Oracle® Database

Database Security Assessment Tool User Guide

Release 3.1.0

F90720-05

May 2024

The Oracle Database Security Assessment Tool

In the age of data breaches and ever-evolving data protection and privacy regulations, it is more important than ever for organizations to be confident that their databases are secure. However, it can be difficult to know whether the databases are configured correctly, who has access to it, and where sensitive data is stored. The Oracle Database Security Assessment Tool (DBSAT) helps identify areas where your database configuration, operation, or implementation introduces risks. DBSAT will recommend changes and controls to help mitigate those risks.

Why the Need for a Security Assessment?

Misconfigured databases are a major contributor to database breaches. Human errors could leave your database open to everyone, or an attacker could maliciously exploit configuration mistakes to gain unauthorized access to sensitive data. This can have a devastating impact on your reputation and bottom line. Knowing where your database configuration introduces risk is the first step in minimizing that risk.

About the Oracle Database Security Assessment Tool

The Oracle Database Security Assessment Tool (DBSAT) analyzes the database configuration, users, their entitlements, security policies and identifies where sensitive data resides to uncover security risks and improve the security posture of Oracle Databases within your organization.

Benefits of Using Oracle Database Security Assessment Tool

Using DBSAT, you can:

- Quickly and easily assess the current security status and identify sensitive data within the Oracle Database.
- Reduce risk exposure using proven Oracle Database security best practices, CIS Benchmark recommendations and Security Technical Implementation Guides (STIG) rules.

- Leverage security findings to accelerate compliance with EU GDPR and other regulations.
- Improve the security posture of your Oracle Databases and promote security best practices.

> **Note:**
>
> DBSAT is a lightweight utility that will not impair system performance in a measurable way.

You can use DBSAT report findings to:

- Minimize immediate short term risks
- Implement a comprehensive security strategy
- Support your regulatory compliance program
- Promote security best practices

Oracle Database Security Assessment Tool Components

The DBSAT consists of the following components:

- **Collector:**

  The **Collector** executes SQL queries and runs operating system commands to collect data from the system to be assessed. It does this primarily by querying database dictionary views. The collected data is written to a JSON file that is used by the DBSAT Reporter in the analysis phase. Note that if the collector is executed remotely it will not collect operating system data. It is recommended to run it in the database server to collect all relevant data.

- **Reporter:**

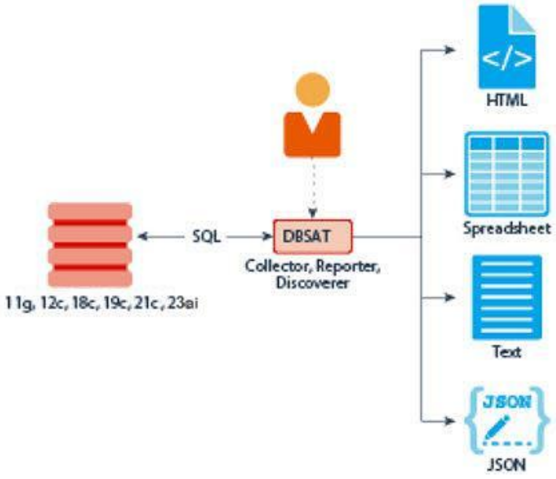
  The **Reporter** analyzes the collected data and generates the Oracle Database Security Assessment Report in HTML, Excel, JSON, and Text formats. The Reporter can run on any machine: PC, laptop, or server. You are not limited to running the Reporter on the database server or the same machine as the Collector.

- **Discoverer:**

  The **Discoverer** executes SQL queries and collects metadata from the database to be assessed, based on the settings specified in the configuration files. It does this primarily by querying database dictionary views. The collected data is then used to generate the Oracle Database Sensitive Data Assessment Report in HTML and CSV formats. The Discoverer can run on any machine: PC, laptop, or server. You are not limited to running the Discoverer on the database server or the same machine as the Collector or Reporter.

The following figure shows the components, sources, and reports of the Oracle Database Security Assessment Tool.

Figure 1-1 DBSAT Components, Sources, and Reports


HTML
Spreadsheet
SQL
DBSAT
Collector, Reporter, Discoverer
11g, 12c, 18c, 19c, 21c, 23ai
Text
JSON
JSON

For more information about the Collector, Reporter, and Discoverer, see Using the Collector and Reporter.

