Tivoli Security Compliance Manager

Version 5.1.1 rel. 2 – July, 2008

Collector and Message Reference Windows 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, Windows 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 Windows Oracle Policy.
- Chapter 3, Collectors

  Provides general information on the new collectors.

Chapter 1.Required Configuration and additional information

Create Database Tables in DB2

Some of the queries in the Windows 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`*.

Create Role and User in Oracle Database

Additionally we have to create a specific role and user in Oracle Database scanned by the collectors, which will be used by the collectors to connect to this database (this user and role has to be created in every instance). There is a script *OraclePreRequisite.sql* provided with the policy to perform necessary actions. This script contains also initial password for mentioned specific user created. After you have verified the contents, use Oracle database management tools to execute this script in order to create user and role. I.e. (logged as Windows user having sufficient permissions):

```
sqlplus "/ as sysdba" @OraclePreRequisite.sql
```

Ensure if all commands were executed successfully (only dropping old settings of user/role can fail if this script wasn't executed before, because they don't exist).

Prepare collectors to work

Two oracle collectors have parameters ORACLE_PASSWORD and VAULT_PASSWORD. Both collectors (win.any.OracleQueriesV1, win.any.PwdFunctionsV1) have to receive the same pair of the password parameters. ORACLE_PASSWORD is the TSCM_USER's initial password which is used during first logging to the Oracle database and than it is reset. New password is stored in the vault file which is encoded with VAULT_PASSWORD**The VAULT_PASSWORD has to be set at the beginning and must not be changed after.**

Troubleshooting and basis of collectors work flow

Only two of the three collectors connect to the Oracle database: win.any.OracleQueriesV1, win.any.PwdFunctionsV1. Both of them respect the same password handling policy. Each time the collector is being run it resets the oracle database password and stores it in the vault file . The ORACLE_PASSWORD is used for the first logging to the Oracle database. The second parameter VAULT_PASSWORD is used to encode the vault file .

If the collector returns `ORA-01017: invalid username/password; logon denied [sid: sidName]` it means that the password has desynchronized. In this case we have to reset the password for TSCM_USER on the specified oracle database to the default one (the one set as the ORACLE_PASSWORD collector parameter) and run collectors (the *Lock after* in *Lock account on failed login* section for appropriate *Profile* must be set to 4. In other case the vault file has to be deleted as well). To resynchronize the Oracle we have to run *OraclePreRequisite.sql script* at the desynchronized instance.

Chapter 2.Policy Templates

This chapter documents the following policy template:

- Windows Oracle Policy

Windows Oracle Policy Template

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

Deployment information for the policy template

The IBM Tivoli Security Compliance Manager Windows 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 recommended to be 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'
`Authorized Users`	Users who can have access to $ORACLE_HOME directory	List of strings	administrator , administrators , system , 'Administrator', 'Administrators', 'SYSTEM'
`DBA Grantees`	List of allowed GRANTEEs for the DBA role.	List of strings	'SYS', 'SYSTEM', 'MWADM', 'TIVADMDB', 'OPS$TIVADM'
`DBA Group Members`	List of userids that are allowed in the DBA group.	List of strings	' administrator ', 'oracle', 'ora', 'mwadm', 'tivadm', 'Administrator', 'Administrators'
`Disallowed User Names`	Disallowed user names.	List of strings	'TRACESVR', 'MDSYS', 'ORDSYS', 'CTXSYS', 'REPADMIN', 'AURORA$ORB $UNAUTHENTICATED', '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`	This parameter specifies a time limit before a previous password can be re-entered.	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
  - 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
  - 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 world access
- 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	OraFilePermsV1

Violation message: Oracle not installed (client id: {0}; Hostname: {1})

SQL query:

```
SELECT       a.cli_id, a.alias as "Hostname"
FROM         jac_sys.clients a
EXCEPT
(SELECT      f.cli_id, f.alias as "Hostname"
FROM         jac_sys.clients f
INNER JOIN   jac_data.win_ora_bin_file_perms_v1 g ON (g.cli_id=f.cli_id))
```

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: PROFILE audit option, is not correct. SID={1} (client id: {0}; Hostname: {2})

SQL query:

```
SELECT       a.cli_id,a.sid, a.hostname
FROM  jac_data.win_ora_version_v1 a
LEFT JOIN    jac_data.win_ora_audit_option_v1 b
ON    (a.cli_id=b.cli_id AND a.sid=b.sid)
EXCEPT
(
      SELECT        c.cli_id, c.sid, c.hostname
      FROM   jac_data.win_ora_audit_option_v1 c
      WHERE  upper(value(audit_option, '')) = 'PROFILE'
      AND    upper(value(user_name, '')) = ''
      AND    upper(value(success, '')) = 'BY ACCESS'
      AND    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: ROLE audit option is not correct. SID={1} (client id: {0}; Hostname: {2})

SQL query:

```
SELECT       a.cli_id,a.sid, a.hostname
FROM  jac_data.win_ora_version_v1 a
LEFT JOIN    jac_data.win_ora_audit_option_v1 b
ON    (a.cli_id=b.cli_id AND a.sid=b.sid)
EXCEPT
(
      SELECT        c.cli_id, c.sid, c.hostname
      FROM   jac_data.win_ora_audit_option_v1 c
      WHERE  upper(value(audit_option, '')) = 'ROLE'
      AND    upper(value(user_name, '')) = ''
      AND    upper(value(success, '')) = 'BY ACCESS'
      AND    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} (client id: {0}; Hostname: {2})

SQL query:

```
SELECT       a.cli_id,a.sid, a.hostname
FROM  jac_data.win_ora_version_v1 a
LEFT JOIN    jac_data.win_ora_audit_option_v1 b
ON    (a.cli_id=b.cli_id AND a.sid=b.sid)
EXCEPT
(
      SELECT        c.cli_id, c.sid, c.hostname
      FROM   jac_data.win_ora_audit_option_v1 c
      WHERE  upper(value(audit_option, '')) = 'USER'
      AND    upper(value(user_name, '')) = ''
      AND    upper(value(success, '')) = 'BY ACCESS'
      AND    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. SID={1} (client id: {0}; Hostname: {4})

SQL query:

```
SELECT       a.cli_id, a.sid,a.name, a.value, a.hostname
FROM         jac_data.win_ora_parameter_v1 a
INNER JOIN   jac_data.win_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. SID={1} (client id: {0}; Hostname: {4})

SQL query:

```
SELECT       cli_id, sid, name, value, hostname
FROM         jac_data.win_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. SID={1} (client id: {0}; Hostname: {2})

SQL query:

```
SELECT       b.cli_id, b.sid, a.hostname
FROM  jac_data.win_ora_audit_option_v1 b
LEFT JOIN    jac_data.win_ora_version_v1 a on a.cli_id=b.cli_id
EXCEPT
      (SELECT       c.cli_id, c.sid, c.hostname
       FROM  jac_data.win_ora_audit_option_v1 c
       WHERE        upper(value(audit_option, '')) = 'CREATE SESSION'
       AND   upper(value(success, '')) = 'BY ACCESS'
       AND   upper(value(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. SID={1} (client id: {0}; Hostname: {2})

