX_ORA_PW_FUNCTION_V1

Column Name	Description	Type (size)
SID	The Oracle SID	VARCHAR(64)
PROFILE	The profile that is incorrectly configured	VARCHAR(128)
LIMIT	The limit	VARCHAR(64)
HC_ID	Temporary id	VARCHAR(2)
HC_DESCRIPTION	Description of problematic id	VARCHAR(128)

Parameters

None

unix.any.OracleQueriesV1.jar

This collector gathers configuration and security information by sending structured queries to running Oracle instances and checking for keywords in listener.ora and sqlnet.ora.

Platforms: AIX, SUNOS, LINUX
Oracle Releases: 8.04, 8.1, 9.2, 10

Tables

UNX_ORA_ARCHIVE_FILES_V1

Table 84.Column information for UNX_ORA_ARCHIVE_FILES_V1

Column Name	Description	Type (size)
SID	The Oracle SID	VARCHAR(64)
VALUE	File name	VARCHAR(128)
MOD_OWNER	Owner file access permissions	VARCHAR(4)
MOD_GROUP	Group file access permissions	VARCHAR(4)
MOD_OTHER	Global access permissions of the file	VARCHAR(4)
OWNER	File owner user name	VARCHAR(64)
GROUP	Group name	VARCHAR(64)

UNX_ORA_AUDIT_OPTION_V1

Table 85.Column information for UNX_ORA_AUDIT_OPTION_V1

Column Name	Description	Type (size)
SID	The Oracle SID	VARCHAR(64)
USER_NAME	The user name	VARCHAR(30)
PROXY_NAME	The proxy name	VARCHAR(30)
AUDIT_OPTION	The audit option name	VARCHAR(40)
SUCCESS	Indication that success auditing is enabled	VARCHAR(10)
FAILURE	Indication that failure auditing is enabled	VARCHAR(10)

UNX_ORA_BSQ_FILE_V1

Table 86.Column information for UNX_ORA_BSQ_FILE_V1

Column Name	Description	Type (size)
SID	The Oracle SID	VARCHAR(64)
FILE_NAME	The file name	VARCHAR(128)
MOD_OWNER	Owner file access permissions	VARCHAR(4)

MOD_GROUP	Group file access permissions	VARCHAR(4)
MOD_OTHER	Global access permissions of the file	VARCHAR(4)
OWNER	File owner user name	VARCHAR(64)
GROUP	Group name	VARCHAR(64)
SUM_1	First number from the sum command	INTEGER
SUM_2	The second number returned from the sum command	INTEGER

Note: This table will contain file information for the following Oracle" files:

- $ORACLE_HOME/rdbms/admin/sql.bsq
- $ORACLE_HOME/rdbms/admin/catalog.bsq

UNX_ORA_CONFIG_FILES_V1

Table 87.Column information for UNX_ORA_CONFIG_FILES_V1

Column Name	Description	Type (size)
SID	The Oracle SID	VARCHAR(64)
VALUE	File name	VARCHAR(128)
MOD_OWNER	Owner file access permissions	VARCHAR(4)
MOD_GROUP	Group file access permissions	VARCHAR(4)
MOD_OTHER	Global access permissions of the file	VARCHAR(4)
OWNER	File owner user name	VARCHAR(64)
GROUP	Group name	VARCHAR(64)

UNX_ORA_CTRL_FILES_V2

Table 88.Column information for UNX_ORA_CTRL_FILES_V2

Column Name	Description	Type (size)
SID	The Oracle SID	VARCHAR(64)
VALUE	File name	VARCHAR(128)
MOD_OWNER	Owner file access permissions	VARCHAR(4)
MOD_GROUP	Group file access permissions	VARCHAR(4)
MOD_OTHER	Global access permissions of the file	VARCHAR(4)
OWNER	File owner user name	VARCHAR(64)
GROUP	Group name	VARCHAR(64)

UNX_ORA_DATA_FILES_V2

Table 89.Column information for UNX_ORA_DATA_FILES_V2

Column Name	Description	Type (size)

SID	The Oracle SID	VARCHAR(64)
FILE_NAME	File name	VARCHAR(64)
TABLESPACE_NAME	The tablespace name	VARCHAR(64)
MOD_OWNER	Owner file access permissions	VARCHAR(4)
MOD_GROUP	Group file access permissions	VARCHAR(4)
MOD_OTHER	Global access permissions of the file	VARCHAR(4)
OWNER	File owner user name	VARCHAR(64)
GROUP	Group name	VARCHAR(64)