Prerequisites

The following sections outline the prerequisites for the Oracle Database Security Assessment Tool:

Supported Operating Systems

The database configuration collection queries run on most supported Oracle Database platforms. However, currently, DBSAT will skip OS data for databases running on Windows platforms.

DBSAT runs on:

- Linux x86-64 and Linux 64-bit Arm
- Windows x64
- Solaris x64 and Solaris SPARC64
- IBM AIX (64-bit) and Linux on zSeries (64-bit)
- HP-UX IA (64-bit)

Supported Database Versions

You can run the DBSAT on Oracle Database 11.2.0.4 and later releases on-premises or in the Cloud, on Oracle Database Standard Edition 2 and Oracle Database Enterprise Edition. You can also run DBSAT against Autonomous Databases (Serverless, Dedicated, and Cloud@Customer), Autonomous JSON Database, Oracle

Exadata Database Service (Dedicated and Cloud@Customer), and Oracle Base Database Service (BaseDB Enterprise Edition and Standard Edition). Some findings will do different checks and provide targeted remarks for these databases. For more information about the target-specific checks and recommendations, see Appendix A.

Security Requirements

DBSAT output files are sensitive because they may reveal weaknesses in the security posture of your database. To prevent unauthorized access to these files, you must implement the following security guidelines:

- Ensure that the directories holding these files are secured with the appropriate permissions.
- Delete the files securely after you implement the recommendations they contain.
- Share them with others in their (by default) encrypted form.
- Grant user permissions to the DBSAT user on a short-term basis and revoke these when no longer necessary.

  For more information about DBSAT user privileges, see Collector Prerequisites. For more information about DBSAT best practices, see: Best Practices

> **Caution:**
>
> This tool is intended to assist you in identifying potential sensitive data and vulnerabilities in your system. Further, the output generated by this tool may include potentially sensitive system configuration data and information that could be used by a skilled attacker to penetrate your system. You are solely responsible for ensuring that the output of this tool, including any generated reports, is handled in accordance with your company's policies.

Oracle Database Security Assessment Tool Prerequisites

DBSAT on Unix/Linux systems must execute under the BASH shell. If the server does not have this shell, you can install it or run DBSAT remotely from a different server that has it (or from a laptop running Windows, from where you can connect to the database).

Zip and UnZip

DBSAT uses Zip and Unzip to compress or decompress the generated files. DBSAT searches for Zip and Unzip utilities in the default locations shown below. In order to use other Zip and Unzip utilities, update the following lines in the relevant script.

Windows (dbsat.bat script):

```
SET ZIP_CMD=%ORACLE_HOME%\bin\zip.exe
SET UNZIP_CMD=%ORACLE_HOME%\bin\unzip.exe
```

> **Note:**
>
> The Unzip utility is not included in Oracle Database 12.2 and higher. Ensure that you have installed a utility such as WinZip or WinRar, and add the path to the utility in the `SET UNZIP_CMD` parameter.

All other platforms (dbsat script):

```
ZIP=/usr/bin/zip
UNZIP=/usr/bin/unzip
DBZIP=${ORACLE_HOME}/bin/zip
```

The following are the prerequisites for the components of the Oracle Database Security Assessment Tool:

Collector Prerequisites

To gather all necessary data, run the DBSAT Collector on the server that hosts the database. The collector uses operating system commands to gather process and file system information that the database alone cannot provide. Besides, the Oracle DBSAT Collector must be run as an OS user with read permissions on files and directories under `ORACLE_HOME` using SQL*Plus (through Oracle Database or Instant Client) to collect and process file system data using OS commands.

