ORACLE

Oracle Database Security Assessment Tool 3.1

Learn how secure your databases are with DBSAT

Pedro Lopes
Product Manager
Oracle Database Security

January 2024

What you don’t know can hurt you

Is the database configured according to Oracle’s best practices?

What security controls are already in place?

What other security controls are available to me?

What users are in the database?

What access do users have?

What sensitive data is in this database?

Top 10 findings

From database security assessments

- No Database Security policies/strategy in place
- No patching/patch management policy in place
- No personalized accounts; No separation of duties; Over-privileged accounts
- No encryption of sensitive/regulated data
- No monitoring/auditing in place
- No password policies; Weak password management
- Non-Production (DEV/TEST/TRAINING) systems with production data
- No cleanup of test/sample accounts
- No anonymization of data sent to third parties
- No OS hardening

What is DBSAT?

Assess your database security before hackers come knocking

Assess Configuration

Patches

Data Encryption

Auditing policies

OS file permissions

Database configuration

Listener configuration

Fine-grained access control

Identify Risky Users

Database accounts

User privileges

User roles

Discover Sensitive Data

What type, where, and how much?

Sample pattern files for Greek, German, Dutch, French, Spanish, Italian, and Portuguese based data models as well.

Assessment Reports

Summary and detailed information

Prioritized, actionable and target specific recommendations

Mapping to EU GDPR, STIG and CIS Benchmark

Runs on 11g to 23c Oracle Databases.

New in DBSAT 3.1 (January 2024)

Updated for Oracle Database 19c CIS Benchmark v1.2

- Added 10 CIS findings
- All CIS related findings updated to reflect changes in numbering scheme

Improved findings

- **`USER.NOEXPIRE`**
  Improved logic and summary
- **`USER.APPOWNER`**
  Optimizations to improve performance and reduce the level of detail
- **`ENCRYPT.TDE`**
  Updated remarks to clarify the usage of the `TABLESPACE_ENCRYPTION` parameter and recommendations when upgrading to Oracle Database 23c and you are using a de-supported algorithm

Added findings

- `USER.DEFAULTPROFILE`
- `PRIV.NETPACKAGEPUBLIC`
- `PRIV.FILESYSTEMPACKAGEPUBLIC`
- `PRIV.ENCRYPTPACKAGEPUBLIC`
- `PRIV.JAVAPACKAGEPUBLIC`
- `PRIV.JOBSCHPACKAGEPUBLIC`
- `PRIV.QUERYPACKAGEPUBLIC`
- `PRIV.CREDPACKAGEPUBLIC`
- `AUDIT.SYNONYMS`
- `CONF.DEFAULTPDBOSUSER`

- **`CONF.PREAUTHREQUESTURL`**
  On ADBs, checks for pre-authenticated URLs

New in DBSAT 3.0 (November 2023)

Updated to STIG V2R8 for the Oracle Database

- Added 30 STIG findings
- Updated all STIG related findings to use STIG Group IDs

Added/Improved findings

- Added: Oracle Database 23c SQL Firewall
- Added: Five new Auditing findings
- Updated: All auditing findings updated
- Added one new finding on Sensitive Data and TSDP
- Updated: INFO.PATCH, ENCRYPT.TDE, NET.ENCRYPT, USER. AUTHVERSION
- And more!

Discoverer

- Added India PAN and Aadhaar Number sensitive types

Improved clarity and quality

- All remarks and recommendations reviewed and updated
- New one-line summary highlights the objective and context of each check.
- “Oracle Best Practices” findings clearly tagged.
- Remarks now include a mention of Oracle Database 23c desupported features
- Rule IDs are updated and expanded for better clarity

Core

- New command line option to exclude users (-u in report).
- Python is no longer required to run DBSAT
- Optimized performance to speed up data collection
- Added support for Linux 64-bit Arm and 23c

New findings

■ DBSAT 3.0 (38)
🟧 DBSAT 3.1 (10)

Total findings: 132

USER.DEFAULTPROFILE
PRIV.NETPACKAGEPUBLIC
PRIV.FILESYSTEMPACKAGEPUBLIC
PRIV.ENCRYPTPACKAGEPUBLIC
PRIV.JAVAPACKAGEPUBLIC
PRIV.JOBSCHPACKAGEPUBLIC
PRIV.QUERYPACKAGEPUBLIC
PRIV.CREDPACKAGEPUBLIC
AUDIT.SYNONYMS
CONF.DEFAULTPDBOSUSER
CONF.PREAUTHREQUESTURL
USER.APPOWNER
USER.SHARED
USER.OBJOWNER
USER.OBJAUTHZ
USER.SECURITYOBJS

USER.GRANTOPTION
USER.SENSITIVEDATA
USER.IDLETIME
USER.TEMP
USER.DEV
USER.REPCAT
PRIV.OBJPUBLIC
AUTHZ.PASSWORDSCRIPTS
AUTHZ.DATAMASKING
AUTHZ.PKI
ACCESS.TSDP
AUDIT.CONDITION
AUDIT.SHAREDPROXY
AUDIT.TABLESPACE
AUDIT.CLEANUPJOBS
AUDIT.DATAPUMP

AUDIT.STIGPOLICY
AUDIT.DATABASEVAULT
AUDIT.LABELSECURITY
ENCRYPT.TLSFIPS
CONF.CONTROLFILES
CONF.REDOLOGS
CONF.ARCHIVELOG
CONF.SQLFIREWALL
CONF.READONLYHOME
CONF.DBCOMPONENTS
CONF.JOB
CONF.SOURCEANALYSIS
NET.CONNECTIONLIMITS
OS.INSTALLATIONUSER
OS.MULTIDB
OS.CMANLOCAL
OS.DIAGNOSTICDEST

Sample finding

A single sentence that describes what should be done *New in 3.0*

Rule ID

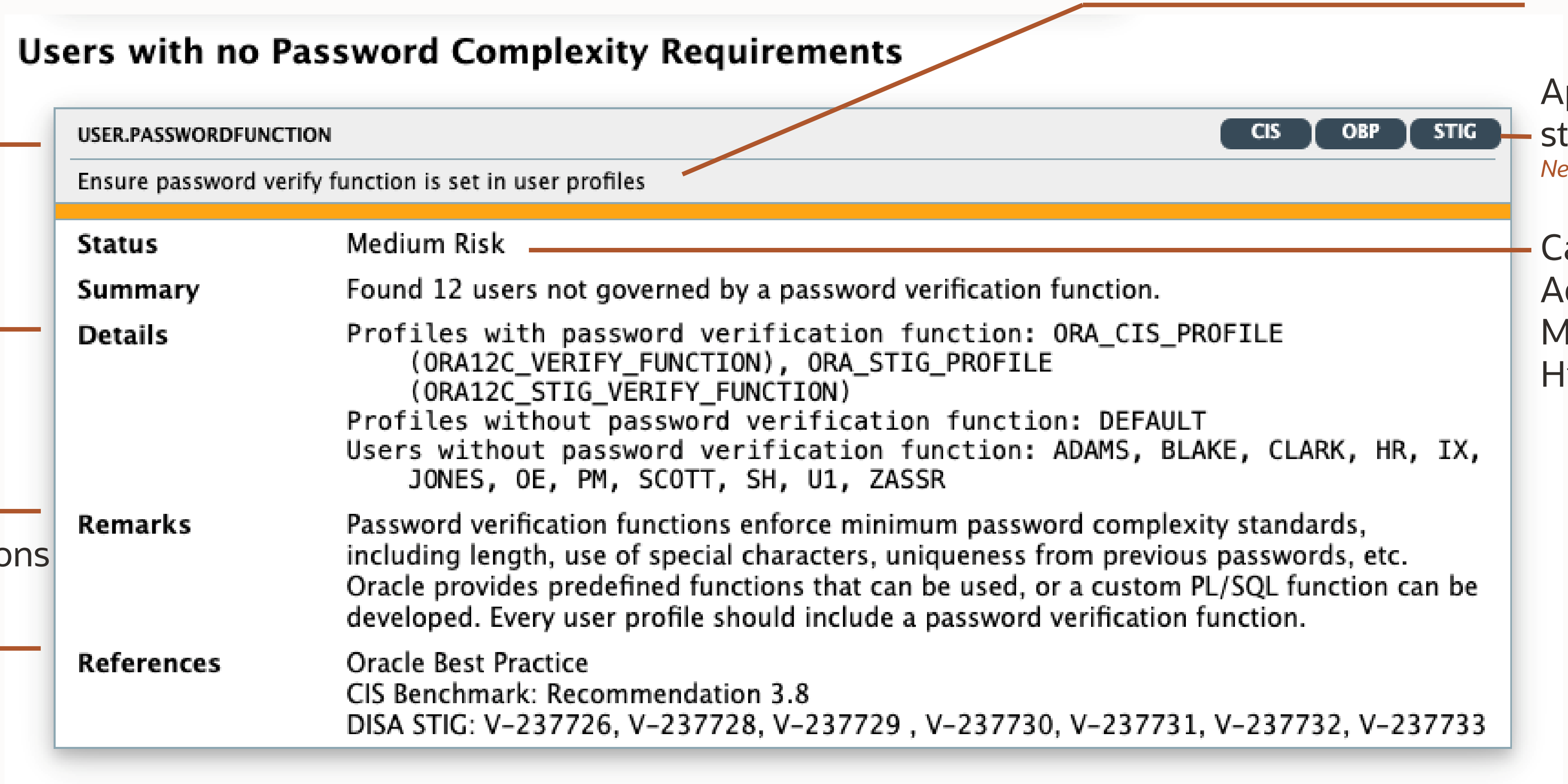
Detail of the Finding

Rationale and Recommendations

Mapping to Regulations

Applicable standards *New OPB in 3.0*

Can be Evaluate, Advisory, Low, Medium, or High Risk



Users with no Password Complexity Requirements

USER.PASSWORDFUNCTION

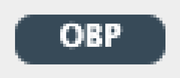
Ensure password verify function is set in user profiles

Status	Medium Risk
Summary	Found 12 users not governed by a password verification function.
Details	Profiles with password verification function: ORA_CIS_PROFILE (ORA12C_VERIFY_FUNCTION), ORA_STIG_PROFILE (ORA12C_STIG_VERIFY_FUNCTION) Profiles without password verification function: DEFAULT Users without password verification function: ADAMS, BLAKE, CLARK, HR, IX, JONES, OE, PM, SCOTT, SH, U1, ZASSR
Remarks	Password verification functions enforce minimum password complexity standards, including length, use of special characters, uniqueness from previous passwords, etc. Oracle provides predefined functions that can be used, or a custom PL/SQL function can be developed. Every user profile should include a password verification function.
References	Oracle Best Practice CIS Benchmark: Recommendation 3.8 DISA STIG: V-237726, V-237728, V-237729 , V-237730, V-237731, V-237732, V-237733

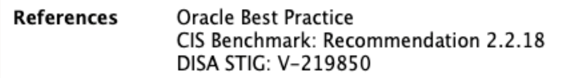
Oracle Best Practice (OBP)

NEW in 3.0

Clearly identify checks that are Oracle best practices ➡



OBP



References Oracle Best Practice
CIS Benchmark: Recommendation 2.2.18
DISA STIG: V-219850

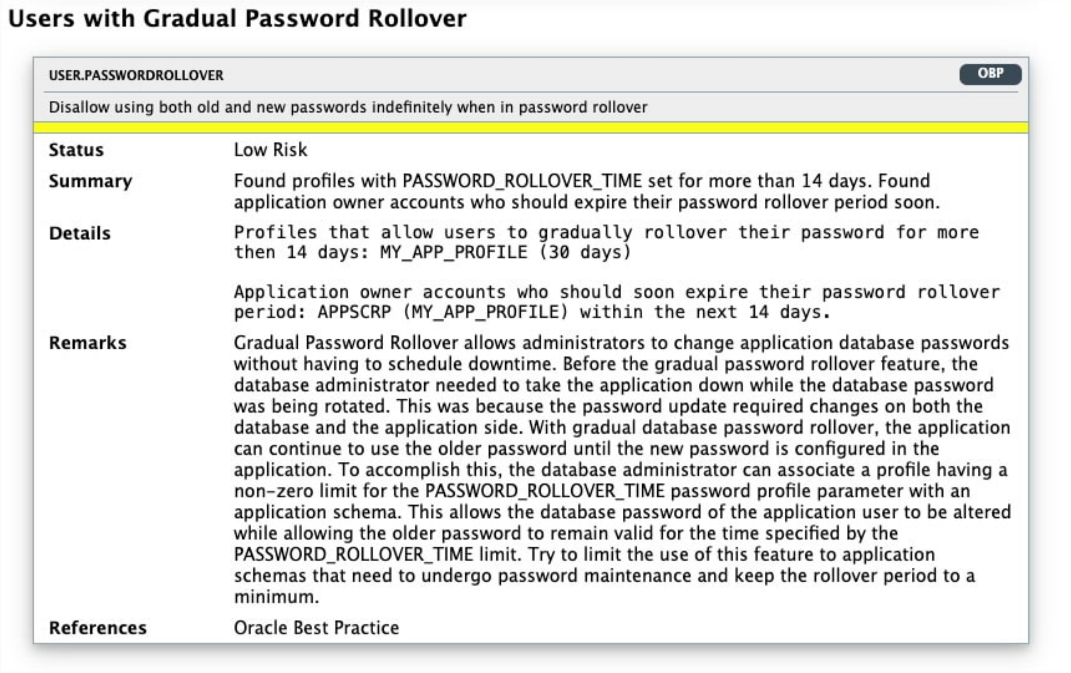
A check can be an OBP but not part of CIS or STIG because:

- **Specialization: Oracle's depth of knowledge**
  Oracle has a broader and deeper view on the Oracle Database and its features
- **Release cycles: Oracle Database release cycle vs standard/framework updates**
  Releases occur at different times
- **Technology updates: Oracle Database innovations**
  New features are introduced in every release, in patches, and can be backported
- **Standard/Framework did not identify feature or do not recognize risk**

Oracle Best Practice

Example

NEW in 3.0



Users with Gradual Password Rollover

USER.PASSWORDROLLOVER OBP

Disallow using both old and new passwords indefinitely when in password rollover

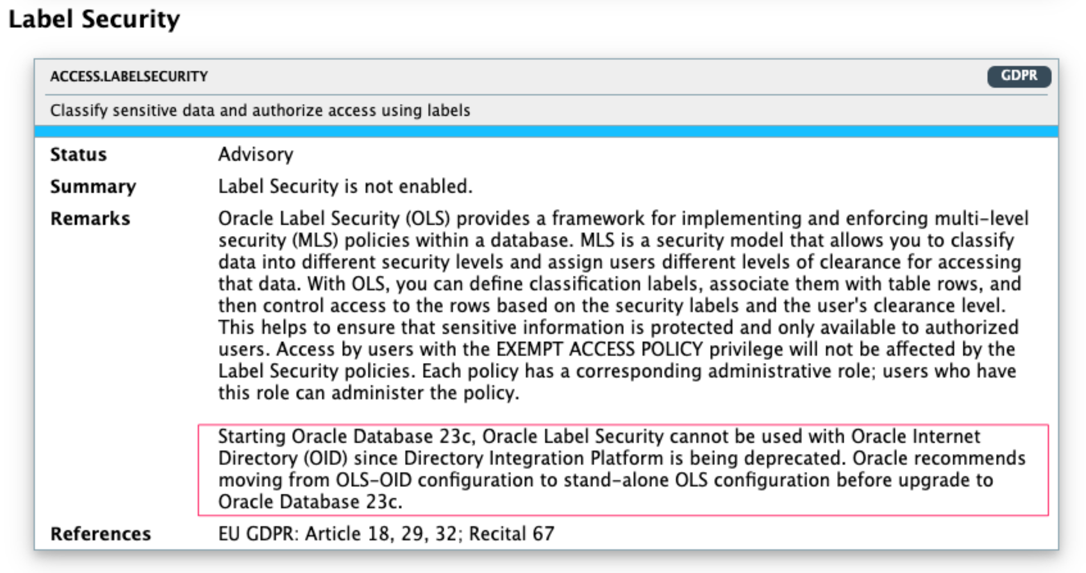
Status	Low Risk
Summary	Found profiles with PASSWORD_ROLLOVER_TIME set for more than 14 days. Found application owner accounts who should expire their password rollover period soon.
Details	Profiles that allow users to gradually rollover their password for more then 14 days: MY_APP_PROFILE (30 days) Application owner accounts who should soon expire their password rollover period: APPSCRP (MY_APP_PROFILE) within the next 14 days.
Remarks	Gradual Password Rollover allows administrators to change application database passwords without having to schedule downtime. Before the gradual password rollover feature, the database administrator needed to take the application down while the database password was being rotated. This was because the password update required changes on both the database and the application side. With gradual database password rollover, the application can continue to use the older password until the new password is configured in the application. To accomplish this, the database administrator can associate a profile having a non-zero limit for the PASSWORD_ROLLOVER_TIME password profile parameter with an application schema. This allows the database password of the application user to be altered while allowing the older password to remain valid for the time specified by the PASSWORD_ROLLOVER_TIME limit. Try to limit the use of this feature to application schemas that need to undergo password maintenance and keep the rollover period to a minimum.
References	Oracle Best Practice

Gradual Password Rollover was introduced in Oracle Database 19c in 2021 but still isn't reflected in STIG or CIS.

Oracle Database 23c *desupport* notices

NEW in 3.0

Desupport notices list database features and parameters that are reaching or have reached their end-of-life so you can take proactive measures to phase out their usage.



Label Security

ACCESS.LABELSECURITY GDPR

Classify sensitive data and authorize access using labels

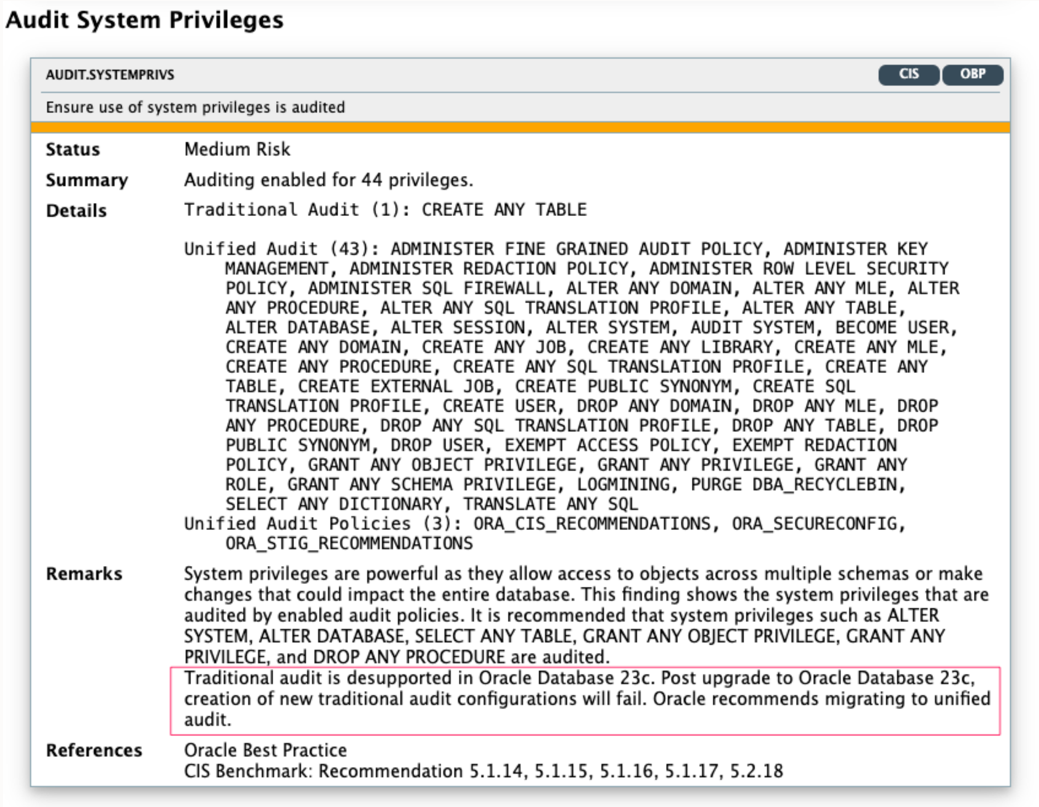
Status Advisory

Summary Label Security is not enabled.

Remarks Oracle Label Security (OLS) provides a framework for implementing and enforcing multi-level security (MLS) policies within a database. MLS is a security model that allows you to classify data into different security levels and assign users different levels of clearance for accessing that data. With OLS, you can define classification labels, associate them with table rows, and then control access to the rows based on the security labels and the user's clearance level. This helps to ensure that sensitive information is protected and only available to authorized users. Access by users with the EXEMPT ACCESS POLICY privilege will not be affected by the Label Security policies. Each policy has a corresponding administrative role; users who have this role can administer the policy.

Starting Oracle Database 23c, Oracle Label Security cannot be used with Oracle Internet Directory (OID) since Directory Integration Platform is being deprecated. Oracle recommends moving from OLS-OID configuration to stand-alone OLS configuration before upgrade to Oracle Database 23c.

References EU GDPR: Article 18, 29, 32; Recital 67



Audit System Privileges

AUDIT.SYSTEMPRIVS CIS OBP

Ensure use of system privileges is audited

Status Medium Risk

Summary Auditing enabled for 44 privileges.

Details

```
Traditional Audit (1): CREATE ANY TABLE

Unified Audit (43): ADMINISTER FINE GRAINED AUDIT POLICY, ADMINISTER KEY
    MANAGEMENT, ADMINISTER REDACTION POLICY, ADMINISTER ROW LEVEL SECURITY
    POLICY, ADMINISTER SQL FIREWALL, ALTER ANY DOMAIN, ALTER ANY MLE, ALTER
    ANY PROCEDURE, ALTER ANY SQL TRANSLATION PROFILE, ALTER ANY TABLE,
    ALTER DATABASE, ALTER SESSION, ALTER SYSTEM, AUDIT SYSTEM, BECOME USER,
    CREATE ANY DOMAIN, CREATE ANY JOB, CREATE ANY LIBRARY, CREATE ANY MLE,
    CREATE ANY PROCEDURE, CREATE ANY SQL TRANSLATION PROFILE, CREATE ANY
    TABLE, CREATE EXTERNAL JOB, CREATE PUBLIC SYNONYM, CREATE SQL
    TRANSLATION PROFILE, CREATE USER, DROP ANY DOMAIN, DROP ANY MLE, DROP
    ANY PROCEDURE, DROP ANY SQL TRANSLATION PROFILE, DROP ANY TABLE, DROP
    PUBLIC SYNONYM, DROP USER, EXEMPT ACCESS POLICY, EXEMPT REDACTION
    POLICY, GRANT ANY OBJECT PRIVILEGE, GRANT ANY PRIVILEGE, GRANT ANY
    ROLE, GRANT ANY SCHEMA PRIVILEGE, LOGMINING, PURGE DBA_RECYCLEBIN,
    SELECT ANY DICTIONARY, TRANSLATE ANY SQL
Unified Audit Policies (3): ORA_CIS_RECOMMENDATIONS, ORA_SECURECONFIG,
    ORA_STIG_RECOMMENDATIONS
```

Remarks System privileges are powerful as they allow access to objects across multiple schemas or make changes that could impact the entire database. This finding shows the system privileges that are audited by enabled audit policies. It is recommended that system privileges such as ALTER SYSTEM, ALTER DATABASE, SELECT ANY TABLE, GRANT ANY OBJECT PRIVILEGE, GRANT ANY PRIVILEGE, and DROP ANY PROCEDURE are audited.

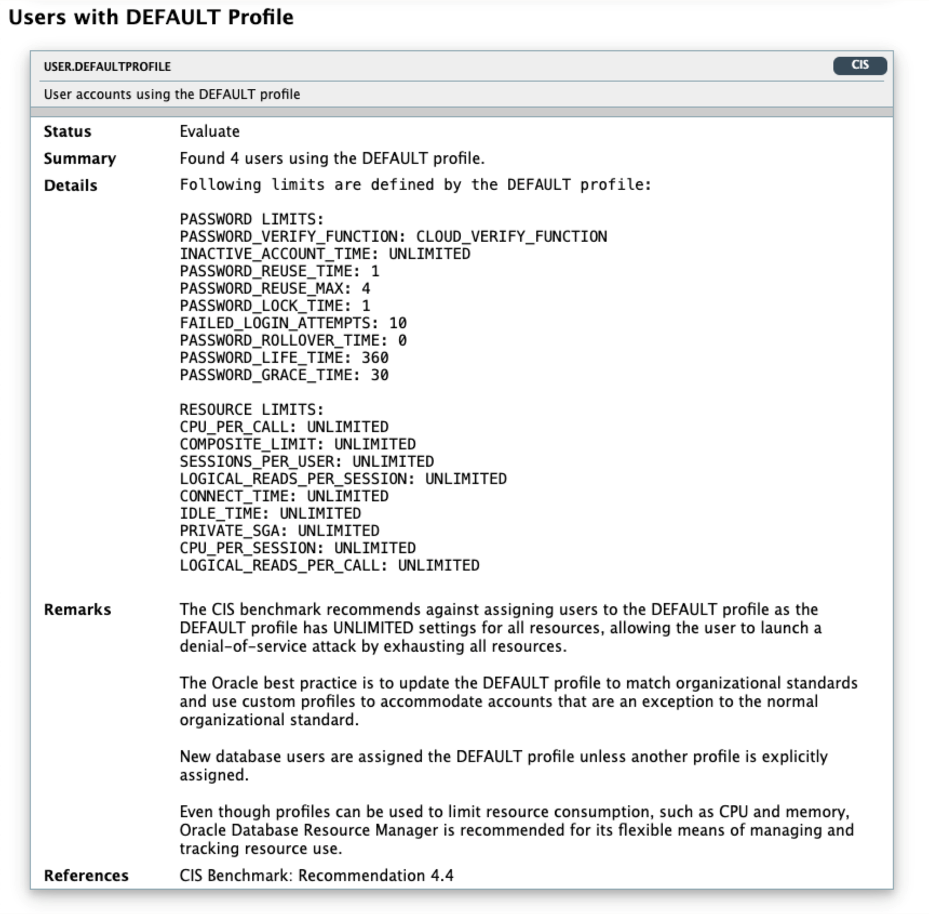
Traditional audit is desupported in Oracle Database 23c. Post upgrade to Oracle Database 23c, creation of new traditional audit configurations will fail. Oracle recommends migrating to unified audit.