SQL query:

```
SELECT       b.cli_id, b.sid, a.hostname
FROM  jac_data.win_ora_audit_option_v1 b
LEFT JOIN    jac_data.win_ora_version_v1 a on a.cli_id=b.cli_id
EXCEPT
      (SELECT       c.cli_id, c.sid, c.hostname
       FROM  jac_data.win_ora_audit_option_v1 c
       WHERE        upper(value(audit_option, '')) = 'SYSTEM AUDIT'
       AND   upper(value(success, '')) = 'BY ACCESS'
       AND   upper(value(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. SID={1} (client id: {0}; Hostname: {2})

SQL query:

```
SELECT       b.cli_id, b.sid, a.hostname
FROM  jac_data.win_ora_audit_option_v1 b
LEFT JOIN    jac_data.win_ora_version_v1 a on a.cli_id=b.cli_id
EXCEPT
      (SELECT       c.cli_id, c.sid, c.hostname
       FROM  jac_data.win_ora_audit_option_v1 c
       WHERE        upper(value(audit_option, '')) = 'SYSTEM GRANT'
       AND   upper(value(success, '')) = 'BY ACCESS'
       AND   upper(value(failure, '')) = 'BY ACCESS'
      )
```

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 10.Collector Data / OraFilePermsV1 Data Exists Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Required collector data is missing or is too old: win.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.win_ora_version_v1
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 11.Collector Data / OraPwdFunctionsV1 Attributes

Priority	Normal
Collector instance name	OraPwdFunctionsV1

Violation message: Required collector data is missing or is too old: win.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.win_ora_pw_function_v1
WHERE logdate > TIMESTAMP(CHAR(CURRENT DATE - $(Max Collector Data Age) DAYS) || '-00.00.00')
```

Collector Data / OraFilePermsV1 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 / OracleQueriesV1 Data Exists Attributes

Priority	Normal
Collector instance name	OraFilePermsV1

Violation message: Required collector data is missing or is too old: win.any.OraFilePermsV1. (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.win_ora_file_perms_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 13.Encryption / DBLINK_ENCRYPT_LOGIN Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

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

SQL query:

```
SELECT       a.cli_id, a.sid, b.name, b.value, a.hostname
FROM         jac_data.win_ora_version_v1 a
INNER JOIN   jac_data.win_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 14.File Permissions / Default protection of database files Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Database file,{3}, permissions are incorrect. The file shouldn't be world-writable. (client id: {0}; Hostname: {1}; SID: {2})

SQL query:

```
SELECT a.cli_id, a.hostname, a.sid, a.file_name
FROM  jac_data.win_ora_temp_files_v1 a
WHERE (a.user_name NOT IN ($(Authorizated users))
AND   (a.perms_type=-1 OR a.perms_type=1)
AND   (a.file_read_data=1
       OR    a.file_write_data=1
       OR    a.file_append_data=1
       OR    a.file_read_ea=1
       OR    a.file_write_ea=1
       OR    a.file_execute=1
       OR    a.file_delete_child=1
       OR    a.file_read_attribute=1
       OR    a.file_write_attribute=1
       OR    a.delete=1
       OR    a.read_control=1
       OR    a.write_dac=1
       OR    a.write_owner=1))
UNION
SELECT b.cli_id, b.hostname, b.sid, b.file_name
FROM  jac_data.win_ora_data_files_v1 b
```

```
WHERE (b.user_name NOT IN ($(Authorizated users))
AND   (b.perms_type=-1 OR b.perms_type=1)
AND   (b.file_read_data=1
       OR    b.file_write_data=1
       OR    b.file_append_data=1
       OR    b.file_read_ea=1
       OR    b.file_write_ea=1
       OR    b.file_execute=1
       OR    b.file_delete_child=1
       OR    b.file_read_attribute=1
       OR    b.file_write_attribute=1
       OR    b.delete=1
       OR    b.read_control=1
       OR    b.write_dac=1
       OR    b.write_owner=1))
```

File Permissions / Listener.ora access permissions

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

Table 15.File Permissions / Listener.ora access permissions Attributes

Priority	Normal
Collector instance name	OraFilePermsV1

Violation message: Oracle database control file {2} has incorrect world access permissions. (client id: {0}; Hostname: {1})

SQL query:

```
SELECT a.cli_id, a.hostname, a.file_name
FROM  jac_data.win_ora_listener_file_perms_v1 a
WHERE (a.user_name NOT IN ($(Authorizated users))
AND   (a.perms_type=-1 OR a.perms_type=1)
AND   (a.file_read_data=1
       OR    a.file_write_data=1
       OR    a.file_append_data=1
       OR    a.file_read_ea=1
       OR    a.file_write_ea=1
       OR    a.file_execute=1
       OR    a.file_delete_child=1
       OR    a.file_read_attribute=1
       OR    a.file_write_attribute=1
       OR    a.delete=1
       OR    a.read_control=1
       OR    a.write_dac=1
       OR    a.write_owner=1))
```

File Permissions / Mirror Control Files

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

Table 16.File Permissions / Mirror Control Files Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: File {3} has no mirror. (client id: {0}; Hostname: {1}; SID: {2}).

SQL query:

```
with distinctControlFiles as
      (SELECT DISTINCT cli_id, sid, hostname, file_name FROM jac_data.win_ora_ctrl_files_v1)

SELECT              cli_id, sid, hostname, count(file_name) as Files
FROM         distinctControlFiles
GROUP BY            cli_id, sid, hostname
HAVING              count(file_name) < 2
```

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 17.Identify and Authenticate / ALTER SESSION privilege Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: ALTER SESSION privilege invalid. GRANTEE={3} PRIVILEGE={4} (client id: {0}; Hostname: {1}; SID: {2})

SQL query:

```
SELECT       cli_id, hostname, sid, grantee, privilege
FROM         jac_data.win_ora_sys_privs_v1
WHERE        (UPPER(privilege) = 'ALTER SESSION')
AND   UPPER(grantee)
NOT IN
      (SELECT       y.username
       FROM         jac_add.oracle_users_v1 y
       WHERE usertype IN ($(Allowed Grantors)))
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 18.Identify and Authenticate / ANY Privileges Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Grantee {3} must not have privilege {4}. (client id: {0}; Hostname: {1}; SID: {2})

SQL query:

```
SELECT       cli_id, hostname, sid, grantee, privilege
FROM         jac_data.win_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
       WHERE        usertype IN ($(Allowed Grantors)))
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 19.Identify and Authenticate / AUDIT privileges Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Incorrect audit privilege. GRANTEE={3} PRIVILEGE={4} (client id: {0}; Hostname: {1}; SID: {2})

SQL query:

```
SELECT       cli_id, hostname, sid, grantee, privilege
FROM         jac_data.win_ora_sys_privs_v1
WHERE        (UPPER(privilege) LIKE 'AUDIT%')
AND          UPPER(grantee)
NOT IN
      (SELECT       username
       FROM         jac_add.oracle_users_v1 x
       WHERE usertype IN ($(Allowed Grantors)))
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 20.Identify and Authenticate / DBA Role Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Unauthorized user with DBA-Role. User={3}. Role={4}. (client id: {0}; Hostname: {1}; SID: {2})

SQL query:

```
SELECT       cli_id, hostname, sid, grantee, granted_role
FROM         jac_data.win_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 21.Identify and Authenticate / DBA Group Attributes

Priority	Normal
Collector instance name	OraFilePermsV1

Violation message: Unauthorized user, {2} has inappropriate access permissions to a file {3}. (client id: {0}; Hostname: {1}; SID: {2})

SQL query:

```
SELECT cli_id, hostname, user_name, file_name
FROM  jac_data.win_ora_bin_file_perms_v1
WHERE lower(user_name) 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 22.Identify and Authenticate / Disallowed User Accounts Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Disallowed user, {3}, has role {4}. (client id: {0}; Hostname: {1}; SID: {2})

SQL query:

```
SELECT       a.cli_id, a.hostname, a.sid, a.username, b.granted_role
FROM  jac_data.win_ora_user_profile_v1 a LEFT OUTER JOIN jac_data.win_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 23.Identify and Authenticate / Failed Login Attempts Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

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

SQL query:

```
SELECT a.cli_id, a.sid, a.hostname, b.username, a.profile, a.resource_name, a.limit
FROM  jac_data.win_ora_profile_settings_v1 a INNER JOIN jac_data.win_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 24.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}. (client id: {0}; Hostname: {1}; SID: {2})

SQL query:

```
SELECT       a.cli_id, a.hostname, a.sid, b.username, a.profile, resource_name, a.limit,  $
              (Minimum Idle Time Limit)
FROM         jac_data.win_ora_profile_settings_v1 a
INNER JOIN   jac_data.win_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 25.Identify and Authenticate / LOCK ANY privilege Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: LOCK privilege incorrect. GRANTEE={3} PRIVILEGE={4}. (client id: {0}; Hostname: {1}; SID: {2})

SQL query:

```
SELECT       cli_id, hostname, sid, grantee, privilege
FROM         jac_data.win_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 26.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}. (client id: {0}; Hostname: {1}; SID: {2})

SQL query:

```
SELECT       cli_id, hostname, sid, grantee, granted_role
FROM         jac_data.win_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 27.Identify and Authenticate / Password Grace Time Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: ORA PROFILE SETTINGS PASSWORD GRACE TIME NOT STANDARD. USERNAME={2} PROFILE={3} RESOURCE NAME={4} LIMIT={5}. (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.win_ora_profile_settings_v1 a
INNER JOIN   jac_data.win_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 28.Identify and Authenticate / Password Lock TimeAttributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: User {3} has {5} set to {6}. Should be at least {7}. SID={1}. Profile={3}. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       a.cli_id, a.hostname, a.sid, username, a.profile, resource_name, limit,
              $(Minimum Password Lock Time)
FROM         jac_data.win_ora_profile_settings_v1 a
INNER JOIN   jac_data.win_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 29.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}" . (Client: {0}, Hostname: {1}, SID={2})

SQL query:

```
SELECT        u.cli_id, u.hostname, u.sid, u.username, u.profile, p.limit, p.comment
FROM         jac_data.win_ora_user_profile_v1 u
INNER JOIN   jac_data.win_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.comment 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 30.Identify and Authenticate / Privileges Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

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

SQL query:

```
SELECT       cli_id, sid, hostname, grantee
FROM         jac_data.win_ora_tab_privs_v1
WHERE        grantee
NOT IN
      (SELECT       role
       FROM  jac_data.win_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 31. Identify and Authenticate / Resource Limit Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

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

SQL query:

```
SELECT       cli_id, hostname, sid, name, value
FROM         jac_data.win_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 32.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: {1}, SID={2})

SQL query:

```
SELECT       a.cli_id, a.hostname, a.sid, a.grantee, a.granted_role
FROM         jac_data.win_ora_role_privs_v1 a
WHERE        a.granted_role
IN
      (SELECT DISTINCT grantee
       FROM        jac_data.win_ora_sys_privs_v1
       WHERE       grantee
       IN
             (SELECT      role
              FROM        jac_data.win_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 33.Identify and Authenticate / Restrict System Privileges Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

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

SQL query:

```
SELECT       cli_id, hostname , sid, grantee, privilege
FROM         jac_data.win_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 34.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: {1}, SID={2})

SQL query:

```
SELECT       cli_id, hostname, sid, username, sysdba, sysoper
FROM         jac_data.win_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 35.Privileges Permissions / Grants to Public Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

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

SQL query:

```
SELECT       cli_id, hostname, sid, 'ROLE' , GRANTEE, GRANTED_ROLE
FROM         jac_data.win_ora_role_privs_v1
WHERE        GRANTEE = 'PUBLIC'
```

```
UNION
SELECT       cli_id, hostname, sid, 'SYSTEM' , GRANTEE, PRIVILEGE
FROM         jac_data.win_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 36.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: {1}, SID={2})

SQL query:

```
SELECT       cli_id, hostname, sid, GRANTEE, grantor
FROM         jac_data.win_ora_tab_privs_v1
WHERE        upper(GRANTEE) = 'PUBLIC'
AND   grantor
NOT IN
      (SELECT       username
       FROM         jac_add.oracle_users_v1 a
       WHERE usertype IN ($(Allowed Grantors)))
```

Protecting OSR Resources / Archive Logging Enabled

This compliance query ensures that archive log mode is enabled.

Table 37.Protecting OSR Resources / Archive Logging Enabled Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Archive log mode is not enabled. Database logmode={3} Automatic archival={4}. (Client: {0}, Hostname: {1}, SID={2})

SQL query:

```
SELECT       cli_id, hostname, sid, database_logmode, automatic_archival
FROM         jac_data.win_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 38.Protecting OSR Resources / Archive log files Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Archive log file {3} has incorrect world access permissions. (client id: {0}; Hostname: {1}; SID: {2})

SQL query:

```
SELECT a.cli_id, a.hostname, a.sid, a.file_name
FROM  jac_data.win_ora_archive_files_v1 a
WHERE (a.user_name NOT IN ($(Authorizated users))
AND   (a.perms_type=-1 OR a.perms_type=1)
AND   (a.file_read_data=1
       OR    a.file_write_data=1
       OR    a.file_append_data=1
       OR    a.file_read_ea=1
       OR    a.file_write_ea=1
       OR    a.file_delete_child=1
       OR    a.file_read_attribute=1
       OR    a.file_write_attribute=1
       OR    a.delete=1
       OR    a.read_control=1
       OR    a.write_dac=1
       OR    a.write_owner=1))
```

Protecting OSR Resources / Control file access permission

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

Table 39.Protecting OSR Resources / Control file access permission Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Oracle database control file {3} has incorrect world access permissions. (client id: {0}; Hostname: {1}; SID: {2})

SQL query:

```
SELECT       a.cli_id, a.hostname, a.sid, a.file_name
FROM         jac_data.win_ora_ctrl_files_v1 a
WHERE        (a.user_name NOT IN ($(Authorizated users))
AND          (a.perms_type=-1 OR a.perms_type=1)
AND          (a.file_read_data=1 OR a.file_write_data=1
              OR    a.file_append_data=1
              OR    a.file_read_ea=1
              OR    a.file_write_ea=1
              OR    a.file_delete_child=1
              OR    a.file_read_attribute=1
              OR    a.file_write_attribute=1
              OR    a.delete=1
              OR    a.read_control=1
              OR    a.write_dac=1
              OR    a.write_owner=1))
```

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

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

Table 40.Protecting OSR Resources / Init<database.sid>.ORA(initialization file) Attributes

Priority	Normal
Collector instance name	OraFilePermsV1

Violation message: File {2} has incorrect world access permissions. (client id: {0}; Hostname: {1})

SQL query:

```
SELECT a.cli_id, a.hostname, a.file_name
FROM  jac_data.win_ora_file_perms_v1 a
WHERE (a.user_name NOT IN ($(Authorizated users))
AND   (a.perms_type=-1 OR a.perms_type=1)
AND   (a.file_read_data=1 OR a.file_write_data=1
       OR    a.file_append_data=1
       OR    a.file_read_ea=1
       OR    a.file_write_ea=1
       OR    a.file_delete_child=1
       OR    a.file_read_attribute=1
       OR    a.file_write_attribute=1
       OR    a.delete=1
       OR    a.read_control=1
       OR    a.write_dac=1
       OR    a.write_owner=1))
```

Protecting OSR Resources / Listener.ora password access

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

Table 41.Protecting OSR Resources / Listener.ora password access Attributes

Priority	Normal
Collector instance name	OraFilePermsV1

Violation message: File {2} has incorrect world access permissions. (client id: {0}; Hostname: {1})

SQL query:

```
SELECT a.cli_id, a.hostname, a.file_name, a.content, a.comment
FROM  jac_data.win_ora_listener_file_perms_v1 a
WHERE content IS NOT NULL AND comment=0
AND   (a.user_name NOT IN ($(Authorizated users))
AND   (a.perms_type=-1 OR a.perms_type=1)
AND   (a.file_read_data=1 OR a.file_write_data=1
       OR    a.file_append_data=1
       OR    a.file_read_ea=1
       OR    a.file_write_ea=1
       OR    a.file_delete_child=1
```

```
        OR    a.file_read_attribute=1
        OR    a.file_write_attribute=1
        OR    a.delete=1
        OR    a.read_control=1
        OR    a.write_dac=1
        OR    a.write_owner=1))
```

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 42.Protecting OSR Resources / Oracle Program File Access Attributes

Priority	Normal
Collector instance name	OraFilePermsV1

Violation message: File {2} has incorrect world access permissions. (client id: {0}; Hostname: {1})

SQL query:

```
SELECT a.cli_id, a.hostname, a.file_name
FROM  jac_data.win_ora_bin_file_perms_v1 a
WHERE (a.user_name NOT IN ($(Authorizated users))
AND   (a.perms_type=-1 OR a.perms_type=1)
AND   (a.file_read_data=1 OR a.file_write_data=1
        OR    a.file_append_data=1
        OR    a.file_read_ea=1
        OR    a.file_write_ea=1
        OR    a.file_delete_child=1
        OR    a.file_read_attribute=1
        OR    a.file_write_attribute=1
        OR    a.delete=1
        OR    a.read_control=1
        OR    a.write_dac=1 OR a.write_owner=1))
```

Protecting OSR Resources / Oracle config file permission

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

Table 43.Protecting OSR Resources / Oracle config file permission Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Oracle config file {3} has incorrect world access permissions. (client id: {0}; Hostname: {1}; SID: {2})

SQL query:

```
SELECT a.cli_id, a.hostname, a.sid, a.file_name
FROM  jac_data.win_ora_config_files_v1 a
WHERE (a.user_name NOT IN ($(Authorizated users))
AND   (a.perms_type=-1 OR a.perms_type=1)
AND   (a.file_read_data=1 OR a.file_write_data=1
        OR    a.file_append_data=1
        OR    a.file_read_ea=1
        OR    a.file_write_ea=1
        OR    a.file_delete_child=1
        OR    a.file_read_attribute=1
        OR    a.file_write_attribute=1
        OR    a.delete=1
        OR    a.read_control=1
        OR    a.write_dac=1
        OR    a.write_owner=1))
```

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 44.Protecting OSR Resources / Redo log files access permissions Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Redo file {3} has incorrect world access permissions. (client id:{0}; Hostname: {1}; SID: {2})

SQL query:

```
SELECT a.cli_id, a.hostname, a.sid, a.file_name
FROM  jac_data.win_ora_redo_files_v1 a
WHERE (a.user_name NOT IN ($(Authorizated users))
AND   (a.perms_type=-1 OR a.perms_type=1)
AND   (a.file_read_data=1 OR a.file_write_data=1
        OR    a.file_append_data=1
        OR    a.file_read_ea=1
        OR    a.file_write_ea=1
        OR    a.file_delete_child=1
        OR    a.file_read_attribute=1
        OR    a.file_write_attribute=1
        OR    a.delete=1
        OR    a.read_control=1
        OR    a.write_dac=1 OR a.write_owner=1))
```

Protecting OSR Resources / Rollback Segments

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

Table 45.Protecting OSR Resources / Rollback Segments Attributes

Priority	Normal
Collector instance name	OracleQueriesV1, OraFilePermsV1

Violation message: Rollback file{3} has incorrect world access permissions.(client id:{0};Hostname:{1};SID: {2})

SQL query:

```
SELECT       a.cli_id, a.hostname, a.sid, a.file_name
FROM         jac_data.win_ora_rollback_files_v1 a
WHERE        (a.user_name NOT IN ($(Authorizated users))
AND          (a.perms_type=-1 OR a.perms_type=1)
AND          (a.file_read_data=1 OR a.file_write_data=1
              OR    a.file_append_data=1
              OR    a.file_read_ea=1
              OR    a.file_write_ea=1
              OR    a.file_delete_child=1
              OR    a.file_read_attribute=1
              OR    a.file_write_attribute=1
              OR    a.delete=1
              OR    a.read_control=1
              OR    a.write_dac=1
              OR    a.write_owner=1))
```

Protecting OSR Resources / Table Space Data Files

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

Table 46.Protecting OSR Resources / Table Space Data Files Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Table space data file{3} has incorrect world access permissions.(client id: {0}; Hostname: {1}; SID: {2})

SQL query:

```
SELECT a.cli_id, a.hostname, a.sid, a.file_name
FROM  jac_data.win_ora_data_files_v1 a
WHERE (a.user_name NOT IN ($(Authorizated users))
AND   (a.perms_type=-1 OR a.perms_type=1)
AND   (a.file_read_data=1 OR a.file_write_data=1
       OR    a.file_append_data=1
       OR    a.file_read_ea=1
       OR    a.file_write_ea=1
       OR    a.file_delete_child=1
       OR    a.file_read_attribute=1
       OR    a.file_write_attribute=1
       OR    a.delete=1
       OR    a.read_control=1
       OR    a.write_dac=1 OR a.write_owner=1))
```

Protecting OSR Resources / Temporary File Access Permission

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

Table 47.Protecting OSR Resources / Temporary File Access Permission Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Temporary file {3} has incorrect world access permissions. (client id: {0}; Hostname: {1}; SID: {2})

SQL query:

```
SELECT a.cli_id, a.hostname, a.sid, a.file_name
FROM  jac_data.win_ora_temp_files_v1 a
WHERE (a.user_name NOT IN ($(Authorizated users))
AND   (a.perms_type=-1 OR a.perms_type=1)
AND   (a.file_read_data=1 OR a.file_write_data=1
       OR    a.file_append_data=1
       OR    a.file_read_ea=1
       OR    a.file_write_ea=1
       OR    a.file_delete_child=1
       OR    a.file_read_attribute=1
       OR    a.file_write_attribute=1
       OR    a.delete=1
       OR    a.read_control=1
       OR    a.write_dac=1 OR a.write_owner=1))
```

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 48.Protecting OSR Resources / UTLPWDMG.SQL world access Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: Oracle utlpwdmg.sql file {3} has incorrect world access permissions. (client id: {0}; Hostname: {1}; SID: {2})

SQL query:

```
SELECT a.cli_id, a.hostname, a.sid, a.file_name
FROM  jac_data.win_ora_utlpwd_files_v1 a
WHERE (a.user_name NOT IN ($(Authorizated users))
AND   (a.perms_type=-1 OR a.perms_type=1)
AND   (a.file_read_data=1 OR a.file_write_data=1
       OR    a.file_append_data=1
       OR    a.file_read_ea=1
       OR    a.file_write_ea=1
       OR    a.file_delete_child=1
       OR    a.file_read_attribute=1
       OR    a.file_write_attribute=1
       OR    a.delete=1
       OR    a.read_control=1
       OR    a.write_dac=1 OR a.write_owner=1))
```

Roles, Views, and Access Control / Host Command

This compliance query ensures that the HOST command is disabled.

Table 49.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.win_ora_version_v1
WHERE        (cli_id, sid)
NOT IN
      (SELECT       cli_id, sid
       FROM         jac_data.win_ora_clp_product_profile_v1
       WHERE        upper(product) = 'SQL*PLUS'
       AND          userid = '%'
       AND          char_value = 'DISABLED'
       AND          attribute = 'HOST' )
```

Roles, Views, and Access Control / Oracle default role

This compliance query ensures that roles are assigned appropriately.

Table 50.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.win_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 51.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.win_ora_version_v1
WHERE        (cli_id, sid, hostname)
NOT IN
      (SELECT       cli_id, sid, hostname
       FROM         jac_data.win_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 52.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 53.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.win_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 54.UTL / Utl_file package Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

Violation message: {4} is public. Privilege={5}. (Client: {0}, Hostname: {2}, SID={1})

SQL query:

```
SELECT       cli_id, sid, hostname, grantee, table_name, privilege
FROM         jac_data.win_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 55.UTL / Utl_file_dirAttributes

Priority	Normal
Collector instance name	OracleQueriesV1

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

SQL query:

```
SELECT       cli_id, sid, hostname, name, value
FROM         jac_data.win_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 56.User Settings / Disallowed User Names Attributes

Priority	Normal
Collector instance name	OracleQueriesV1

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

SQL query:

```
SELECT       cli_id, sid, hostname, username
FROM         jac_data.win_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 57.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.win_ora_profile_settings_v1 a
INNER JOIN   jac_data.win_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 58.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}. (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,
      $(Password Reuse Limit) as required_setting
FROM         jac_data.win_ora_profile_settings_v1 p
INNER JOIN   jac_data.win_ora_user_profile_v1 u
ON           (p.cli_id=u.cli_id AND u.sid=p.sid AND u.profile=p.profile)
WHERE        resource_name='PASSWORD_REUSE_MAX'
AND (((substr(p.limit,1,1) between '0' AND '9') AND integer(p.limit)<$(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 59.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, username, a.profile, resource_name, limit
FROM         jac_data.win_ora_profile_settings_v1 a
INNER JOIN   jac_data.win_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 60.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, username, b.profile, a.resource_name, a.limit
FROM         jac_data.win_ora_profile_settings_v1 a
INNER JOIN   jac_data.win_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 61.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.win_ora_strd_users_v2
WHERE        username IN ($(PWD Changing Standard Users))
```

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.

win.any.OraFilePermsV1.jar

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

Platforms: Windows

Oracle Releases: 8.04, 8.1, 9.2, 10

Tables

WIN_ORA_FILE_PERMS_V1

Table 62.Column information for WIN_ORA_FILE_PERMS_V1

Column	Description	Size	Type
SID	Oracle Database SID	64	VARCHAR
FILE_NAME	File's name	256	VARCHAR
USER_NAME	User name	64	VARCHAR
PERMS_TYPE	Indicates the type of the permissions gathered by the collector (-1 effective, 0 deny, 1 allow)	0	SMALLINT
FILE_READ_DATA	Permission to read from a file, or list the contents of a directory.	0	SMALLINT
FILE_WRITE_DATA	Permission to write to a file, or create a new file inside a directory.	0	SMALLINT
FILE_APPEND_DATA	Permission to append data to a file, create a new subdirectory inside a directory, or create a pipe instance.	0	SMALLINT
FILE_READ_EA	Permission to read extended attributes	0	SMALLINT
FILE_WRITE_EA	Permission to write extended attributes	0	SMALLINT
FILE_EXECUTE	Permission to execute a file or access a directory	0	SMALLINT
FILE_DELETE_CHILD	Permission to delete a file from a directory	0	SMALLINT
FILE_READ_ATTRIBUTE	Permission to read attributes	0	SMALLINT
FILE_WRITE_ATTRIBUTE	Permission to write attributes	0	SMALLINT
DELETE	Permission to delete a file or directory.	0	SMALLINT
READ_CONTROL	Permission to read permissions.	0	SMALLINT
WRITE_DAC	Permission to write permissions	0	SMALLINT
WRITE_OWNER	Permission to take ownership	0	SMALLINT
SYNCHRONIZE	Permission to use object for synchronization	0	SMALLINT
MS_API_ERROR_CODE	Value returned by the executables (more detail information can be found in winerr.h)	0	INTEGER

WIN_ORA_BIN_FILE_PERMS_V1

Table 63.Column information for WIN_ORA_BIN_FILE_PERMS_V1

Column	Description	Size	Type
SID	Oracle Database SID	64	VARCHAR
FILE_NAME	File's name	256	VARCHAR
USER_NAME	User name	64	VARCHAR
PERMS_TYPE	Indicates the type of the permissions gathered by the collector (-1 effective, 0 deny, 1 allow)	0	SMALLINT
FILE_READ_DATA	Permission to read from a file, or list the contents of a directory.	0	SMALLINT
FILE_WRITE_DATA	Permission to write to a file, or create a new file inside a directory.	0	SMALLINT
FILE_APPEND_DATA	Permission to append data to a file, create a new subdirectory inside a directory, or create a pipe instance.	0	SMALLINT
FILE_READ_EA	Permission to read extended attributes	0	SMALLINT
FILE_WRITE_EA	Permission to write extended attributes	0	SMALLINT
FILE_EXECUTE	Permission to execute a file or access a directory	0	SMALLINT
FILE_DELETE_CHILD	Permission to delete a file from a directory	0	SMALLINT
FILE_READ_ATTRIBUTE	Permission to read attributes	0	SMALLINT
FILE_WRITE_ATTRIBUTE	Permission to write attributes	0	SMALLINT
DELETE	Permission to delete a file or directory.	0	SMALLINT
READ_CONTROL	Permission to read permissions.	0	SMALLINT
WRITE_DAC	Permission to write permissions	0	SMALLINT
WRITE_OWNER	Permission to take ownership	0	SMALLINT
SYNCHRONIZE	Permission to use object for synchronization	0	SMALLINT
MS_API_ERROR_CODE	Value returned by the executables (more detail information can be found in winerr.h)	0	INTEGER