The Oracle DBSAT Collector collects most of its data by querying database views. It must connect to the database as a user with sufficient privileges to select from these views. Grant the DBSAT user the following privileges:

- `CREATE SESSION`
- `READ` or `SELECT` on `SYS.REGISTRY$HISTORY`
- Role `SELECT_CATALOG_ROLE`
- Role `DV_SECANALYST` (if Database Vault is enabled or if Database Vault Operations Control is enabled)
- Role `AUDIT_VIEWER` (12*c* and later)
- Role `CAPTURE_ADMIN` (12*c* and later)
- `READ` or `SELECT` on `SYS.DBA_USERS_WITH_DEFPWD`
- `READ` on `SYS.DBA_AUDIT_MGMT_CONFIG_PARAMS`
- `READ` on `SYS.DBA_CREDENTIALS`

- `EXECUTE` on `SYS.DBMS_SQL`

> **Note:**
>
> If you plan to run only the Discoverer component, you can assign only the following privileges:
>
> - `CREATE SESSION`
> - Role `SELECT_CATALOG_ROLE`
>
> In order to successfully collect Database Vault information in a Database Vault protected environment, you must connect as a non-SYS user with the `DV_SECANALYST` role.

Sample Script to Create a User with Minimum Privileges

You can create a user with required minimum privileges to run the Oracle Database Security Assessment Tool Collector with a script.

Purpose

Create a DBSAT user to run the DBSAT Collector script with required privileges.

Sample Script

```
create user dbsat_user identified by dbsat_user;
--If Database Vault is enabled, connect as DV_ACCTMGR to run this
command
grant create session to dbsat_user;
grant select_catalog_role to dbsat_user;
grant select on sys.registry$history to dbsat_user;
grant read on sys.dba_audit_mgmt_config_params to dbsat_user;
grant select on sys.dba_users_with_defpwd to dbsat_user;
grant read on sys.dba_credentials to dbsat_user;
grant execute on sys.dbms_sql to dbsat_user;
grant audit_viewer to dbsat_user; // 12c and later
grant capture_admin to dbsat_user;// 12c and later covers
sys.dba_priv_captures, sys.priv_capture$, sys.capture_run_log$
--If Database Vault is enabled, connect as DV_OWNER to run this
command
grant DV_SECANALYST to dbsat_user;
```

Reporter Prerequisites

The Reporter is a Java program and requires the Java Runtime Environment (JRE) 1.8 (jdk8-u172) or later to run.

The JAVA_HOME environment variable must be set and should point to the installation directory on your system, which contains the bin and lib directories. For example:

```
$ export JAVA_HOME=/u01/app/jdk1.8.0_201
```

Discoverer Prerequisites

The Discoverer is a Java program and requires the Java Runtime Environment (JRE) 1.8 (jdk8-u172) or later to run.

The JAVA_HOME environment variable must be set and should point to the installation directory on your system, which contains the bin and lib directories. For example:

```
$ export JAVA_HOME=/u01/app/jdk1.8.0_201
```

The Discoverer collects metadata from database dictionary views and matches them against the patterns specified to discover sensitive data. The Discoverer must connect to the database as a user with sufficient privileges to select from these views. For more information about DBSAT user privileges, see Collector Prerequisites.

> **Note:**
>
> The Discoverer relies on table statistics to get row counts. In order to get accurate row count results, DBMS_STATS should be executed by the Database Administrator before the DBSAT user runs the Discoverer.

Installing the Oracle Database Security Assessment Tool

To install the DBSAT:

1. Log in to the database server.
2. Create the dbsat directory:

   ```
   mkdir -p /home/oracle/dbsat
   ```

3. Download or copy the dbsat.zip file to the database server, and unzip the file.

   ```
   unzip dbsat.zip -d /home/oracle/dbsat
   ```

   Where -d refers to the directory path.

These commands are for Linux / Unix. If the installation takes place on Windows, you will use similar commands for Windows.

The DBSAT is installed on the database server.

You can run the Collector, Reporter, and Discoverer from the /home/oracle/dbsat directory.

You can also add this directory to your `PATH` and skip the step of going to the directory every time you want to run the tool.