References Oracle Best Practice
CIS Benchmark: Recommendation 5.1.14, 5.1.15, 5.1.16, 5.1.17, 5.2.18

CIS findings in DBSAT (1/6)

Sample findings

NEW in 3.1



Users with DEFAULT Profile

USER.DEFAULTPROFILE CIS

User accounts using the DEFAULT profile

Status Evaluate

Summary Found 4 users using the DEFAULT profile.

Details

```
Following limits are defined by the DEFAULT profile:

PASSWORD LIMITS:
PASSWORD_VERIFY_FUNCTION: CLOUD_VERIFY_FUNCTION
INACTIVE_ACCOUNT_TIME: UNLIMITED
PASSWORD_REUSE_TIME: 1
PASSWORD_REUSE_MAX: 4
PASSWORD_LOCK_TIME: 1
FAILED_LOGIN_ATTEMPTS: 10
PASSWORD_ROLLOVER_TIME: 0
PASSWORD_LIFE_TIME: 360
PASSWORD_GRACE_TIME: 30

RESOURCE LIMITS:
CPU_PER_CALL: UNLIMITED
COMPOSITE_LIMIT: UNLIMITED
SESSIONS_PER_USER: UNLIMITED
LOGICAL_READS_PER_SESSION: UNLIMITED
CONNECT_TIME: UNLIMITED
IDLE_TIME: UNLIMITED
PRIVATE_SGA: UNLIMITED
CPU_PER_SESSION: UNLIMITED
LOGICAL_READS_PER_CALL: UNLIMITED
```

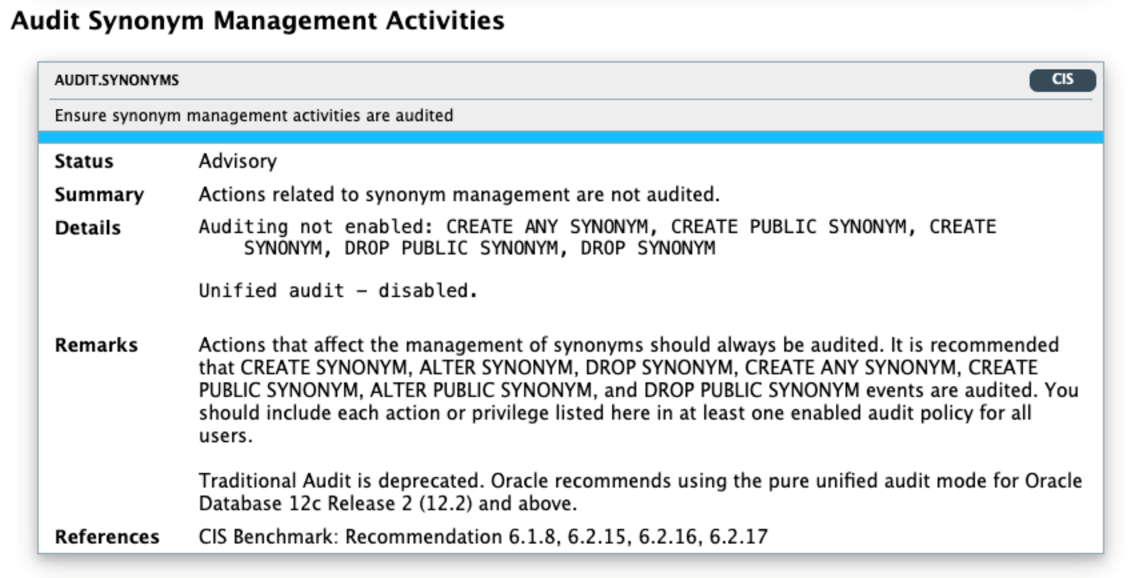
Remarks The CIS benchmark recommends against assigning users to the DEFAULT profile as the DEFAULT profile has UNLIMITED settings for all resources, allowing the user to launch a denial-of-service attack by exhausting all resources.

The Oracle best practice is to update the DEFAULT profile to match organizational standards and use custom profiles to accommodate accounts that are an exception to the normal organizational standard.

New database users are assigned the DEFAULT profile unless another profile is explicitly assigned.

Even though profiles can be used to limit resource consumption, such as CPU and memory, Oracle Database Resource Manager is recommended for its flexible means of managing and tracking resource use.

References CIS Benchmark: Recommendation 4.4



Audit Synonym Management Activities

AUDIT.SYNONYMS CIS

Ensure synonym management activities are audited

Status Advisory

Summary Actions related to synonym management are not audited.

Details

```
Auditing not enabled: CREATE ANY SYNONYM, CREATE PUBLIC SYNONYM, CREATE
    SYNONYM, DROP PUBLIC SYNONYM, DROP SYNONYM

Unified audit - disabled.
```

Remarks Actions that affect the management of synonyms should always be audited. It is recommended that CREATE SYNONYM, ALTER SYNONYM, DROP SYNONYM, CREATE ANY SYNONYM, CREATE PUBLIC SYNONYM, ALTER PUBLIC SYNONYM, and DROP PUBLIC SYNONYM events are audited. You should include each action or privilege listed here in at least one enabled audit policy for all users.

Traditional Audit is deprecated. Oracle recommends using the pure unified audit mode for Oracle Database 12c Release 2 (12.2) and above.

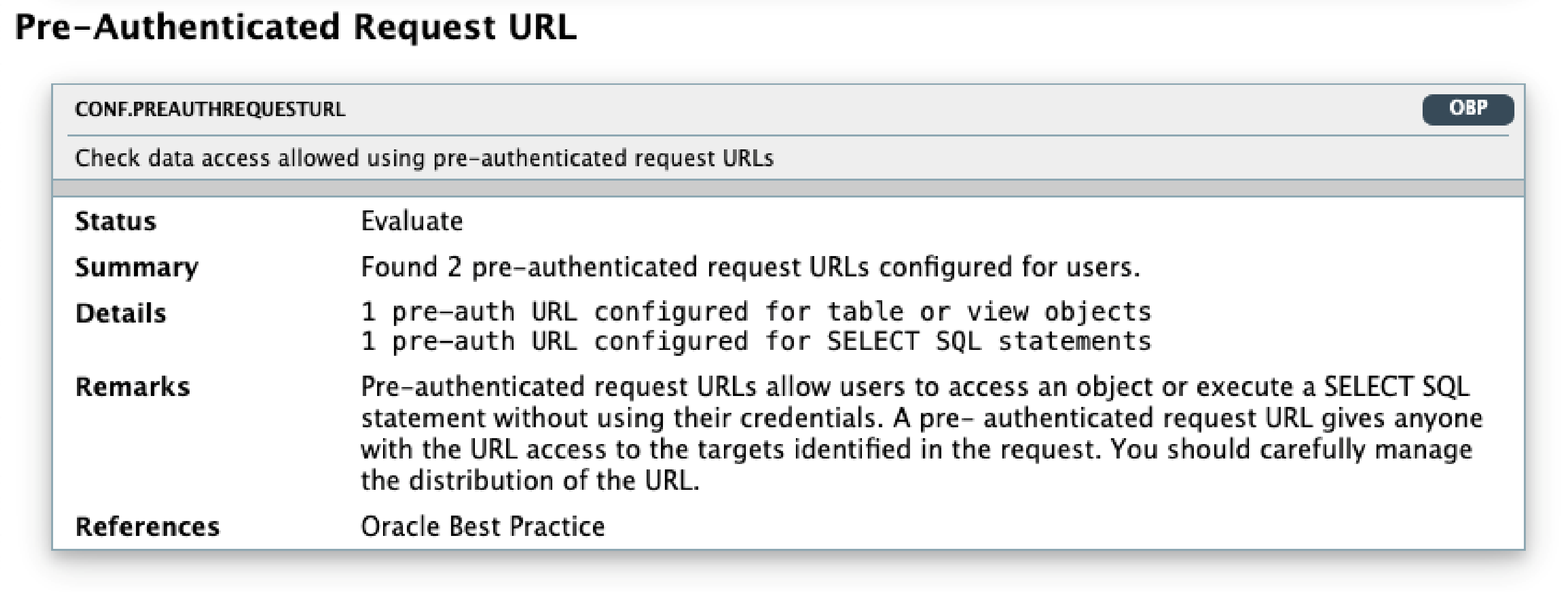
References CIS Benchmark: Recommendation 6.1.8, 6.2.15, 6.2.16, 6.2.17

CIS findings in DBSAT (2/6)

Sample findings

NEW in 3.1

Only for Autonomous Database Serverless targets



Pre-Authenticated Request URL

CONF.PREAUTHREQUESTURL — OBP

Check data access allowed using pre-authenticated request URLs

Status	Evaluate
Summary	Found 2 pre-authenticated request URLs configured for users.

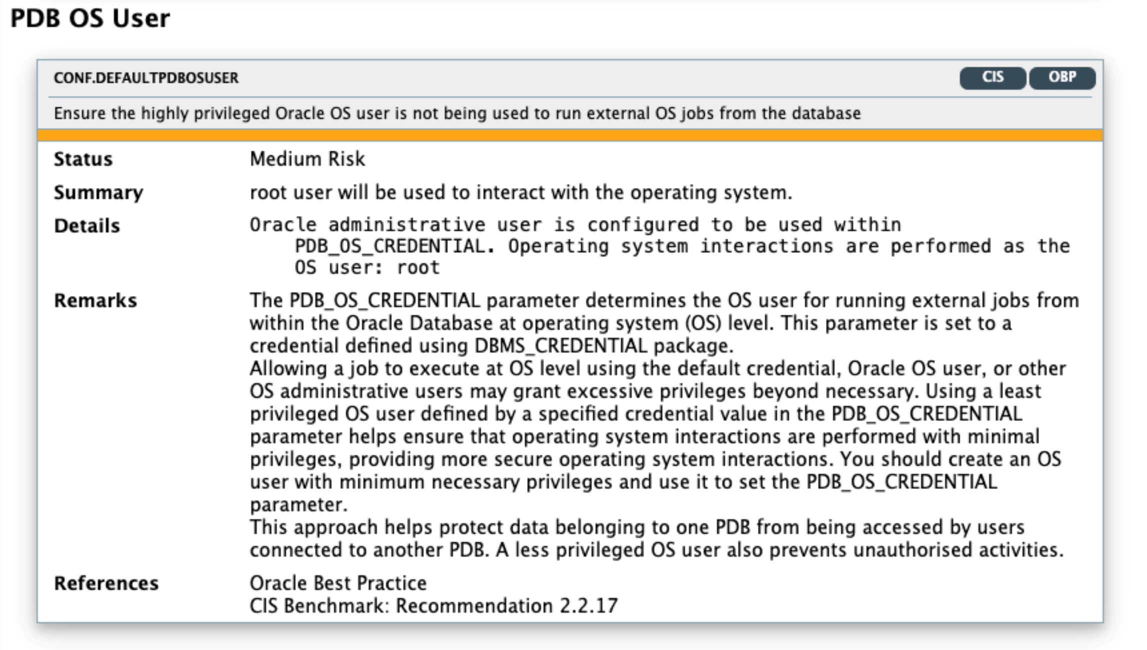
Details	`1 pre-auth URL configured for table or view objects`
	`1 pre-auth URL configured for SELECT SQL statements`

Remarks	Pre-authenticated request URLs allow users to access an object or execute a SELECT SQL statement without using their credentials. A pre- authenticated request URL gives anyone with the URL access to the targets identified in the request. You should carefully manage the distribution of the URL.
References	Oracle Best Practice

CIS findings in DBSAT (3/6)

Sample findings

NEW in 3.1



PDB OS User

CONF.DEFAULTPDBOSUSER

Ensure the highly privileged Oracle OS user is not being used to run external OS jobs from the database

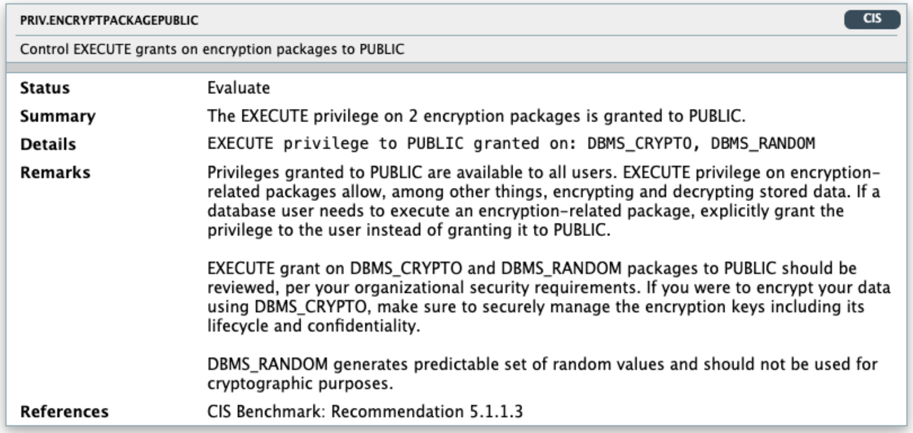
Status	Medium Risk
Summary	root user will be used to interact with the operating system.
Details	Oracle administrative user is configured to be used within PDB_OS_CREDENTIAL. Operating system interactions are performed as the OS user: root
Remarks	The PDB_OS_CREDENTIAL parameter determines the OS user for running external jobs from within the Oracle Database at operating system (OS) level. This parameter is set to a credential defined using DBMS_CREDENTIAL package. Allowing a job to execute at OS level using the default credential, Oracle OS user, or other OS administrative users may grant excessive privileges beyond necessary. Using a least privileged OS user defined by a specified credential value in the PDB_OS_CREDENTIAL parameter helps ensure that operating system interactions are performed with minimal privileges, providing more secure operating system interactions. You should create an OS user with minimum necessary privileges and use it to set the PDB_OS_CREDENTIAL parameter. This approach helps protect data belonging to one PDB from being accessed by users connected to another PDB. A less privileged OS user also prevents unauthorised activities.
References	Oracle Best Practice CIS Benchmark: Recommendation 2.2.17

CIS findings in DBSAT – Grants to PUBLIC (4/6)

Sample findings

NEW in 3.1

Encryption Packages Granted to PUBLIC



PRIV.ENCRYPTPACKAGEPUBLIC CIS

Control EXECUTE grants on encryption packages to PUBLIC

Status Evaluate

Summary The EXECUTE privilege on 2 encryption packages is granted to PUBLIC.