WIN_ORA_LISTENER_FILE_PERMS_V1

Table 64.Column information for WIN_ORA_LISTENER_FILE_PERMS_V1

Column	Description	Size	Type
SID	Oracle Database SID	64	VARCHAR
FILE_NAME	File's name	256	VARCHAR
USER_NAME	User name	64	VARCHAR
PERMS_TYPE	Indicates the type of the permissions gathered by the collector (-1 effective, 0 deny, 1 allow)	0	SMALLINT
FILE_READ_DATA	Permission to read from a file, or list the contents of a directory.	0	SMALLINT
FILE_WRITE_DATA	Permission to write to a file, or create a new file inside a directory.	0	SMALLINT
FILE_APPEND_DATA	Permission to append data to a file, create a new subdirectory inside a directory, or create a pipe instance.	0	SMALLINT
FILE_READ_EA	Permission to read extended attributes	0	SMALLINT
FILE_WRITE_EA	Permission to write extended attributes	0	SMALLINT
FILE_EXECUTE	Permission to execute a file or access a directory	0	SMALLINT
FILE_DELETE_CHILD	Permission to delete a file from a directory	0	SMALLINT
FILE_READ_ATTRIBUTE	Permission to read attributes	0	SMALLINT
FILE_WRITE_ATTRIBUTE	Permission to write attributes	0	SMALLINT
DELETE	Permission to delete a file or directory.	0	SMALLINT
READ_CONTROL	Permission to read permissions.	0	SMALLINT
WRITE_DAC	Permission to write permissions	0	SMALLINT
WRITE_OWNER	Permission to take ownership	0	SMALLINT
SYNCHRONIZE	Permission to use object for synchronization	0	SMALLINT
MS_API_ERROR_CODE	Value returned by the executables (more detail information can be found in winerr.h)	0	INTEGER
COMMENT	Whether the line containing the keyword (PASSWORD_, password_) is commented, if there is no value the keyword has not been found in listener file.	0	SMALLINT
CONTENT	Content associated with the keywords, PASSWORDS_ and passwords_	512	VARCHAR

Parameters

None.

win.any.OraPwdFunctionsV1.jar

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

Platforms: Windows
Oracle Releases: 8.04, 8.1, 9.2, 10

Tables

WIN_ORA_PW_FUNCTION_V1

Table 65.Column information for WIN_ORA_PW_FUNCTION_V1

Column	Description	Size	Type
SID	Oracle Database SID	64	VARCHAR
PROFILE	The Profile that is incorrectly configured	128	VARCHAR
LIMIT	The Limit	64	VARCHAR
COMMENT	Comment generated by Oracle	512	VARCHAR

Parameters

Parameter	Description	Required	Default
ORACLE_PASSWORD	Password used to log into the Oracle database for the first time	Yes	Or4cl3#P4ssw0rd
VAULT_PASSWORD	Password used to encode the vault file.	Yes	None

win.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: Windows
Oracle Releases: 8.04, 8.1, 9.2, 10

Tables

WIN_ORA_ARCHIVE_FILES_V1

Table 66.Column information for WIN_ORA_ARCHIVE_FILES_V1

Column	Description	Size	Type
SID	Oracle Database SID	64	VARCHAR
FILE_NAME	File's name	256	VARCHAR
USER_NAME	User name	64	VARCHAR
PERMS_TYPE	Indicates the type of the permissions gathered by the collector (-1 effective, 0 deny, 1 allow)	0	SMALLINT
FILE_READ_DATA	Permission to read from a file, or list the contents of a directory.	0	SMALLINT
FILE_WRITE_DATA	Permission to write to a file, or create a new file inside a directory.	0	SMALLINT
FILE_APPEND_DATA	Permission to append data to a file, create a new subdirectory inside a directory, or create a pipe instance.	0	SMALLINT
FILE_READ_EA	Permission to read extended attributes	0	SMALLINT
FILE_WRITE_EA	Permission to write extended attributes	0	SMALLINT
FILE_EXECUTE	Permission to execute a file or access a directory	0	SMALLINT
FILE_DELETE_CHILD	Permission to delete a file from a directory	0	SMALLINT
FILE_READ_ATTRIBUTE	Permission to read attributes	0	SMALLINT
FILE_WRITE_ATTRIBUTE	Permission to write attributes	0	SMALLINT
DELETE	Permission to delete a file or directory.	0	SMALLINT
READ_CONTROL	Permission to read permissions.	0	SMALLINT
WRITE_DAC	Permission to write permissions	0	SMALLINT
WRITE_OWNER	Permission to take ownership	0	SMALLINT
SYNCHRONIZE	Permission to use object for synchronization	0	SMALLINT
MS_API_ERROR_CODE	Value returned by the executables (more detail information can be found in winerr.h)	0	INTEGER

WIN_ORA_AUDIT_OPTION_V1

Table 67.Column information for WIN_ORA_AUDIT_OPTION_V1

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

WIN_ORA_BSQ_FILE_V1

Table 68.Column information for WIN_ORA_BSQ_FILE_V1

Column	Description	Size	Type
SID	Oracle Database SID	64	VARCHAR
FILE_NAME	The file name	128	VARCHAR
FINGERPRINT	MD5 encoded with Base64	64	VARCHAR

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

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

WIN_ORA_CONFIG_FILES_V1

Table 69.Column information for WIN_ORA_CONFIG_FILES_V1

Column	Description	Size	Type
SID	Oracle Database SID	64	VARCHAR
FILE_NAME	File's name	256	VARCHAR
USER_NAME	User name	64	VARCHAR
PERMS_TYPE	Indicates the type of the permissions gathered by the collector (-1 effective, 0 deny, 1 allow)	0	SMALLINT
FILE_READ_DATA	Permission to read from a file, or list the contents of a directory.	0	SMALLINT
FILE_WRITE_DATA	Permission to write to a file, or create a new file inside a directory.	0	SMALLINT
FILE_APPEND_DATA	Permission to append data to a file, create a new subdirectory inside a directory, or create a pipe instance.	0	SMALLINT
FILE_READ_EA	Permission to read extended attributes	0	SMALLINT
FILE_WRITE_EA	Permission to write extended attributes	0	SMALLINT
FILE_EXECUTE	Permission to execute a file or access a directory	0	SMALLINT
FILE_DELETE_CHILD	Permission to delete a file from a directory	0	SMALLINT
FILE_READ_ATTRIBUTE	Permission to read attributes	0	SMALLINT
FILE_WRITE_ATTRIBUTE	Permission to write attributes	0	SMALLINT
DELETE	Permission to delete a file or directory.	0	SMALLINT
READ_CONTROL	Permission to read permissions.	0	SMALLINT
WRITE_DAC	Permission to write permissions	0	SMALLINT
WRITE_OWNER	Permission to take ownership	0	SMALLINT
SYNCHRONIZE	Permission to use object for synchronization	0	SMALLINT
MS_API_ERROR_CODE	Value returned by the executables (more detail information can be found in winerr.h)	0	INTEGER