Using the Collector and Reporter

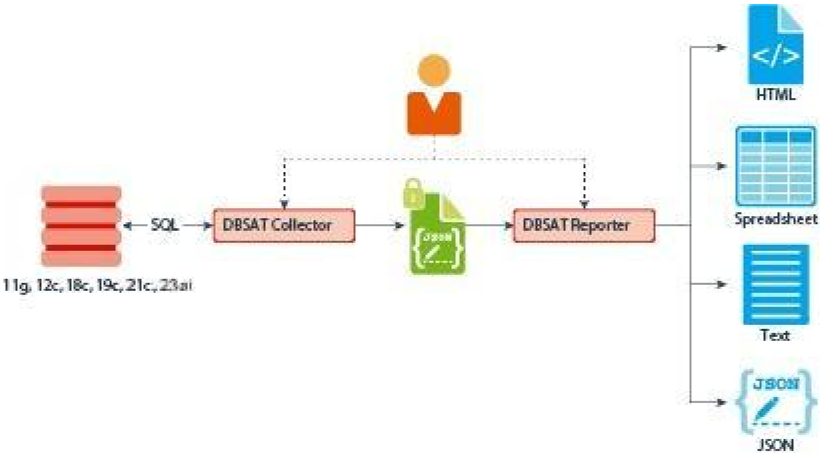
You can generate the Oracle Database Security Assessment Report and the Oracle Database Sensitive Data Assessment Report with the Collector, Reporter, and Discoverer components.

Oracle Database Security Assessment Report

The Collector and Reporter components are used to generate the Oracle Database Security Assessment Report.

The following figure shows the components and architecture of the Collector and Reporter.

Figure 1-2   Collector and Reporter Components and Architecture



Running the Collector

The Collector queries the database to collect data that will be analyzed by the Reporter.

> **Note:**
>
> The Collector connects to the database. Ensure that the target database and listener are running before running the Collector.

To run the Collector, do the following:

1. Specify the arguments to run the Collector:

   ```
   $ dbsat collect <database_connect_string> <output_file>
   ```

   The `dbsat collect` command has the following options and arguments:

   - *`database_connect_string`*

     Specifies the connection string to connect to the database.

     Example: `system@ORCL`

   - *`output_file`*

     Specifies the location and file name for the Database Security Assessment report. Do not add an extension.

     Example: `/home/oracle/dbsat/output_ORCL`

2. Run the Collector.

   ```
   $ ./dbsat collect system@ORCL output_ORCL
   ```

   The following output is displayed:

   ```
   Connecting to the target Oracle database...

   SQL*Plus: Release 19.0.0.0.0 - Mon Jan 30 10:19:15 2023
   Version 19.13.0.0.0

   Copyright (c) 1982, 2021, Oracle.  All rights reserved.


   Connected to:
   Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 -
   Production
   Version 19.13.0.0.0

   Setup complete.
   SQL queries complete.
   Warning: Exit status 256 from OS rule: dbcs_status
   OS commands complete.
   Disconnected from Oracle Database 19c Enterprise Edition Release
   19.0.0.0.0 - Production
   Version 19.13.0.0.0
   DBSAT Collector completed successfully.

   Calling /u01/app/oracle/product/version/db_1/bin/zip to encrypt
   output_ORCL.json...

   Enter password:
   Verify password:
     adding: output_ORCL.json (deflated 88%)
   ```

```
zip completed successfully.
$
```

> **Note:**
>
> DBSAT can display warnings informing that some checks were skipped. These can be safely ignored as the execution proceeds. Some reasons to skip checks include wrong permissions, missing .ora files, not applicable to that target type, and more. For details, please refer to My Oracle Support.
>
> Running the Collector in the root container in a multitenant container database collects data specific to the root container and not from its pluggable databases. If you need to access specific pluggable databases, you must run the Collector for these pluggable databases separately.
>
> If you do not want to encrypt the file invoke the `dbsat collect` script with the `-n` option. This is not recommended.

Running the Reporter

The Reporter analyzes the data collected by the Collector and makes recommendations to improve the security of the database.

You can invoke the Reporter with `dbsat report`.

To run the Reporter, do the following:

1. Check that Java Runtime Environment (JRE) 1.8 (jdk8-u172) or later is installed.

   ```
   $ java -version
   ```

   A similar output is displayed:

   ```
   java version "1.8.0_191"
   ```

2. Specify the arguments to run the Reporter.

   ```
   $ dbsat report [-a] [-n] [-g] [-x <section>] [-u <user> ]
   <input_file>
   ```

   Where the argument *`input_file`* stands for the full or relative path to the data file `output_ORCL` produced by the DBSAT Collector. If this file was encrypted during data collection, you will need to supply the encryption password when prompted by the Reporter.