Details

```
EXECUTE privilege to PUBLIC granted on: DBMS_CRYPTO, DBMS_RANDOM
```

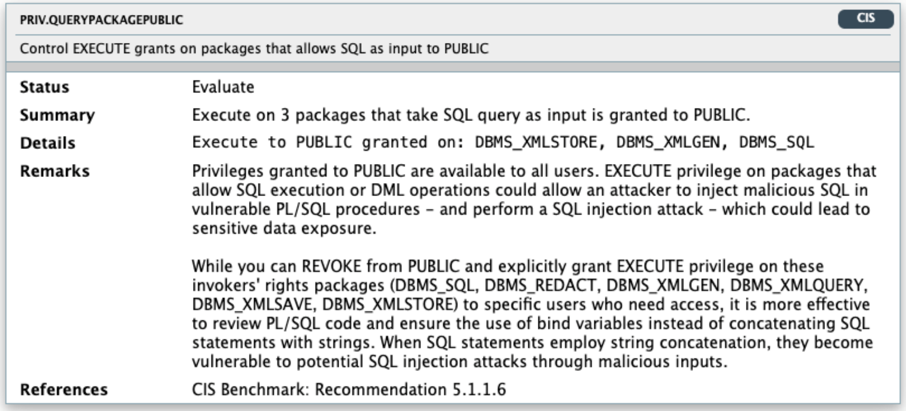
Remarks Privileges granted to PUBLIC are available to all users. EXECUTE privilege on encryption-related packages allow, among other things, encrypting and decrypting stored data. If a database user needs to execute an encryption-related package, explicitly grant the privilege to the user instead of granting it to PUBLIC.

EXECUTE grant on DBMS_CRYPTO and DBMS_RANDOM packages to PUBLIC should be reviewed, per your organizational security requirements. If you were to encrypt your data using DBMS_CRYPTO, make sure to securely manage the encryption keys including its lifecycle and confidentiality.

DBMS_RANDOM generates predictable set of random values and should not be used for cryptographic purposes.

References CIS Benchmark: Recommendation 5.1.1.3

SQL Packages Granted to PUBLIC



PRIV.QUERYPACKAGEPUBLIC CIS

Control EXECUTE grants on packages that allows SQL as input to PUBLIC

Status Evaluate

Summary Execute on 3 packages that take SQL query as input is granted to PUBLIC.

Details

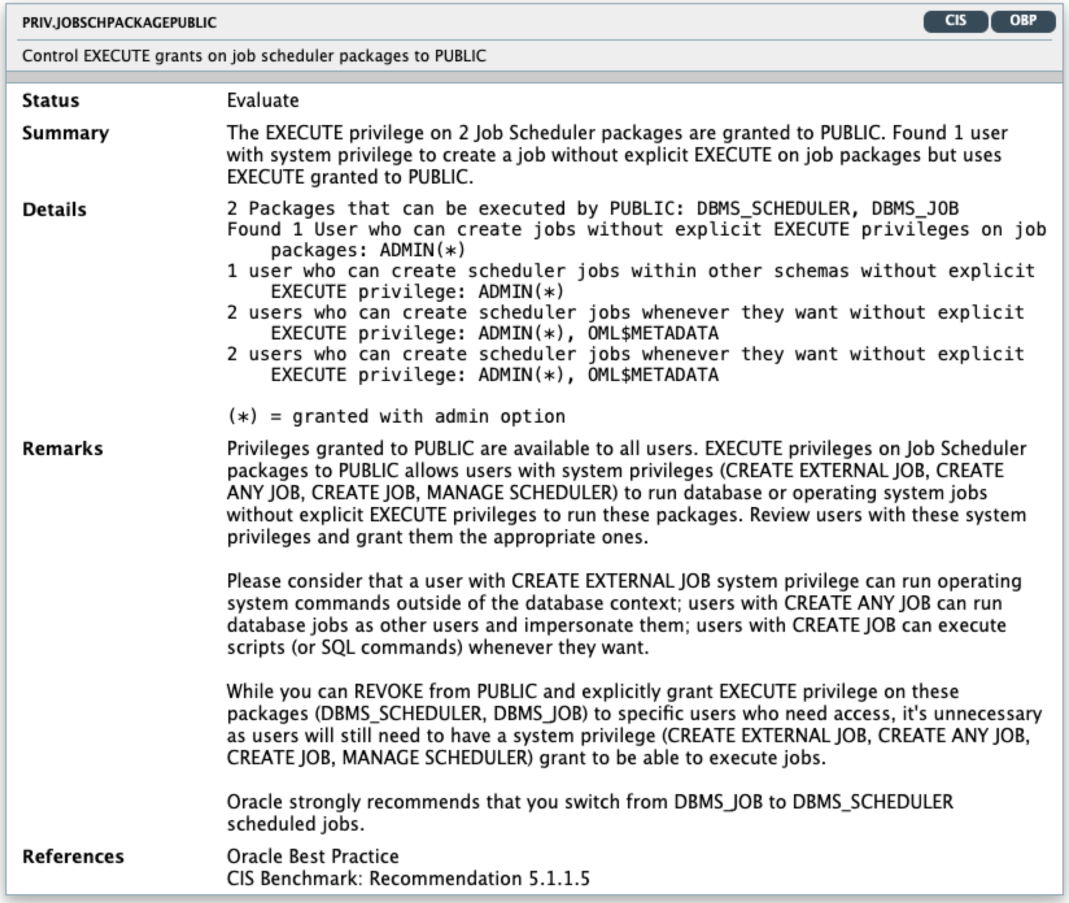
```
Execute to PUBLIC granted on: DBMS_XMLSTORE, DBMS_XMLGEN, DBMS_SQL
```

Remarks Privileges granted to PUBLIC are available to all users. EXECUTE privilege on packages that allow SQL execution or DML operations could allow an attacker to inject malicious SQL in vulnerable PL/SQL procedures - and perform a SQL injection attack - which could lead to sensitive data exposure.

While you can REVOKE from PUBLIC and explicitly grant EXECUTE privilege on these invokers' rights packages (DBMS_SQL, DBMS_REDACT, DBMS_XMLGEN, DBMS_XMLQUERY, DBMS_XMLSAVE, DBMS_XMLSTORE) to specific users who need access, it is more effective to review PL/SQL code and ensure the use of bind variables instead of concatenating SQL statements with strings. When SQL statements employ string concatenation, they become vulnerable to potential SQL injection attacks through malicious inputs.

References CIS Benchmark: Recommendation 5.1.1.6

Scheduler Job Packages Granted to PUBLIC



PRIV.JOBSCHPACKAGEPUBLIC CIS OBP

Control EXECUTE grants on job scheduler packages to PUBLIC

Status Evaluate

Summary The EXECUTE privilege on 2 Job Scheduler packages are granted to PUBLIC. Found 1 user with system privilege to create a job without explicit EXECUTE on job packages but uses EXECUTE granted to PUBLIC.

Details

```
2 Packages that can be executed by PUBLIC: DBMS_SCHEDULER, DBMS_JOB
Found 1 User who can create jobs without explicit EXECUTE privileges on job
    packages: ADMIN(*)
1 user who can create scheduler jobs within other schemas without explicit
    EXECUTE privilege: ADMIN(*)
2 users who can create scheduler jobs whenever they want without explicit
    EXECUTE privilege: ADMIN(*), OML$METADATA
2 users who can create scheduler jobs whenever they want without explicit
    EXECUTE privilege: ADMIN(*), OML$METADATA

(*) = granted with admin option
```

Remarks Privileges granted to PUBLIC are available to all users. EXECUTE privileges on Job Scheduler packages to PUBLIC allows users with system privileges (CREATE EXTERNAL JOB, CREATE ANY JOB, CREATE JOB, MANAGE SCHEDULER) to run database or operating system jobs without explicit EXECUTE privileges to run these packages. Review users with these system privileges and grant them the appropriate ones.

Please consider that a user with CREATE EXTERNAL JOB system privilege can run operating system commands outside of the database context; users with CREATE ANY JOB can run database jobs as other users and impersonate them; users with CREATE JOB can execute scripts (or SQL commands) whenever they want.

While you can REVOKE from PUBLIC and explicitly grant EXECUTE privilege on these packages (DBMS_SCHEDULER, DBMS_JOB) to specific users who need access, it's unnecessary as users will still need to have a system privilege (CREATE EXTERNAL JOB, CREATE ANY JOB, CREATE JOB, MANAGE SCHEDULER) grant to be able to execute jobs.

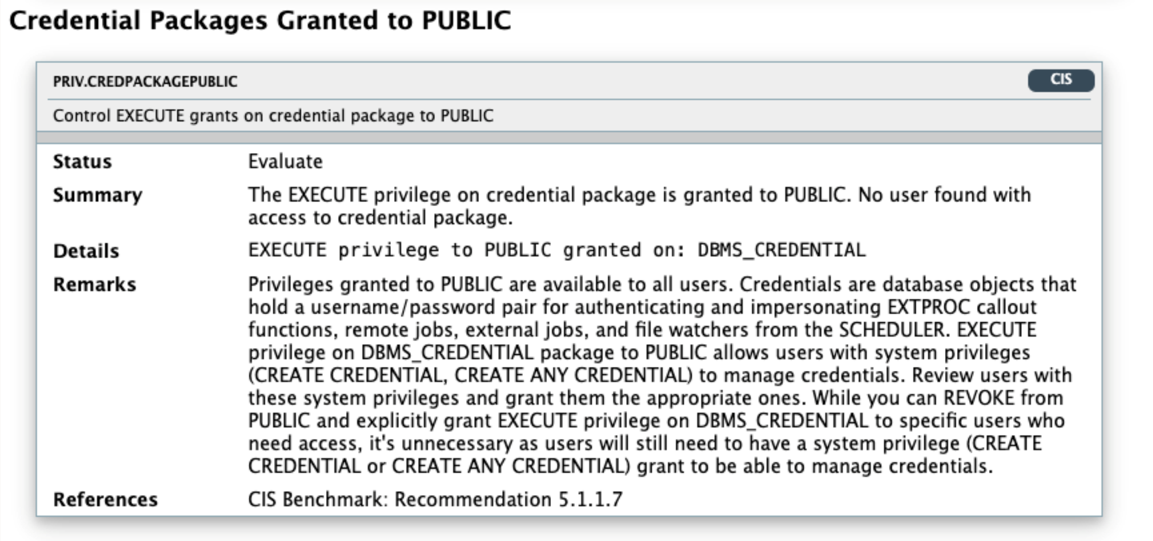
Oracle strongly recommends that you switch from DBMS_JOB to DBMS_SCHEDULER scheduled jobs.

References Oracle Best Practice
CIS Benchmark: Recommendation 5.1.1.5

CIS findings in DBSAT – Grants to PUBLIC (5/6)