UNX_ORA_SID_FILES_V2

Table 90.Column information for UNX_ORA_SID_FILES_V2

Column Name	Description	Type (size)
SID	The Oracle SID	VARCHAR(64)
FILE_TYPE	Init.ora or spfile.ora	VARCHAR(16)
FILE_NAME	The file name	VARCHAR(64)
MOD_OWNER	Owner file access permissions	VARCHAR(4)
MOD_GROUP	Group file access permissions	VARCHAR(4)
MOD_OTHER	Global access permissions of the file	VARCHAR(4)
OWNER	File owner user name	VARCHAR(64)
GROUP	Group name	VARCHAR(64)

UNX_ORA_REDO_FILES_V1

Table 91.Column information for UNX_ORA_REDO_FILES_V1

Column Name	Description	Type (size)
SID	The Oracle SID	VARCHAR(64)
MEMBER	File name	VARCHAR(128)
MOD_OWNER	Owner file access permissions	VARCHAR(4)
MOD_GROUP	Group file access permissions	VARCHAR(4)
MOD_OTHER	Global access permissions of the file	VARCHAR(4)
OWNER	File owner user name	VARCHAR(64)
GROUP	Group name	VARCHAR(64)
GROUP#	The group number	INTEGER
TYPE	Online/Offline	VARCHAR(7)

UNX_ORA_ROLLBACK_FILES_V1

Table 92.Column information for UNX_ORA_ROLLBACK_FILES_V1

Column Name	Description	Type (size)
SID	The Oracle SID	VARCHAR(64)
FILE_NAME	File name	VARCHAR(64)
TABLESPACE_NAME	The tablespace name	VARCHAR(64)
MOD_OWNER	Owner file access permissions	VARCHAR(4)
MOD_GROUP	Group file access permissions	VARCHAR(4)
MOD_OTHER	Global access permissions of the file	VARCHAR(4)
OWNER	File owner user name	VARCHAR(64)
GROUP	Group name	VARCHAR(64)

UNX_ORA_CLP_PRODUCT_PROFILE_V1

Table 93.Column information for UNX_ORA_CLP_PRODUCT_PROFILE_V1

Column Name	Description	Type (size)
SID	The Oracle SID	VARCHAR(64)
PRODUCT	Product name selected from system.SQLPLUS_PRODUCT_PROFILE	VARCHAR(30)
USERID	The user id selected from system.SQLPLUS_PRODUCT_PROFILE	VARCHAR(30)
ATTRIBUTE	The attribute selected from systemSQLPLUS_PRODUCT_PROFILE	VARCHAR(240)
CHAR_VALUE	The CHAR_VALUE selected from system.SQLPLUS_PRODUCT_PROFILE	VARCHAR(240)

UNX_ORA_SYNONYM_V1

Table 94.Column information for UNX_ORA_SYNONYM_V1

Column Name	Description	Type (size)
SID	The Oracle SID	VARCHAR(64)
SYNONYM_NAME	The synonym name	VARCHAR(30)
TABLE_OWNER	The table owner	VARCHAR(30)
TABLE_NAME	The table name	VARCHAR(30)

UNX_ORA_TEMP_FILES_V1

Table 95.Column information for UNX_ORA_TEMP_FILES_V1

Column Name	Description	Type (size)
SID	The Oracle SID	VARCHAR(64)
FILE_ID	File id	VARCHAR(16)

FILE_NAME	File name	VARCHAR(64)
TABLESPACE_NAME	The tablespace name	VARCHAR(64)
BYTES	Size	VARCHAR(16)
MOD_OWNER	Owner file access permissions	VARCHAR(4)
MOD_GROUP	Group file access permissions	VARCHAR(4)
MOD_OTHER	Global access permissions of the file	VARCHAR(4)
OWNER	File owner user name	VARCHAR(64)
GROUP	Group name	VARCHAR(64)

UNX_ORA_USR_PW_EXT_V2

Table 96.Column information for UNX_ORA_USR_PW_EXT_V2

Column Name	Description	Type (size)
SID	The Oracle SID	VARCHAR(64)
USERNAME	User name	VARCHAR(32)
PASSWORD	Password	VARCHAR(32)

Note: This table includes all dba_users whose password is external .