   The Reporter supports the following command-line options:

   - *`-a`*

     Runs the report for all the database accounts including locked or schema only accounts that are Oracle-supplied.

- *-n*

  Specifies no encryption for output.

  > **Note:**
  >
  > For security reasons, this is not recommended.

- *-g*

  Shows all grants including common grants in a pluggable database.

- -u

  Specify users to exclude from report.

  To exclude multiple users use a comma-separated list, for example: -u SCOTT,DEBRA

- *-x*

  Excludes a section from the report.

  Valid sections are:

  - USER: **User Accounts**
  - PRIV: **Privileges and Roles**
  - AUTHZ: **Authorization Control**
  - ENCRYPT: **Encryption**
  - ACCESS: **Fine-Grained Access Control**
  - AUDIT: **Auditing**
  - CONF: **Database Configuration**
  - NET: **Network Configuration**
  - OS: **Operating System**

  To exclude multiple sections use a comma-separated list, for example:

  ```
  -x USER,PRIV
  ```

  Or:

  ```
  -x USER -x PRIV
  ```

  Omitting this option will include all sections of the report.

The same path name is used to generate the report files produced by the Reporter in HTML, Excel, JSON, and Text formats with the appropriate file extensions.

3. Run the Reporter.

```
$ ./dbsat report output_ORCL
```

The following output appears:

```
Archive:  output_ORCL.zip
[output_ORCL.zip] output_ORCL.json password:
  inflating: output_ORCL.json
DBSAT Reporter ran successfully.
Calling /usr/bin/zip to encrypt the generated reports...
Enter password:
Verify password:
    zip warning: output_ORCL_report.zip not found or empty
  adding: output_ORCL_report.txt (deflated 82%)
  adding: output_ORCL_report.html (deflated 86%)
  adding: output_ORCL_report.xlsx (deflated 3%)
  adding: output_ORCL_report.json (deflated 85%)
zip completed successfully.
```

4. Specify a password to encrypt the output report `.zip` file.

   The `.zip` file is created.

   > **Note:**
   >
   > The `.zip` file is used for Reporter and Discoverer output. To avoid confusion, it is recommended that you use the same password while creating both outputs.

5. Extract the contents of the `.zip` file to access the Oracle Database Security Assessment Report. When prompted, enter the password to decrypt the `.zip` file specified in Step *4*.

   The contents of the `.zip` file are extracted.

6. Use the appropriate tools to read the recommendations from the report files.

   Example: Use `vi` on Linux to read the `.txt` files.

   Example: Use a browser to display the `.html` files.

> **Note:**
>
> DBSAT recommendations do not adjust for individual applications. In cases where the application requirements differ from DBSAT, you will frequently have to accept the finding as-is, possibly mitigating the finding through some other control. Unless the risk is too high for you to accept, the application requirements should usually supersede the DBSAT recommendation.

Oracle Database Security Assessment Report

The Collector and Reporter components are used to generate the Oracle Database Security Assessment (DBSAT) Report in HTML, Excel, JSON, and Text formats. All reports contain similar information but in different formats.

The HTML report provides detailed assessment results in a format that is easy to navigate. The Excel format provides a high-level summary of each finding without the detailed output included in the HTML report. It also allows you to add columns for your tracking and prioritization purposes. A report in text format makes it convenient to copy portions of the output for other usages. Finally, a JSON document containing the report contents is provided for easier filtering, comparison, aggregation, and integration with other tools.

The following Database Security Assessment Report sections will use the HTML report as an example and highlight the findings along with the sections they belong to, the rule ID, and a short description.

At the top of the report, you will find information about the Collector and Reporter run details, such as the data collection and report generation dates, along with the reporter version. Follows the Database Identity information, where you will find details about the target database. Then, the Summary table presents all the findings per section/ domain and their severity level.

Findings

DBSAT reporter resulting analysis is reported in units called Findings, and in each Finding, you see:

1. **Rule ID**: The Rule ID has two parts: the prefix identifies the report section, and the suffix identifies the specific rule.
2. **One-line summary**: One-line summary highlighting the objective and context of each check.
3. **Status**: The Status helps you prioritize implementing DBSAT recommendations. It indicates the level of risk associated with the finding, allowing you to make informed decisions about remediation.