Sample findings

NEW in 3.1



Credential Packages Granted to PUBLIC

PRIV.CREDPACKAGEPUBLIC CIS

Control EXECUTE grants on credential package to PUBLIC

Status Evaluate

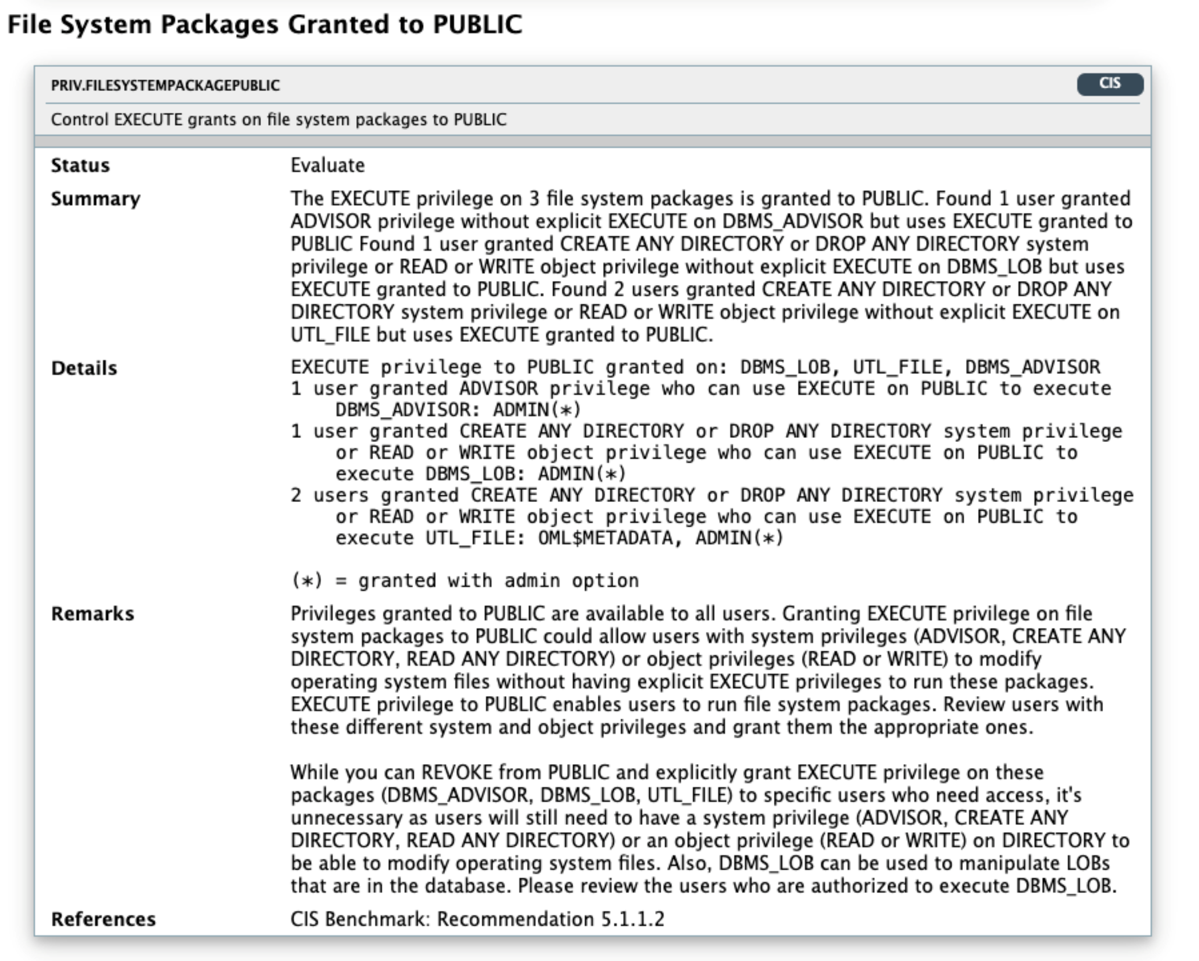
Summary The EXECUTE privilege on credential package is granted to PUBLIC. No user found with access to credential package.

Details

```
EXECUTE privilege to PUBLIC granted on: DBMS_CREDENTIAL
```

Remarks Privileges granted to PUBLIC are available to all users. Credentials are database objects that hold a username/password pair for authenticating and impersonating EXTPROC callout functions, remote jobs, external jobs, and file watchers from the SCHEDULER. EXECUTE privilege on DBMS_CREDENTIAL package to PUBLIC allows users with system privileges (CREATE CREDENTIAL, CREATE ANY CREDENTIAL) to manage credentials. Review users with these system privileges and grant them the appropriate ones. While you can REVOKE from PUBLIC and explicitly grant EXECUTE privilege on DBMS_CREDENTIAL to specific users who need access, it's unnecessary as users will still need to have a system privilege (CREATE CREDENTIAL or CREATE ANY CREDENTIAL) grant to be able to manage credentials.

References CIS Benchmark: Recommendation 5.1.1.7



File System Packages Granted to PUBLIC

PRIV.FILESYSTEMPACKAGEPUBLIC CIS

Control EXECUTE grants on file system packages to PUBLIC

Status Evaluate

Summary The EXECUTE privilege on 3 file system packages is granted to PUBLIC. Found 1 user granted ADVISOR privilege without explicit EXECUTE on DBMS_ADVISOR but uses EXECUTE granted to PUBLIC Found 1 user granted CREATE ANY DIRECTORY or DROP ANY DIRECTORY system privilege or READ or WRITE object privilege without explicit EXECUTE on DBMS_LOB but uses EXECUTE granted to PUBLIC. Found 2 users granted CREATE ANY DIRECTORY or DROP ANY DIRECTORY system privilege or READ or WRITE object privilege without explicit EXECUTE on UTL_FILE but uses EXECUTE granted to PUBLIC.

Details

```
EXECUTE privilege to PUBLIC granted on: DBMS_LOB, UTL_FILE, DBMS_ADVISOR
1 user granted ADVISOR privilege who can use EXECUTE on PUBLIC to execute
    DBMS_ADVISOR: ADMIN(*)
1 user granted CREATE ANY DIRECTORY or DROP ANY DIRECTORY system privilege
    or READ or WRITE object privilege who can use EXECUTE on PUBLIC to
    execute DBMS_LOB: ADMIN(*)
2 users granted CREATE ANY DIRECTORY or DROP ANY DIRECTORY system privilege
    or READ or WRITE object privilege who can use EXECUTE on PUBLIC to
    execute UTL_FILE: OML$METADATA, ADMIN(*)

(*) = granted with admin option
```

Remarks Privileges granted to PUBLIC are available to all users. Granting EXECUTE privilege on file system packages to PUBLIC could allow users with system privileges (ADVISOR, CREATE ANY DIRECTORY, READ ANY DIRECTORY) or object privileges (READ or WRITE) to modify operating system files without having explicit EXECUTE privileges to run these packages. EXECUTE privilege to PUBLIC enables users to run file system packages. Review users with these different system and object privileges and grant them the appropriate ones.

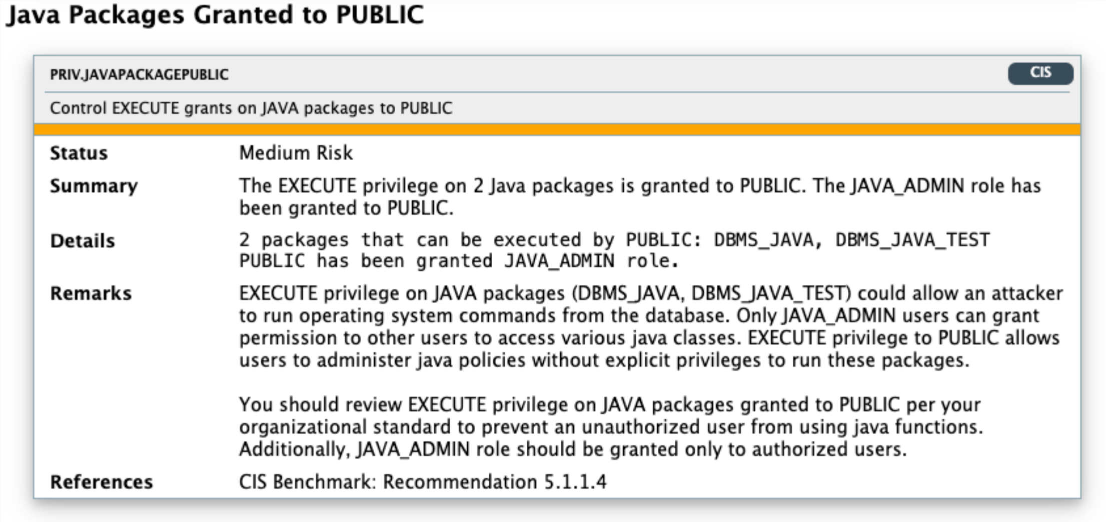
While you can REVOKE from PUBLIC and explicitly grant EXECUTE privilege on these packages (DBMS_ADVISOR, DBMS_LOB, UTL_FILE) to specific users who need access, it's unnecessary as users will still need to have a system privilege (ADVISOR, CREATE ANY DIRECTORY, READ ANY DIRECTORY) or an object privilege (READ or WRITE) on DIRECTORY to be able to modify operating system files. Also, DBMS_LOB can be used to manipulate LOBs that are in the database. Please review the users who are authorized to execute DBMS_LOB.

References CIS Benchmark: Recommendation 5.1.1.2

CIS findings in DBSAT – Grants to PUBLIC (6/6)

Sample findings

NEW in 3.1



Java Packages Granted to PUBLIC

PRIV.JAVAPACKAGEPUBLIC — CIS

Control EXECUTE grants on JAVA packages to PUBLIC

Status Medium Risk

Summary The EXECUTE privilege on 2 Java packages is granted to PUBLIC. The JAVA_ADMIN role has been granted to PUBLIC.

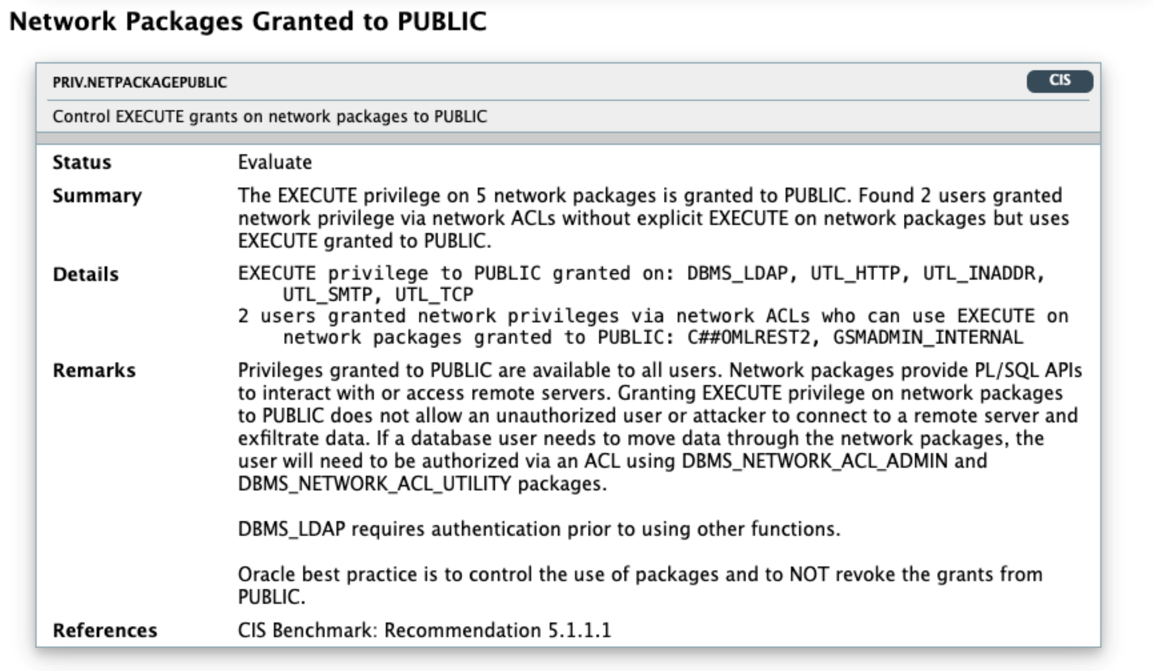
Details

```
2 packages that can be executed by PUBLIC: DBMS_JAVA, DBMS_JAVA_TEST
PUBLIC has been granted JAVA_ADMIN role.
```

Remarks EXECUTE privilege on JAVA packages (DBMS_JAVA, DBMS_JAVA_TEST) could allow an attacker to run operating system commands from the database. Only JAVA_ADMIN users can grant permission to other users to access various java classes. EXECUTE privilege to PUBLIC allows users to administer java policies without explicit privileges to run these packages.

You should review EXECUTE privilege on JAVA packages granted to PUBLIC per your organizational standard to prevent an unauthorized user from using java functions. Additionally, JAVA_ADMIN role should be granted only to authorized users.

References CIS Benchmark: Recommendation 5.1.1.4



Network Packages Granted to PUBLIC

PRIV.NETPACKAGEPUBLIC — CIS

Control EXECUTE grants on network packages to PUBLIC

Status Evaluate

Summary The EXECUTE privilege on 5 network packages is granted to PUBLIC. Found 2 users granted network privilege via network ACLs without explicit EXECUTE on network packages but uses EXECUTE granted to PUBLIC.

Details

```
EXECUTE privilege to PUBLIC granted on: DBMS_LDAP, UTL_HTTP, UTL_INADDR,
    UTL_SMTP, UTL_TCP
2 users granted network privileges via network ACLs who can use EXECUTE on
    network packages granted to PUBLIC: C##OMLREST2, GSMADMIN_INTERNAL
```

Remarks Privileges granted to PUBLIC are available to all users. Network packages provide PL/SQL APIs to interact with or access remote servers. Granting EXECUTE privilege on network packages to PUBLIC does not allow an unauthorized user or attacker to connect to a remote server and exfiltrate data. If a database user needs to move data through the network packages, the user will need to be authorized via an ACL using DBMS_NETWORK_ACL_ADMIN and DBMS_NETWORK_ACL_UTILITY packages.

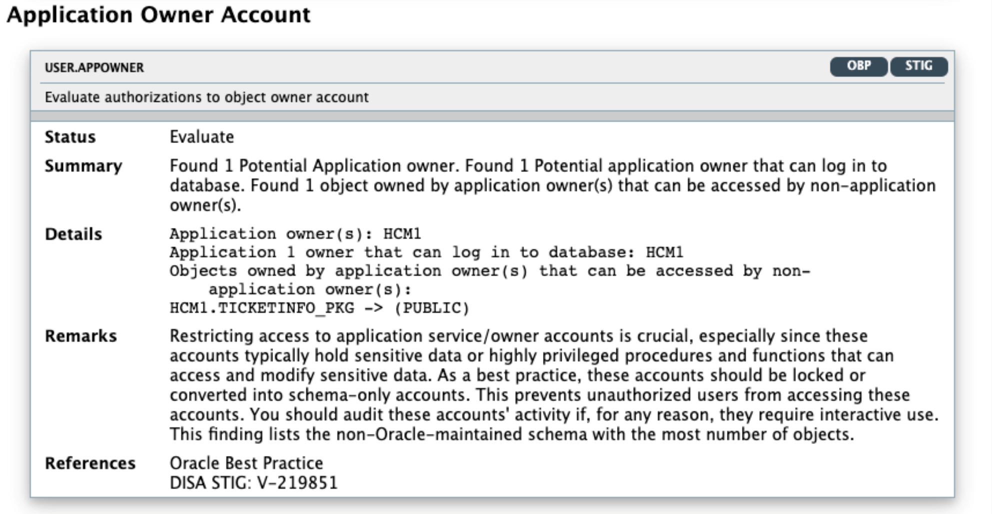
DBMS_LDAP requires authentication prior to using other functions.