WIN_ORA_CTRL_FILES_V2

Table 70.Column information for WIN_ORA_CTRL_FILES_V2

Column	Description	Size	Type
SID	Oracle Database SID	64	VARCHAR
FILE_NAME	File's name	256	VARCHAR
USER_NAME	User name	64	VARCHAR
PERMS_TYPE	Indicates the type of the permissions gathered by the collector (-1 effective, 0 deny, 1 allow)	0	SMALLINT
FILE_READ_DATA	Permission to read from a file, or list the contents of a directory.	0	SMALLINT
FILE_WRITE_DATA	Permission to write to a file, or create a new file inside a directory.	0	SMALLINT
FILE_APPEND_DATA	Permission to append data to a file, create a new subdirectory inside a directory, or create a pipe instance.	0	SMALLINT
FILE_READ_EA	Permission to read extended attributes	0	SMALLINT
FILE_WRITE_EA	Permission to write extended attributes	0	SMALLINT
FILE_EXECUTE	Permission to execute a file or access a directory	0	SMALLINT
FILE_DELETE_CHILD	Permission to delete a file from a directory	0	SMALLINT
FILE_READ_ATTRIBUTE	Permission to read attributes	0	SMALLINT
FILE_WRITE_ATTRIBUTE	Permission to write attributes	0	SMALLINT
DELETE	Permission to delete a file or directory.	0	SMALLINT
READ_CONTROL	Permission to read permissions.	0	SMALLINT
WRITE_DAC	Permission to write permissions	0	SMALLINT
WRITE_OWNER	Permission to take ownership	0	SMALLINT
SYNCHRONIZE	Permission to use object for synchronization	0	SMALLINT
MS_API_ERROR_CODE	Value returned by the executables (more detail information can be found in winerr.h)	0	INTEGER

WIN_ORA_DATA_FILES_V2

Table 71.Column information for WIN_ORA_DATA_FILES_V2

Column	Description	Size	Type
SID	Oracle Database SID	64	VARCHAR
FILE_NAME	File's name	256	VARCHAR
USER_NAME	User name	64	VARCHAR
PERMS_TYPE	Indicates the type of the permissions gathered by the collector (-1 effective, 0 deny, 1 allow)	0	SMALLINT
FILE_READ_DATA	Permission to read from a file, or list the contents of a directory.	0	SMALLINT
FILE_WRITE_DATA	Permission to write to a file, or create a new file inside a directory.	0	SMALLINT
FILE_APPEND_DATA	Permission to append data to a file, create a new subdirectory inside a directory, or create a pipe instance.	0	SMALLINT
FILE_READ_EA	Permission to read extended attributes	0	SMALLINT
FILE_WRITE_EA	Permission to write extended attributes	0	SMALLINT
FILE_EXECUTE	Permission to execute a file or access a directory	0	SMALLINT
FILE_DELETE_CHILD	Permission to delete a file from a directory	0	SMALLINT
FILE_READ_ATTRIBUTE	Permission to read attributes	0	SMALLINT
FILE_WRITE_ATTRIBUTE	Permission to write attributes	0	SMALLINT
DELETE	Permission to delete a file or directory.	0	SMALLINT
READ_CONTROL	Permission to read permissions.	0	SMALLINT
WRITE_DAC	Permission to write permissions	0	SMALLINT
WRITE_OWNER	Permission to take ownership	0	SMALLINT
SYNCHRONIZE	Permission to use object for synchronization	0	SMALLINT
MS_API_ERROR_CODE	Value returned by the executables (more detail information can be found in winerr.h)	0	INTEGER

WIN_ORA_REDO_FILES_V1

Table 72.Column information for WIN_ORA_REDO_FILES_V1

Column	Description	Size	Type
SID	Oracle Database SID	64	VARCHAR
FILE_NAME	File's name	256	VARCHAR
USER_NAME	User name	64	VARCHAR
PERMS_TYPE	Indicates the type of the permissions gathered by the collector (-1 effective, 0 deny, 1 allow)	0	SMALLINT
FILE_READ_DATA	Permission to read from a file, or list the contents of a directory.	0	SMALLINT
FILE_WRITE_DATA	Permission to write to a file, or create a new file inside a directory.	0	SMALLINT
FILE_APPEND_DATA	Permission to append data to a file, create a new subdirectory inside a directory, or create a pipe instance.	0	SMALLINT
FILE_READ_EA	Permission to read extended attributes	0	SMALLINT
FILE_WRITE_EA	Permission to write extended attributes	0	SMALLINT
FILE_EXECUTE	Permission to execute a file or access a directory	0	SMALLINT
FILE_DELETE_CHILD	Permission to delete a file from a directory	0	SMALLINT
FILE_READ_ATTRIBUTE	Permission to read attributes	0	SMALLINT
FILE_WRITE_ATTRIBUTE	Permission to write attributes	0	SMALLINT
DELETE	Permission to delete a file or directory.	0	SMALLINT
READ_CONTROL	Permission to read permissions.	0	SMALLINT
WRITE_DAC	Permission to write permissions	0	SMALLINT
WRITE_OWNER	Permission to take ownership	0	SMALLINT
SYNCHRONIZE	Permission to use object for synchronization	0	SMALLINT
MS_API_ERROR_CODE	Value returned by the executables (more detail information can be found in winerr.h)	0	INTEGER

WIN_ORA_ROLLBACK_FILES_V1

Table 73.Column information for WIN_ORA_ROLLBACK_FILES_V1

Column	Description	Size	Type
SID	Oracle Database SID	64	VARCHAR
FILE_NAME	File's name	256	VARCHAR
USER_NAME	User name	64	VARCHAR
PERMS_TYPE	Indicates the type of the permissions gathered by the collector (-1 effective, 0 deny, 1 allow)	0	SMALLINT
FILE_READ_DATA	Permission to read from a file, or list the contents of a directory.	0	SMALLINT
FILE_WRITE_DATA	Permission to write to a file, or create a new file inside a directory.	0	SMALLINT
FILE_APPEND_DATA	Permission to append data to a file, create a new subdirectory inside a directory, or create a pipe instance.	0	SMALLINT
FILE_READ_EA	Permission to read extended attributes	0	SMALLINT
FILE_WRITE_EA	Permission to write extended attributes	0	SMALLINT
FILE_EXECUTE	Permission to execute a file or access a directory	0	SMALLINT
FILE_DELETE_CHILD	Permission to delete a file from a directory	0	SMALLINT
FILE_READ_ATTRIBUTE	Permission to read attributes	0	SMALLINT
FILE_WRITE_ATTRIBUTE	Permission to write attributes	0	SMALLINT
DELETE	Permission to delete a file or directory.	0	SMALLINT
READ_CONTROL	Permission to read permissions.	0	SMALLINT
WRITE_DAC	Permission to write permissions	0	SMALLINT
WRITE_OWNER	Permission to take ownership	0	SMALLINT
SYNCHRONIZE	Permission to use object for synchronization	0	SMALLINT
MS_API_ERROR_CODE	Value returned by the executables (more detail information can be found in winerr.h)	0	INTEGER

WIN_ORA_CLP_PRODUCT_PROFILE_V1

Table 74.Column information for WIN_ORA_CLP_PRODUCT_PROFILE_V1

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

WIN_ORA_SYNONYM_V1

Table 75.Column information for WIN_ORA_SYNONYM_V1

Column	Description	Size	Type
SID	The Oracle SID	64	VARCHAR
SYNONYM_NAME	The synonym name	30	VARCHAR
TABLE_OWNER	The table owner	30	VARCHAR
TABLE_NAME	The table name	30	VARCHAR