UNX_ORA_UTL_PRIVS_V1

Table 97.Column information for UNX_ORA_UTL_PRIVS_V1

Column Name	Description	Type (size)
SID	The Oracle SID	VARCHAR(64)
GRANTEE	The grantee of the privilege	VARCHAR(30)
OWNER	Owner	VARCHAR(30)
TABLE_NAME	The table name	VARCHAR(30)
PRIVILEGE	The privilege name	VARCHAR(30)

UNX_ORA_UTLPWD_FILE_V1

Table 98.Column information for UNX_ORA_UTLPWD_FILE_V1

Column Name	Description	Type (size)
SID	The Oracle SID	VARCHAR(64)
VALUE	File name	VARCHAR(128)
MOD_OWNER	Owner file access permissions	VARCHAR(4)
MOD_GROUP	Group file access permissions	VARCHAR(4)
MOD_OTHER	Global access permissions of the file	VARCHAR(4)
OWNER	File owner user name	VARCHAR(64)

GROUP	Group name	VARCHAR(64)

UNX_ORA_VERSION_V1

Table 99.Column information for UNX_ORA_VERSION_V1

Column Name	Description	Type (size)
SID	The Oracle SID	VARCHAR(64)
LEVEL_1	Integer value of first significant value of the current Oracle version	INTEGER
LEVEL_2	Integer value of second significant value of the current Oracle version	INTEGER
LEVEL_3	Integer value of the third significant value of the current Oracle version	INTEGER
LEVEL_4	Integer value of the forth significant value of the current Oracle version	INTEGER
LEVEL_5	Integer value of the fifth significant value of the current Oracle version	INTEGER
SAP	/usr/sap file exists	VARCHAR(5)

UNX_ORA_ARCHIVE_V1

Table 100.Column information for UNX_ORA_ARCHIVE_V1

Column Name	Description	Type (size)
SID	The Oracle SID	VARCHAR(64)
DATABASE_LOGMODE	The database log mode	VARCHAR(64)
AUTOMATIC_ARCHIVAL	Automatic archival	VARCHAR(64)

UNX_ORA_COL_PRIVS_V1

Table 101.Column information for UNX_ORA_COL_PRIVS_V1

Column Name	Description	Type (size)
SID	The Oracle SID	VARCHAR(64)
GRANTEE	The user who has been granted column privileges	VARCHAR(30)

UNX_ORA_PARAMETER_V1

Table 102.Column information for UNX_ORA_PARAMETER_V1

Column Name	Description	Type (size)
SID	The Oracle SID	VARCHAR(64)
NAME	The NAME from v$parameter	VARCHAR(64)
VALUE	The VALUE from v$parameter	VARCHAR(512)

UNX_ORA_PROFILE_SETTINGS_V1

Table 103.Column information for UNX_ORA_PROFILE_SETTINGS_V1

Column Name	Description	Type (size)
SID	The Oracle SID	VARCHAR(64)
PROFILE	The profile from dba_profiles	VARCHAR(30)
RESOURCE	The resource from dba_profiles where resource_name is one of: • PASSWORD_VERIFY_FUNCTION • PASSWORD_LIFE_TIME • PASSWORD_GRACE_TIME • PASSWORD_REUSE_TIME • PASSWORD_REUSE_MAX • FAILED_LOGIN_ATTEMPTS • PASSWORD_LOCK_TIME • IDLE_TIME	VARCHAR(32)
LIMIT	The LIMIT from dba_profiles	VARCHAR(32)

UNX_ORA_PWFILE_USERS_V1

Table 104.Column information for UNX_ORA_PWFILE_USERS_V1

Column Name	Description	Type (size)
SID	The Oracle SID	VARCHAR(64)
USERNAME	The user name from v$pwfile_users	VARCHAR(32)
SYSDBA	The sysdba from v$pwfile_users	VARCHAR(8)
SYSOPER	The sysoper from v$pwfile_users	VARCHAR(8)

UNX_ORA_ROLE_PRIVS_V1

Table 105.Column information for UNX_ORA_ROLE_PRIVS_V1

Column Name	Description	Type (size)
SID	The Oracle SID	VARCHAR(64)
GRANTEE	The user granted the role privilege	VARCHAR(30)
GRANTED_ROLE	The role granted	VARCHAR(30)
ADMIN_OPTION	The admin option	VARCHAR(3)
DEFAULT_ROLE	The default role	VARCHAR(3)