    - **High Risk**
      Needs immediate attention.
    - **Medium Risk**
      Plan to address these in the short term.
    - **Low Risk**
      Might be fixed during scheduled downtime or bundled with other maintenance activities.
    - **Evaluate**
      Needs manual analysis.
    - **Advisory**
      Poses an opportunity for improvement and raises awareness about other security controls available in the Oracle Database.
    - **Pass**

      No risks were found.

4. **Summary**: Provides a summary of the Finding. When the Finding is informational, the summary typically reports only the number of examined data elements.
5. **Details**: Provides detailed information to explain the finding summary, typically results from the assessed database, followed by any recommendations for changes.
6. **Remarks**: Explain the reason for the rule and recommended actions for remediation.
7. **References**: If the finding is an Oracle Best Practice (OBP) related to an Oracle Database 12c STIG V2R8, CIS Oracle Database Benchmark 12c v2.0.0 recommendation, or related to a GDPR Article/Recitals, it will be mentioned here.

Security Frameworks and Best Practices

DBSAT integrates Oracle Best Practices, Center for Internet Security (CIS) Benchmark, and the US Department of Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) for the Oracle Database to identify potential security risks in Oracle databases.

Initially, DBSAT primarily focused on STIGs and CIS benchmarks, but with version 3.0 and later, it also highlights findings aligned or that are Oracle's own best practices.

Some checks are designated as Oracle Best Practices (OBP) only. This could be due to various factors, such as differences in release cycles or a deeper understanding of Oracle's inner workings. For example, while Oracle releases new features or capabilities, it can take years for standards to include them. For instance, Oracle introduced Gradual Password Rollover in Oracle Database 19c in 2021, but until April 2024, it wasn’t reflected in STIG or CIS.

Multiple security frameworks often cover similar requirements, and DBSAT tags findings accordingly. For instance, if both CIS and STIG recommend avoiding default passwords for database user accounts, DBSAT marks that finding with both frameworks' tags, and as this is an Oracle best practice, it would be as well flagged with the OBP tag.

DBSAT's tagging system lets users focus on findings relevant to their compliance standards. Whether seeking STIG compliance, adherence to CIS benchmark, or alignment with Oracle's best practices, users can easily find and prioritize findings based on their specific requirements.

DBSAT maps findings to:

- STIG V2R8
- Oracle Database 19c CIS Benchmark v1.2.
- Oracle Best Practices
- European Union General Data Protection Regulation (EU GDPR) 2016/679 articles and recitals

Note:

Recommendations reflect best practices for database security and should be part of any strategy for data protection by design and by default.

EU GDPR tagged findings highlight technology that may help you address EU GDPR articles and recitals and other data privacy regulations with similar requirements. Technical controls alone are not sufficient for compliance. Passing all findings does not guarantee compliance.

Sections

DBSAT Security Assessment report starts with a Summary and follows with findings organized in the following categories:

- Basic Information
- User Accounts
- Privileges and Role
- Authorization Control
- Fine-Grained Access Control
- Auditing
- Encryption
- Database Configuration
- Network Configuration
- Operating System