Oracle best practice is to control the use of packages and to NOT revoke the grants from PUBLIC.

References CIS Benchmark: Recommendation 5.1.1.1

STIG findings

Sample findings



Application Owner Account

USER.APPOWNER OBP STIG

Evaluate authorizations to object owner account

Status Evaluate

Summary Found 1 Potential Application owner. Found 1 Potential application owner that can log in to database. Found 1 object owned by application owner(s) that can be accessed by non-application owner(s).

Details

```
Application owner(s): HCM1
Application 1 owner that can log in to database: HCM1
Objects owned by application owner(s) that can be accessed by non-
    application owner(s):
HCM1.TICKETINFO_PKG -> (PUBLIC)
```

Remarks Restricting access to application service/owner accounts is crucial, especially since these accounts typically hold sensitive data or highly privileged procedures and functions that can access and modify sensitive data. As a best practice, these accounts should be locked or converted into schema-only accounts. This prevents unauthorized users from accessing these accounts. You should audit these accounts' activity if, for any reason, they require interactive use. This finding lists the non-Oracle-maintained schema with the most number of objects.

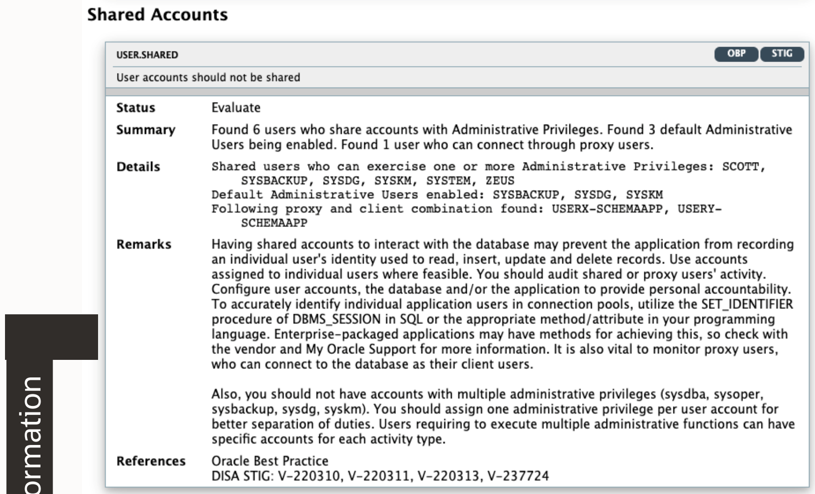
References Oracle Best Practice
DISA STIG: V-219851

- Top user from non Oracle-maintained accounts that own objects

Enhanced in 3.1

Reduced details to list only 10 users that can access app owner objects, resulting in improved performance and smaller, more manageable reports.

NEW in 3.0



Shared Accounts

USER.SHARED OBP STIG

User accounts should not be shared

Status Evaluate

Summary Found 6 users who share accounts with Administrative Privileges. Found 3 default Administrative Users being enabled. Found 1 user who can connect through proxy users.

Details

```
Shared users who can exercise one or more Administrative Privileges: SCOTT,
    SYSBACKUP, SYSDG, SYSKM, SYSTEM, ZEUS
Default Administrative Users enabled: SYSBACKUP, SYSDG, SYSKM
Following proxy and client combination found: USERX-SCHEMAAPP, USERY-
    SCHEMAAPP
```

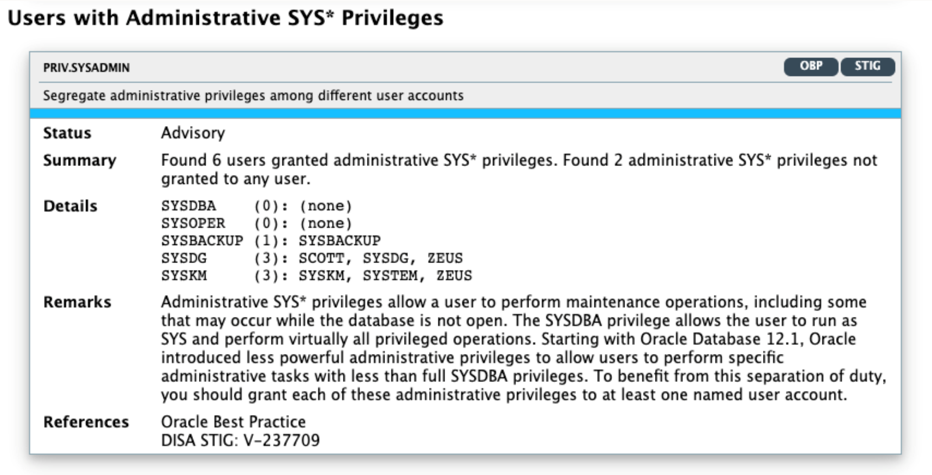
Remarks Having shared accounts to interact with the database may prevent the application from recording an individual user's identity used to read, insert, update and delete records. Use accounts assigned to individual users where feasible. You should audit shared or proxy users' activity. Configure user accounts, the database and/or the application to provide personal accountability. To accurately identify individual application users in connection pools, utilize the SET_IDENTIFIER procedure of DBMS_SESSION in SQL or the appropriate method/attribute in your programming language. Enterprise-packaged applications may have methods for achieving this, so check with the vendor and My Oracle Support for more information. It is also vital to monitor proxy users, who can connect to the database as their client users.

Also, you should not have accounts with multiple administrative privileges (sysdba, sysoper, sysbackup, sysdg, syskm). You should assign one administrative privilege per user account for better separation of duties. Users requiring to execute multiple administrative functions can have specific accounts for each activity type.

References Oracle Best Practice
DISA STIG: V-220310, V-220311, V-220313, V-237724

- Possible shared accounts, including proxy users

More Information



Users with Administrative SYS* Privileges

PRIV.SYSADMIN OBP STIG

Segregate administrative privileges among different user accounts

Status Advisory

Summary Found 6 users granted administrative SYS* privileges. Found 2 administrative SYS* privileges not granted to any user.

Details

```
SYSDBA     (0): (none)
SYSOPER    (0): (none)
SYSBACKUP (1): SYSBACKUP
SYSDG      (3): SCOTT, SYSDG, ZEUS
SYSKM      (3): SYSKM, SYSTEM, ZEUS
```

Remarks Administrative SYS* privileges allow a user to perform maintenance operations, including some that may occur while the database is not open. The SYSDBA privilege allows the user to run as SYS and perform virtually all privileged operations. Starting with Oracle Database 12.1, Oracle introduced less powerful administrative privileges to allow users to perform specific administrative tasks with less than full SYSDBA privileges. To benefit from this separation of duty, you should grant each of these administrative privileges to at least one named user account.

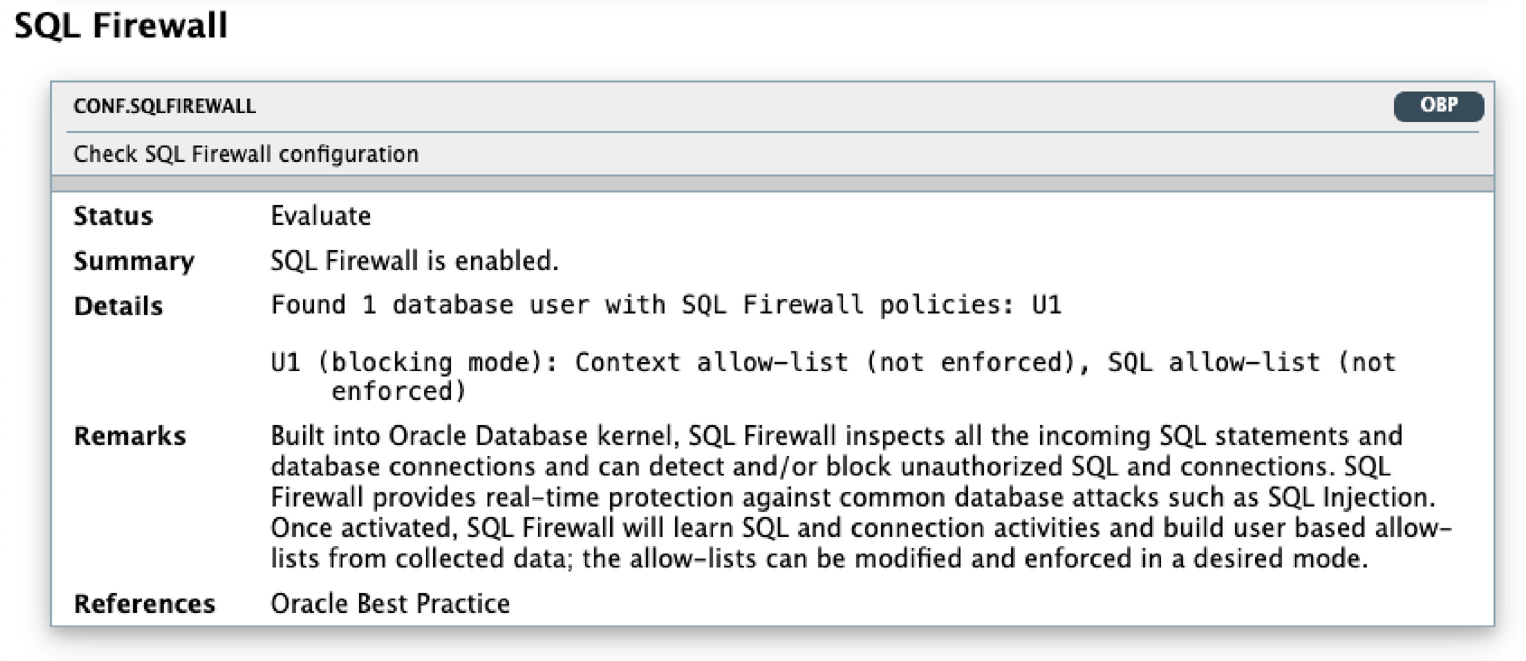
References Oracle Best Practice
DISA STIG: V-237709

- Users with multiple administrative privs – this might compromise SoD

Oracle Database 23c SQL Firewall finding

Sample finding

NEW in 3.0



SQL Firewall

CONF.SQLFIREWALL

Check SQL Firewall configuration

Status	Evaluate
Summary	SQL Firewall is enabled.
Details	Found 1 database user with SQL Firewall policies: U1 U1 (blocking mode): Context allow-list (not enforced), SQL allow-list (not enforced)
Remarks	Built into Oracle Database kernel, SQL Firewall inspects all the incoming SQL statements and database connections and can detect and/or block unauthorized SQL and connections. SQL Firewall provides real-time protection against common database attacks such as SQL Injection. Once activated, SQL Firewall will learn SQL and connection activities and build user based allow-lists from collected data; the allow-lists can be modified and enforced in a desired mode.
References	Oracle Best Practice

How can DBSAT Help?

Assess your database security before hackers come knocking

Know Your Overall Database Security Posture

Know Your Users, Roles, and Privileges

Know Your Sensitive Data

How to Get Started?

Quick & Simple!

3-Step flow

1 Run
./dbsat collect

2 Run
./dbsat report

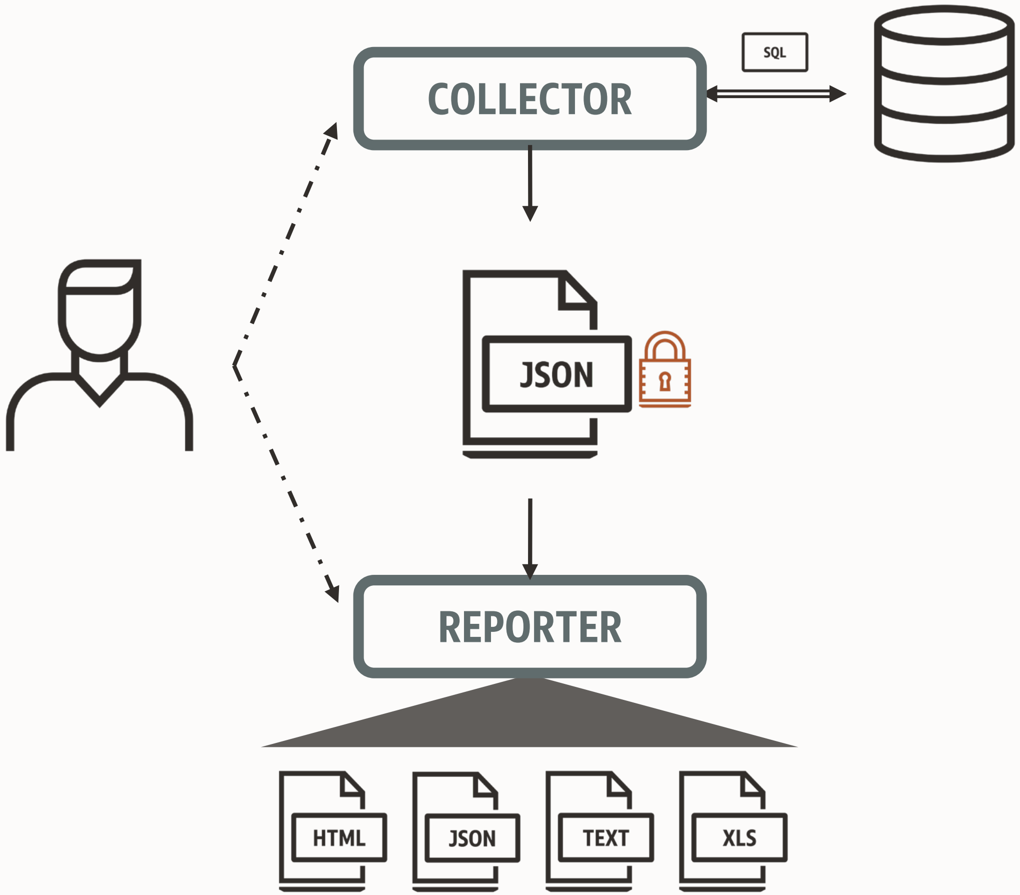
3 Run
./dbsat discover

ORACLE

Collector & Reporter

Collects metadata information on users, roles, privileges, security configuration, and policies in place. Generates a Security Assessment report.