UNX_ORA_ROLES_V1

Table 106.Column information for UNX_ORA_ROLES_V1

Column Name	Description	Type (size)
SID	The Oracle SID	VARCHAR(64)
ROLE	The defined role from dba_roles	VARCHAR(30)
PASSWORD_REQUIRED	Password required	VARCHAR(8)

UNX_ORA_STRD_USERS_V2

Table 107.Column information for UNX_STRD_USERS_V2

Column Name	Description	Type (size)
SID	The Oracle SID	VARCHAR(64)
USERNAME	The user name	VARCHAR(32)

UNX_ORA_SYS_PRIVS_V1

Table 108.Column information for UNX_ORA_PARAMETER_V1

Column Name	Description	Type (size)
SID	The Oracle SID	VARCHAR(64)
GRANTEE	The user granted the privilege	VARCHAR(30)
PRIVILEGE	The granted privilege	VARCHAR(40)
ADMIN_OPTION	The admin_option from dba_sys_privs	VARCHAR(3)

UNX_ORA_TAB_PRIVS_V1

Table 109.Column information for UNX_ORA_TAB_PRIVS_V1

Column Name	Description	Type (size)
SID	The Oracle SID	VARCHAR(64)
GRANTEE	The user granted dba_tab_privs	VARCHAR(30)
GRANTOR	The grantor of the privilege	VARCHAR(30)
OWNER	The table owner	VARCHAR(30)

UNX_ORA_USER_PROFILE_V1

Table 110.Column information for UNX_ORA_USER_PROFILE_V1

Column Name	Description	Type (size)
SID	The Oracle SID	VARCHAR(64)
PROFILE	The profile from dba_users	VARCHAR(30)
USERNAME	The user name from dba_users	VARCHAR(30)

UNX_ORA_SQL_LOG_V1

Table 111.Column information for UNX_ORA_SQL_LOG_V1

Column Name	Description	Type (size)
TIMESTAMP	The time an error was encountered.	VARCHAR(64)
LEVEL	The level of the error logged	VARCHAR(64)
ACTOR	The activities class that encountered the error	VARCHAR(128)
DETAILS	Details of the error encountered	VARCHAR(512)

Note: Since unix.any.OracleQueriesV1.jar invokes many Oracle" sql queries, any errors that are encountered during normal collector processing are returned in this table instead of JAC_DATA.ERROR_LOG.

Parameters

None.

Appendix. Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594
U.S.A

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758
USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program describe in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Customers are responsible for ensuring their own compliance with various laws such as the Graham-Leach-Bliley Act, the Sarbanes-Oxley Act, and the Health Insurance Portability and Accountability Act. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal, accounting or auditing advice, or represent or warrant that its products or services will ensure that customer is in compliance with any law.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Additional notices

THIRD PARTY LICENSE TERMS AND CONDITIONS, NOTICES AND INFORMATION

The license agreement for this product refers you to this file for details concerning terms and conditions applicable to third party software code included in this product, and for certain notices and other information IBM must provide to you under its license to certain software code. The relevant terms and conditions, notices and other information are provided or referenced below. Please note that any non-English version of the licenses below is unofficial and is provided to you for your convenience only. The English version of the licenses below, provided as part of the English version of this file, is the official version.

Notwithstanding the terms and conditions of any other agreement you may have with IBM or any of its related or affiliated entities (collectively “IBM”), the third party software code identified below are “Excluded Components” and are subject to the following terms and conditions:

(a) the Excluded Components are provided on an “AS IS” basis;

(b) IBM DISCLAIMS ANY AND ALL EXPRESS AND IMPLIED WARRANTIES AND CONDITIONS WITH RESPECT TO THE EXCLUDED COMPONENTS, INCLUDING, BUT NOT LIMITED TO, THE WARRANTY OF NON-INFRINGEMENT OR INTERFERENCE AND THE IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE;

(c) IBM will not be liable to you or indemnify you for any claims related to the Excluded Components; and

(d) IBM will not be liable for any direct, indirect, incidental, special, exemplary, punitive or consequential damages with respect to the Excluded Components.

Notice for Apache Software Foundation

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

Trademarks

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

AFS
AIX
DB2
DB2 Universal Database
Domino
IBM
IBM logo
iSeries
pSeries
Lotus
SmartSuite
Tivoli
Tivoli logo
WebSphere
xSeries
zSeries

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Oracle is a registered trademark of Oracle Corporation.

Other company, product, and service names may be trademarks or service marks of others.