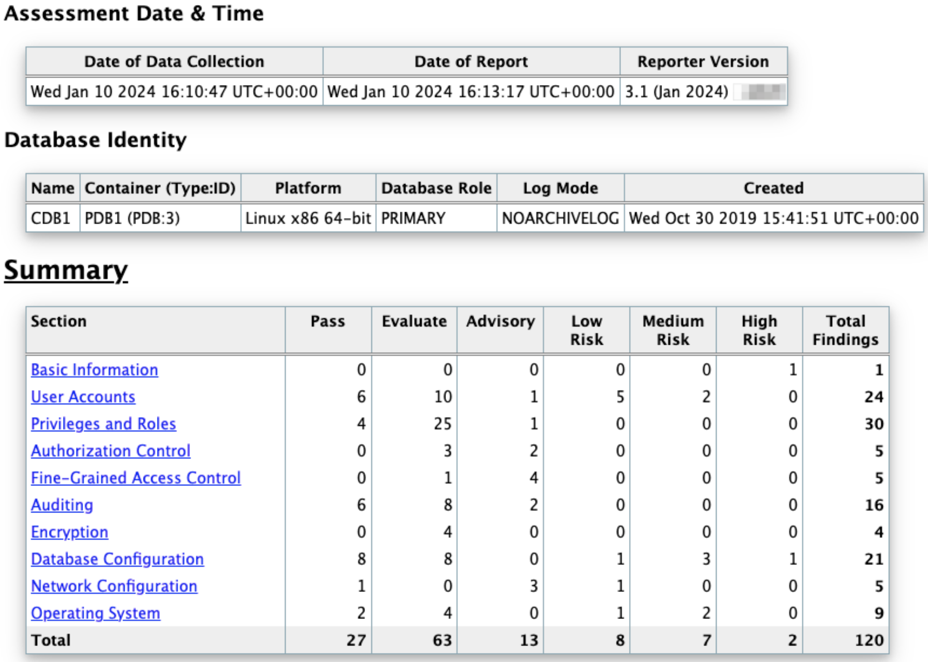
Oracle Database Security Assessment Report — Summary

The Oracle Database Security Assessment Report — Summary section contains the following information:

Section	Description
Assessment Time & Date	Displays the date on which the data was collected and the date on which the final Database Security Assessment report was generated. The DBSAT Reporter version is also displayed.
Database Identity	Displays the details of the database assessed by DBSAT.
Summary	Displays a high level summary of the resulting analysis.

The following figure displays an example of the Oracle Database Security Assessment Report — Summary section.

Figure 1-3 Oracle Database Security Assessment Report — Summary



Assessment Date & Time

Date of Data Collection	Date of Report	Reporter Version
Wed Jan 10 2024 16:10:47 UTC+00:00	Wed Jan 10 2024 16:13:17 UTC+00:00	3.1 (Jan 2024) [redacted]

Database Identity

Name	Container (Type:ID)	Platform	Database Role	Log Mode	Created
CDB1	PDB1 (PDB:3)	Linux x86 64-bit	PRIMARY	NOARCHIVELOG	Wed Oct 30 2019 15:41:51 UTC+00:00

Summary

Section	Pass	Evaluate	Advisory	Low Risk	Medium Risk	High Risk	Total Findings
Basic Information	0	0	0	0	0	1	1
User Accounts	6	10	1	5	2	0	24
Privileges and Roles	4	25	1	0	0	0	30
Authorization Control	0	3	2	0	0	0	5
Fine-Grained Access Control	0	1	4	0	0	0	5
Auditing	6	8	2	0	0	0	16
Encryption	0	4	0	0	0	0	4
Database Configuration	8	8	0	1	3	1	21
Network Configuration	1	0	3	1	0	0	5
Operating System	2	4	0	1	2	0	9
Total	27	63	13	8	7	2	120

The Summary section is followed by the Basic Information section.