WIN_ORA_TEMP_FILES_V1

Table 76.Column information for WIN_ORA_TEMP_FILES_V1

Column	Description	Size	Type
SID	Oracle Database SID	64	VARCHAR
FILE_NAME	File’s name	256	VARCHAR
USER_NAME	User name	64	VARCHAR
PERMS_TYPE	Indicates the type of the permissions gathered by the collector (-1 effective, 0 deny, 1 allow)	0	SMALLINT
FILE_READ_DATA	Permission to read from a file, or list the contents of a directory.	0	SMALLINT
FILE_WRITE_DATA	Permission to write to a file, or create a new file inside a directory.	0	SMALLINT
FILE_APPEND_DATA	Permission to append data to a file, create a new subdirectory inside a directory, or create a pipe instance.	0	SMALLINT
FILE_READ_EA	Permission to read extended attributes	0	SMALLINT
FILE_WRITE_EA	Permission to write extended attributes	0	SMALLINT
FILE_EXECUTE	Permission to execute a file or access a directory	0	SMALLINT
FILE_DELETE_CHILD	Permission to delete a file from a directory	0	SMALLINT
FILE_READ_ATTRIBUTE	Permission to read attributes	0	SMALLINT
FILE_WRITE_ATTRIBUTE	Permission to write attributes	0	SMALLINT
DELETE	Permission to delete a file or directory.	0	SMALLINT
READ_CONTROL	Permission to read permissions.	0	SMALLINT
WRITE_DAC	Permission to write permissions	0	SMALLINT
WRITE_OWNER	Permission to take ownership	0	SMALLINT
SYNCHRONIZE	Permission to use object for synchronization	0	SMALLINT
MS_API_ERROR_CODE	Value returned by the executables (more detail information can be found in winerr.h)	0	INTEGER

WIN_ORA_USR_PW_EXT_V2

Table 77.Column information for WIN_ORA_USR_PW_EXT_V2

Column	Description	Size	Type
SID	The Oracle SID	64	VARCHAR
USERNAME	User name	32	VARCHAR
PASSWORD	Password	32	VARCHAR

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

WIN_ORA_UTL_PRIVS_V1

Table 78.Column information for WIN_ORA_UTL_PRIVS_V1

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

WIN_ORA_UTLPWD_FILE_V1

Table 79.Column information for WIN_ORA_UTLPWD_FILE_V1

Column	Description	Size	Type
SID	Oracle Database SID	64	VARCHAR
FILE_NAME	File's name	256	VARCHAR
USER_NAME	User name	64	VARCHAR
PERMS_TYPE	Indicates the type of the permissions gathered by the collector (-1 effective, 0 deny, 1 allow)	0	SMALLINT
FILE_READ_DATA	Permission to read from a file, or list the contents of a directory.	0	SMALLINT
FILE_WRITE_DATA	Permission to write to a file, or create a new file inside a directory.	0	SMALLINT
FILE_APPEND_DATA	Permission to append data to a file, create a new subdirectory inside a directory, or create a pipe instance.	0	SMALLINT
FILE_READ_EA	Permission to read extended attributes	0	SMALLINT
FILE_WRITE_EA	Permission to write extended attributes	0	SMALLINT
FILE_EXECUTE	Permission to execute a file or access a directory	0	SMALLINT
FILE_DELETE_CHILD	Permission to delete a file from a directory	0	SMALLINT
FILE_READ_ATTRIBUTE	Permission to read attributes	0	SMALLINT
FILE_WRITE_ATTRIBUTE	Permission to write attributes	0	SMALLINT
DELETE	Permission to delete a file or directory.	0	SMALLINT
READ_CONTROL	Permission to read permissions.	0	SMALLINT
WRITE_DAC	Permission to write permissions	0	SMALLINT
WRITE_OWNER	Permission to take ownership	0	SMALLINT
SYNCHRONIZE	Permission to use object for synchronization	0	SMALLINT
MS_API_ERROR_CODE	Value returned by the executables (more detail information can be found in winerr.h)	0	INTEGER

WIN_ORA_VERSION_V1

Table 80.Column information for WIN_ORA_VERSION_V1

Column	Description	Size	Type
SID	The Oracle SID	64	VARCHAR
LEVEL_1	Integer value of first significant value of the current Oracle version	0	INTEGER
LEVEL_2	Integer value of second significant value of the current Oracle version	0	INTEGER
LEVEL_3	Integer value of the third significant value of the current Oracle version	0	INTEGER
LEVEL_4	Integer value of the forth significant value of the current Oracle version	0	INTEGER
LEVEL_5	Integer value of the fifth significant value of the current Oracle version	0	INTEGER
SAP	/usr/sap file exists	5	VARCHAR

WIN_ORA_ARCHIVE_V1

Table 81.Column information for WIN_ORA_ARCHIVE_V1

Column	Description	Size	Type
SID	The Oracle SID	64	VARCHAR
DATABASE_LOGMODE	The database log mode	64	VARCHAR
AUTOMATIC_ARCHIVAL	Automatic archival	64	VARCHAR

WIN_ORA_COL_PRIVS_V1

Table 82.Column information for WIN_ORA_COL_PRIVS_V1

Column	Description	Size	Type
SID	The Oracle SID	64	VARCHAR
GRANTEE	The user who has been granted column privileges	30	VARCHAR
GRANTOR	Name of the user who performed the grant	30	VARCHAR
OWNER	User name of the owner of the object	30	VARCHAR

WIN_ORA_PARAMETER_V1

Table 83.Column information for WIN_ORA_PARAMETER_V1

Column	Description	Size	Type
SID	The Oracle SID	64	VARCHAR
NAME	The NAME from v$parameter	64	VARCHAR
VALUE	The VALUE from v$parameter	512	VARCHAR

WIN_ORA_PROFILE_SETTINGS_V1

Table 84.Column information for WIN_ORA_PROFILE_SETTINGS_V1

Column	Description	Size	Type
SID	The Oracle SID	64	VARCHAR
PROFILE	The profile from dba_profiles	30	VARCHAR
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	32	VARCHAR
LIMIT	The LIMIT from dba_profiles	32	VARCHAR

WIN_ORA_PWFILE_USERS_V1

Table 85.Column information for WIN_ORA_PWFILE_USERS_V1

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

WIN_ORA_ROLE_PRIVS_V1

Table 86.Column information for WIN_ORA_ROLE_PRIVS_V1

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

WIN_ORA_ROLES_V1

Table 87.Column information for WIN_ORA_ROLES_V1

Column	Description	Size	Type
SID	The Oracle SID	64	VARCHAR
ROLE	The defined role from dba_roles	30	VARCHAR
PASSWORD_REQUIRED	Password required	8	VARCHAR

WIN_ORA_STRD_USERS_V2

Table 88.Column information for WIN_STRD_USERS_V2

Column	Description	Size	Type
SID	The Oracle SID	64	VARCHAR
USERNAME	The user name	32	VARCHAR

WIN_ORA_SYS_PRIVS_V1

Table 89.Column information for WIN_ORA_PARAMETER_V1

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

WIN_ORA_TAB_PRIVS_V1

Table 90.Column information for WIN_ORA_TAB_PRIVS_V1

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

WIN_ORA_USER_PROFILE_V1

Table 91.Column information for WIN_ORA_USER_PROFILE_V1

Column	Description	Size	Type
SID	The Oracle SID	64	VARCHAR
PROFILE	The profile from dba_users	30	VARCHAR
USERNAME	The user name from dba_users	30	VARCHAR

WIN_ORA_SQL_LOG_V1

Table 92.Column information for WIN_ORA_SQL_LOG_V1

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

Note: Since win.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

Parameter	Description	Required	Default
ORACLE_PASSWORD	Password used to log into the Oracle database for the first time	Yes	Or4cl3#P4ssw0rd
VAULT_PASSWORD	Password used to encode the vault file.	Yes	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.