- **Generates summary output with prioritized findings**
  Summary table with identified risks organized by domains: Basic information, user accounts, privileges and roles, authorization control, fine-grained access control, auditing, encryption, config, etc.
- **Over 120 detailed findings with remarks**
  Each finding contains a one line explanation of what is expected, a risk level, details, and remarks on best practices.
- **References to Oracle Best Practices, CIS Benchmark, STIG Rules and GDPR articles/recitals**
  Along with Oracle Database security development organization best practices, there is a mapping to CIS, STIG rules, and EU GDPR articles and recitals.



Discoverer

Scan column names and comments metadata to discover sensitive data. Generates a Sensitive Data Assessment report.

- **Discovers sensitive data**

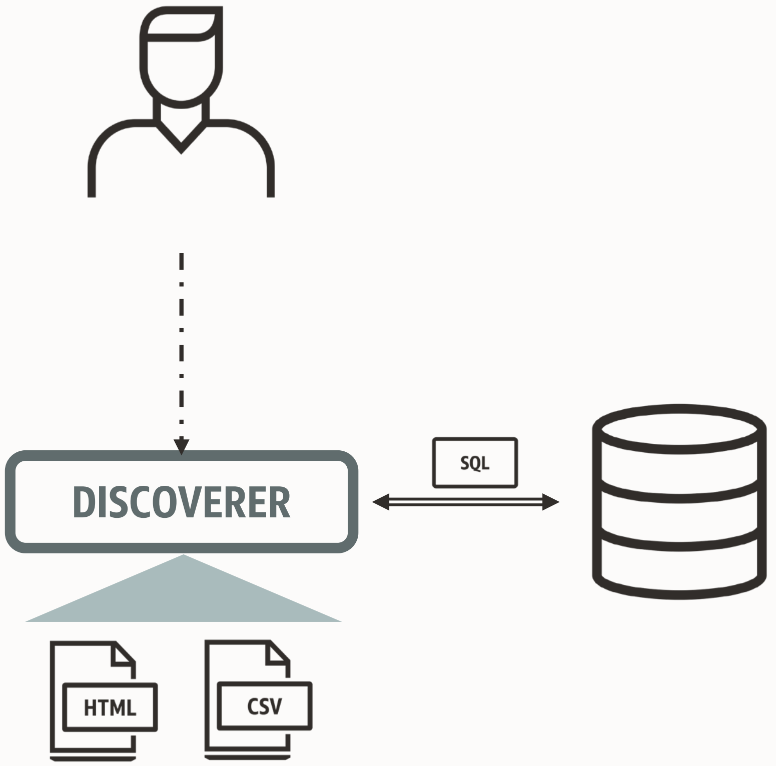
  Get summary and details on Sensitive Data Categories and Types (125+), tables, columns, rows, and risk levels.

- **Provides recommendations on security controls**

  Get recommendations on which security controls to put in place to protect your sensitive data.

- **Customizable**

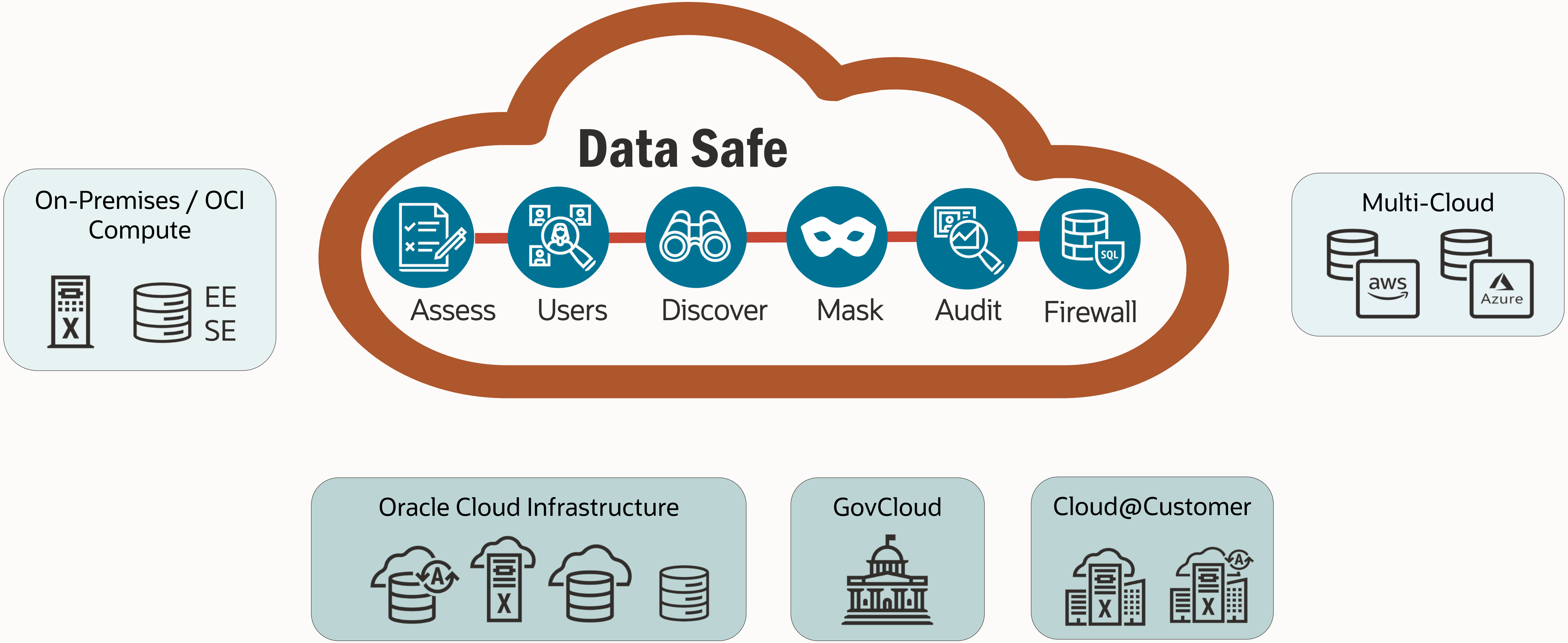
  Leverage the existing sample files to expand or adapt to your specific needs.



What else?

Periodic scheduled assessments, baselining, assessment history, drift report, user risk assessment

Data Safe helps secure Oracle database targets everywhere



Database Security Assessment

Instant feedback on configurations that may introduce unnecessary risk

Comprehensive assessment

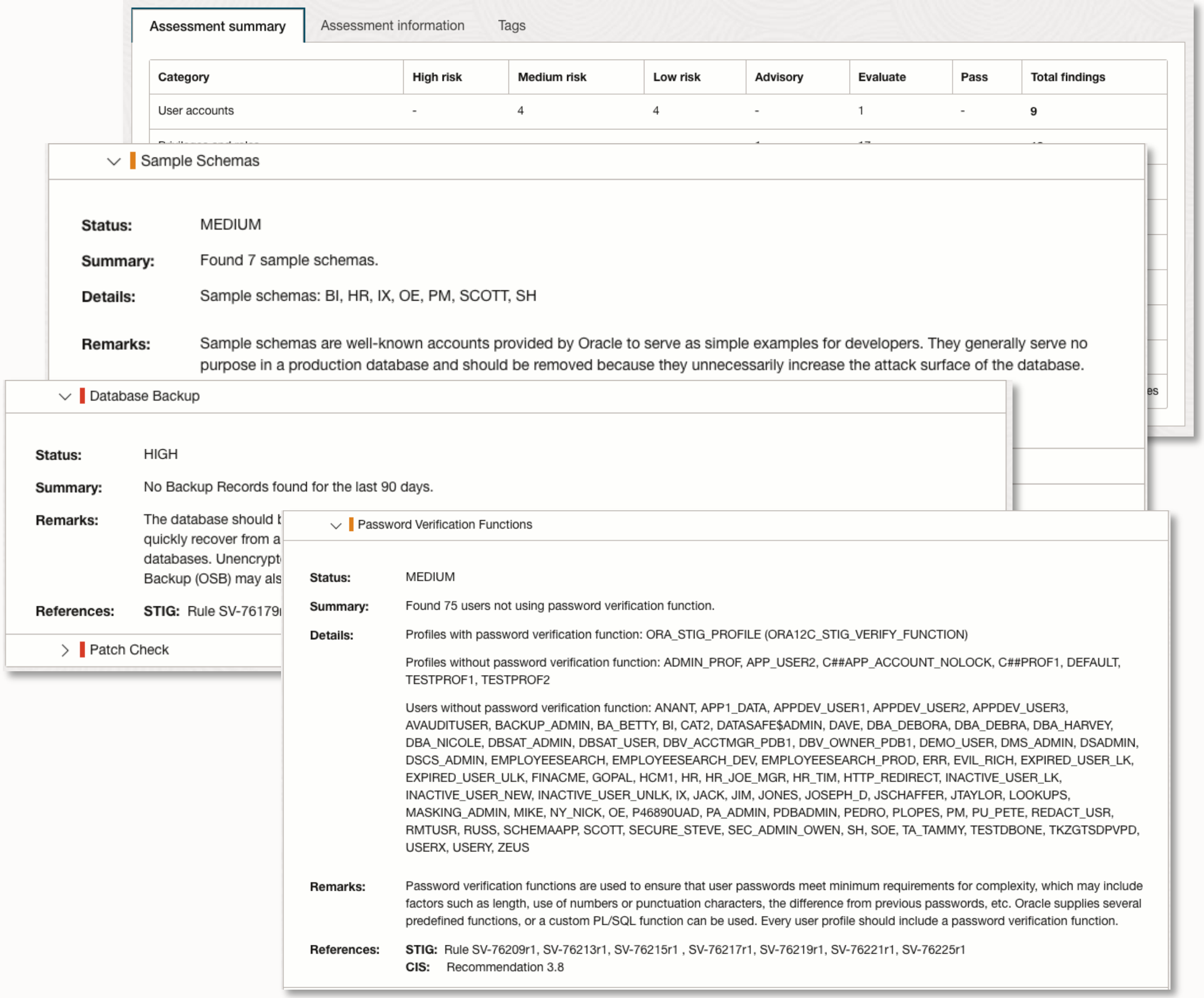
- Security parameters
- Security controls in use
- User Roles and Privileges

Identify drift from best practices

- Set baselines
- Comparison reports
- Events and Notifications
- Assessment history
- Defer risks / change risk level
- Top 5 common control deficiencies

Actionable reports

- Prioritized recommendations
- Compliance mappings & filtering (GDPR, STIG, CIS)



Category	High risk	Medium risk	Low risk	Advisory	Evaluate	Pass	Total findings
User accounts	-	4	4	-	1	-	**9**

Sample Schemas

Status: MEDIUM

Summary: Found 7 sample schemas.

Details: Sample schemas: BI, HR, IX, OE, PM, SCOTT, SH

Remarks: Sample schemas are well-known accounts provided by Oracle to serve as simple examples for developers. They generally serve no purpose in a production database and should be removed because they unnecessarily increase the attack surface of the database.

Database Backup

Status: HIGH

Summary: No Backup Records found for the last 90 days.

Remarks: The database should b
quickly recover from a
databases. Unencrypt
Backup (OSB) may als

References: **STIG:** Rule SV-76179r

Patch Check

Password Verification Functions

Status: MEDIUM

Summary: Found 75 users not using password verification function.

Details: Profiles with password verification function: ORA_STIG_PROFILE (ORA12C_STIG_VERIFY_FUNCTION)

Profiles without password verification function: ADMIN_PROF, APP_USER2, C##APP_ACCOUNT_NOLOCK, C##PROF1, DEFAULT, TESTPROF1, TESTPROF2

Users without password verification function: ANANT, APP1_DATA, APPDEV_USER1, APPDEV_USER2, APPDEV_USER3, AVAUDITUSER, BACKUP_ADMIN, BA_BETTY, BI, CAT2, DATASAFE$ADMIN, DAVE, DBA_DEBORA, DBA_DEBRA, DBA_HARVEY, DBA_NICOLE, DBSAT_ADMIN, DBSAT_USER, DBV_ACCTMGR_PDB1, DBV_OWNER_PDB1, DEMO_USER, DMS_ADMIN, DSADMIN, DSCS_ADMIN, EMPLOYEESEARCH, EMPLOYEESEARCH_DEV, EMPLOYEESEARCH_PROD, ERR, EVIL_RICH, EXPIRED_USER_LK, EXPIRED_USER_ULK, FINACME, GOPAL, HCM1, HR, HR_JOE_MGR, HR_TIM, HTTP_REDIRECT, INACTIVE_USER_LK, INACTIVE_USER_NEW, INACTIVE_USER_UNLK, IX, JACK, JIM, JONES, JOSEPH_D, JSCHAFFER, JTAYLOR, LOOKUPS, MASKING_ADMIN, MIKE, NY_NICK, OE, P46890UAD, PA_ADMIN, PDBADMIN, PEDRO, PLOPES, PM, PU_PETE, REDACT_USR, RMTUSR, RUSS, SCHEMAAPP, SCOTT, SECURE_STEVE, SEC_ADMIN_OWEN, SH, SOE, TA_TAMMY, TESTDBONE, TKZGTSDPVPD, USERX, USERY, ZEUS

Remarks: Password verification functions are used to ensure that user passwords meet minimum requirements for complexity, which may include factors such as length, use of numbers or punctuation characters, the difference from previous passwords, etc. Oracle supplies several predefined functions, or a custom PL/SQL function can be used. Every user profile should include a password verification function.

References: **STIG:** Rule SV-76209r1, SV-76213r1, SV-76215r1 , SV-76217r1, SV-76219r1, SV-76221r1, SV-76225r1
CIS: Recommendation 3.8

User Risk Assessment

Reduce user risk by managing roles/privileges and policies

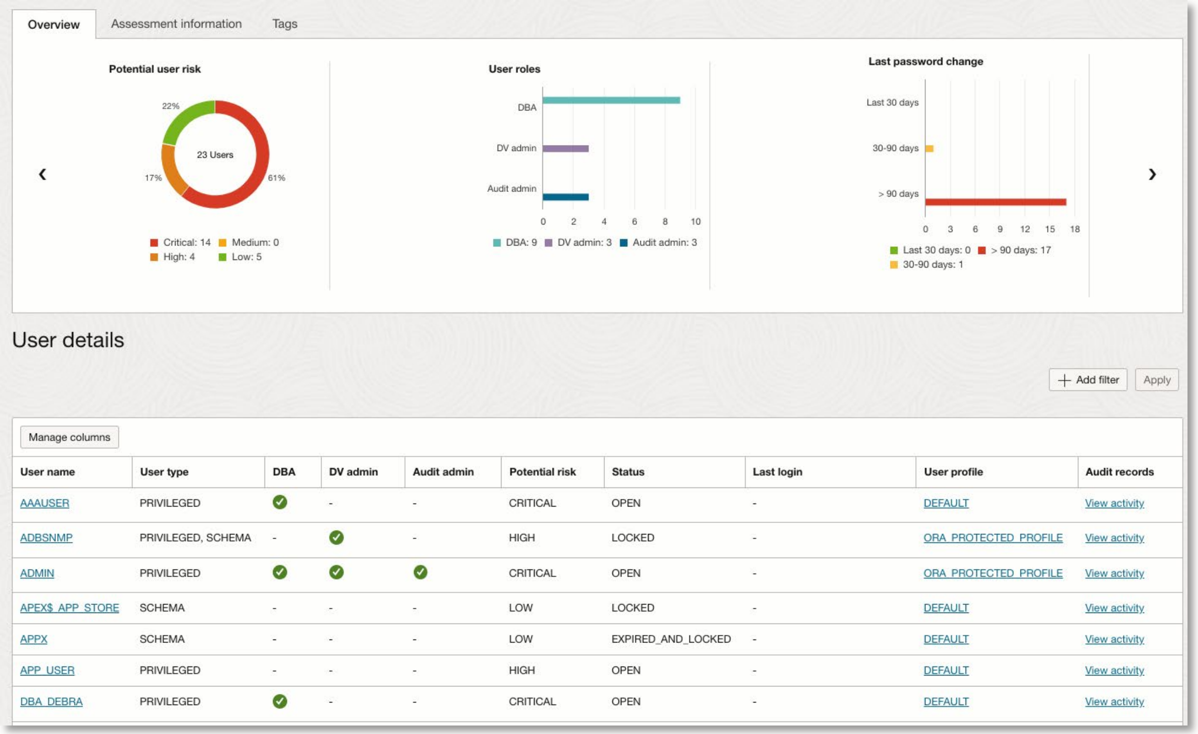
Identify over-privileged risky users

Identify user accounts, their privilege and role grants, their potential risk, and schema access details.

Individual target and fleet view

User Profile Insight

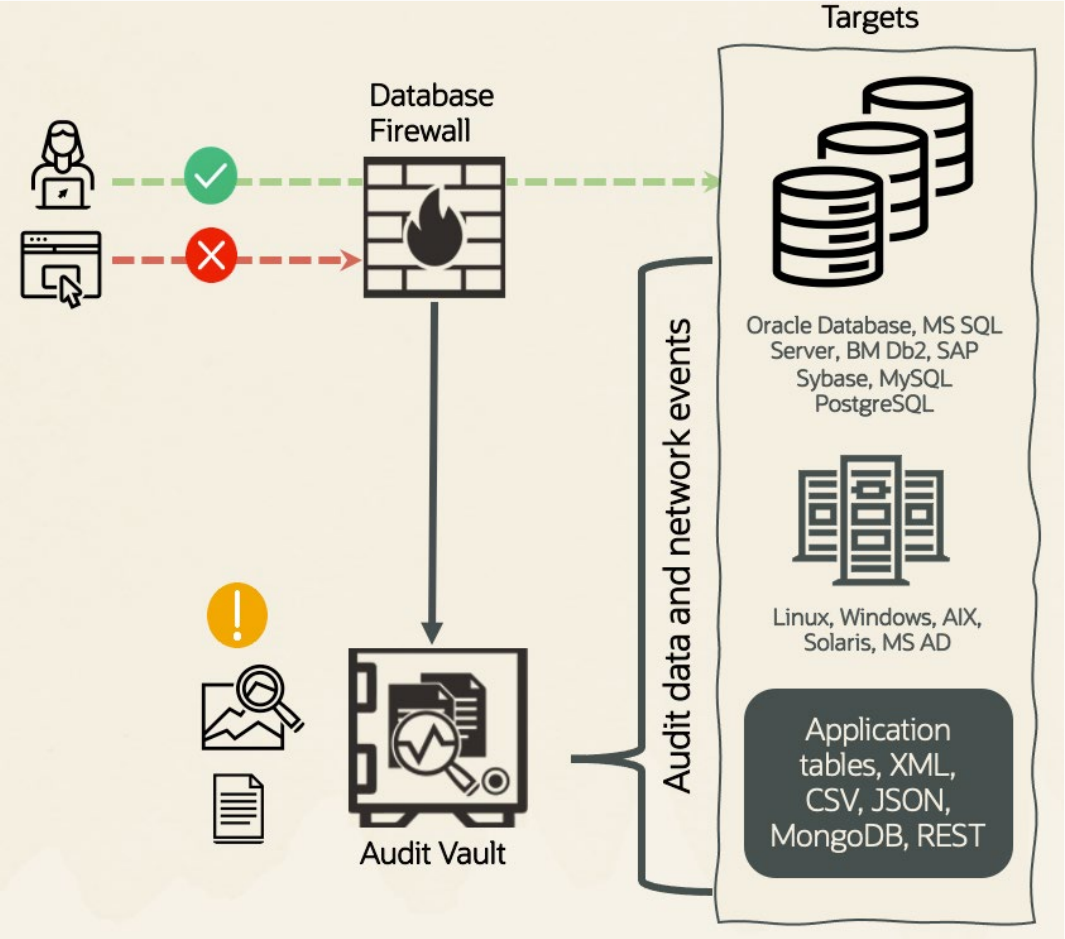
- Review their password parameters including their password complexity verification function.
- Identify users and profiles without password governance policies.
- Identify which profiles are assigned to which users.
- Identify discrepancies in user profiles password attributes across multiple targets.



User details

User name	User type	DBA	DV admin	Audit admin	Potential risk	Status	Last login	User profile	Audit records
AAAUSER	PRIVILEGED	✓	-	-	CRITICAL	OPEN	-	DEFAULT	View activity
ADBSNMP	PRIVILEGED, SCHEMA	-	✓	-	HIGH	LOCKED	-	ORA_PROTECTED_PROFILE	View activity
ADMIN	PRIVILEGED	✓	✓	✓	CRITICAL	OPEN	-	ORA_PROTECTED_PROFILE	View activity
APEX$_APP_STORE	SCHEMA	-	-	-	LOW	LOCKED	-	DEFAULT	View activity
APPX	SCHEMA	-	-	-	LOW	EXPIRED_AND_LOCKED	-	DEFAULT	View activity
APP_USER	PRIVILEGED	-	-	-	HIGH	OPEN	-	DEFAULT	View activity
DBA_DEBRA	PRIVILEGED	✓	-	-	CRITICAL	OPEN	-	DEFAULT	View activity

Oracle Audit Vault and Database Firewall


Targets
Database Firewall
Oracle Database, MS SQL Server, BM Db2, SAP Sybase, MySQL PostgreSQL
Linux, Windows, AIX, Solaris, MS AD
Application tables, XML, CSV, JSON, MongoDB, REST
Audit data and network events
Audit Vault

Oracle Audit Vault and Database Firewall (AVDF) is a complete Database Activity Monitoring (DAM) solution that combines native audit data with network-based SQL traffic capture.

Monitors privileged user activity

Understands what happened after an incident

Blocks unauthorized access

Alerts on suspicious activity

Simplifies regulatory compliance

AVDF Database Security Posture Management

Security Assessment

Know your security configuration and identify drift from your accepted security baseline

Sensitive Data Discovery

Know what your sensitive objects are and where they are stored.

Privileged User Discovery

Know who your privileged users are and what permissions they have.

Audit Insights

Know how your sensitive data has been used by database users

DBSAT vs. Data Safe vs. AVDF capabilities (2/2)

Capabilities	Data Safe	AVDF	DBSAT
Overall security configuration status	Yes	Yes	Yes
Configuration drift detection and reporting	Yes	Yes	-
User Risk Assessment/User Entitlement Reporting	Yes	Yes+	-
Sensitive Data Discovery	Yes	Yes*	Yes*
Centralized management of assessment on multiple targets	Yes	Yes	-
Historical reports and management	Yes	Yes	-
Supports cloud, on-premises and Cloud@Customer targets	Yes	Yes	Yes
Available as	OCI Cloud Service	OCI Marketplace image or on-premises installation	Command line

+ No risk scoring; AVDF entitlement report includes user role and privilege grants, system privilege grants, object privilege grants - with drift.
** Checks only for column names and comments, but not data*

DBSAT vs. Data Safe vs. AVDF capabilities (2/2)

Capabilities	Data Safe	AVDF	DBSAT
Configure deferred risks	Yes	-	-
Top 5 common control deficiencies	Yes	-	-
Security Controls in use	Yes	Yes	Yes

Summary

Easy to install and run

Download DBSAT 3.1 today from
https://www.oracle.com/security/database-security/assessment-tool/

Collect security config data by running ‘`dbsat collect`’ on the target

Run ‘`dbsat report`’ to generate security assessment report

Run ‘`dbsat discover`’ to generate sensitive data report

Available to all Oracle database customers with active support contract

Action plan

Monday Morning

Run DBSAT to assess your current database security state.

What is measured gets done!

Next 30 days

Fix obvious mistakes and high risk findings.

Evaluate **Data Safe** or **Audit Vault and Database Firewall**.

A data breach impacts your business.

Next 90 days

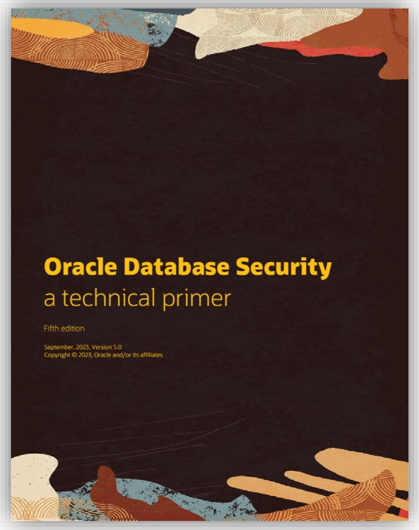
Update Data Security strategy to include database security best practices.

Plan. Trust is hard to build and easy to lose.

Learn More

O.com: www.oracle.com/security/database-security/
Blog: https://blogs.oracle.com/database/category/db-security

NEW: eBook 5th Edition: www.oracle.com/securingthedatabase



Oracle Database Security
a technical primer
Fifth edition
September, 2023, Version 5.0
Copyright © 2023, Oracle and/or its affiliates

Oracle LiveLabs - Try it yourself

- DBSAT: https://bit.ly/dbsat-livelab
- Data Safe: https://bit.ly/datasafe-livelabs
- AVDF: https://bit.ly/avdf-livelab
- Other Database Security: https://bit.ly/golivelabsdbsec

AskTOM Office Hours offers free, open Q&A sessions with Oracle Database PM/experts. We hold a LIVE session on the second Wednesday of each month, at 15:00 UTC here https://bit.ly/asktomdbsec

Ask Tom
Database Security

Q&A

ORACLE

Our mission is to help people see data in new ways, discover insights, unlock endless possibilities.