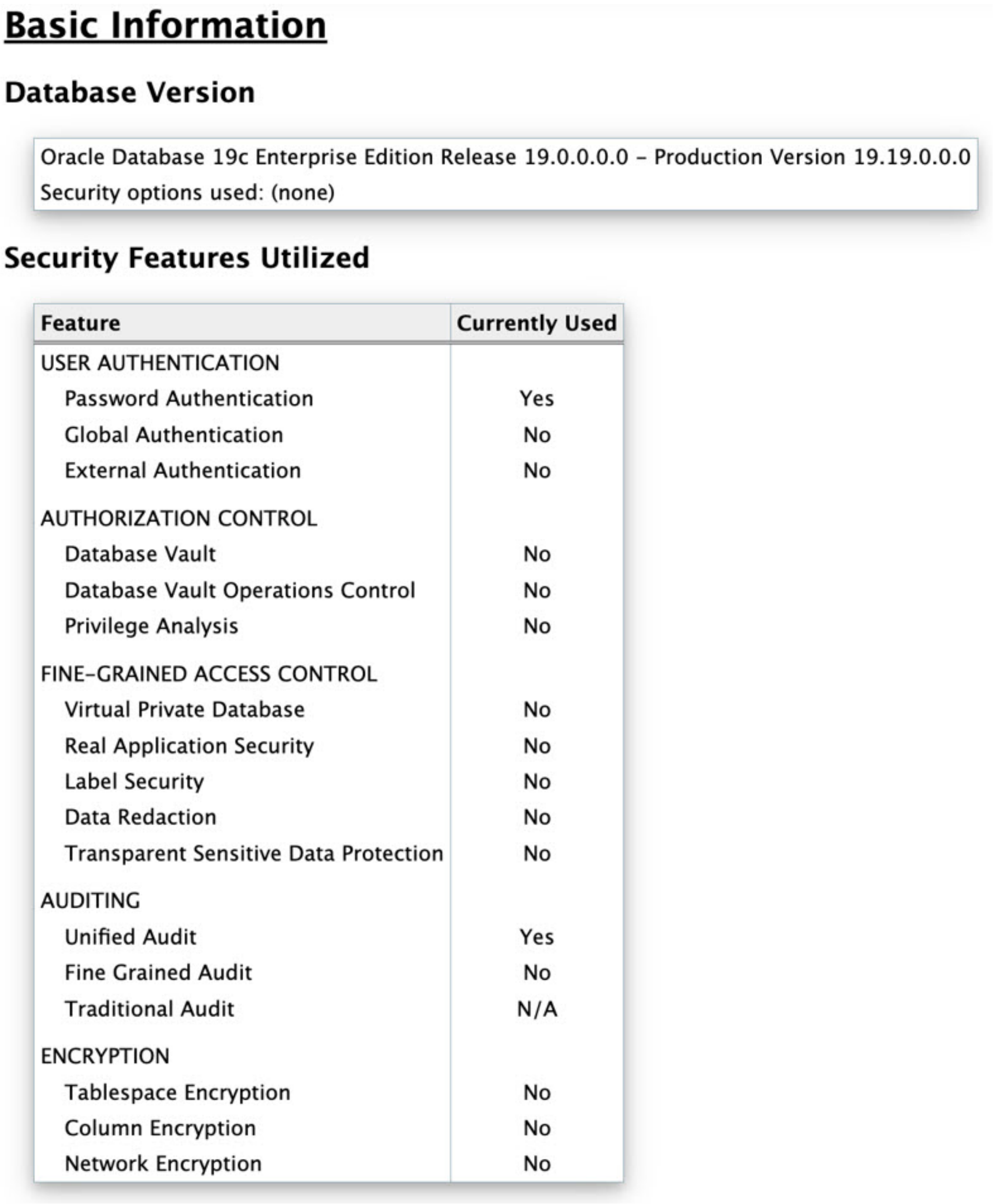
Oracle Database Security Assessment Report — Basic Information

The Oracle Database Security Assessment Report — Basic Information section contains the following information:

Section	Finding ID	Description
Database Version	-	Displays the version of the database assessed by the Collector and Reporter.
Security Features Utilized	-	Displays the security features and indicates if they are in use.
Patch Check	INFO.PATCH	Displays information about the patches installed. It is vital to keep the database software up-to-date with security fixes as they are released. Oracle issues comprehensive patches in the form of Release Updates on a regular quarterly schedule. Patch Set Updates and Bundle Patches were available for database versions up to 12.1.0.2.

The following figure displays an example of the Oracle Database Security Assessment Report — Basic Information section.

Figure 1-4 Oracle Database Security Assessment Report — Basic Information



Basic Information

Database Version

```
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production Version 19.19.0.0.0
Security options used: (none)
```

Security Features Utilized

Feature	Currently Used
USER AUTHENTICATION	
Password Authentication	Yes
Global Authentication	No
External Authentication	No
AUTHORIZATION CONTROL	
Database Vault	No
Database Vault Operations Control	No
Privilege Analysis	No
FINE-GRAINED ACCESS CONTROL	
Virtual Private Database	No
Real Application Security	No
Label Security	No
Data Redaction	No
Transparent Sensitive Data Protection	No
AUDITING	
Unified Audit	Yes
Fine Grained Audit	No
Traditional Audit	N/A
ENCRYPTION	
Tablespace Encryption	No
Column Encryption	No
Network Encryption	No

The Basic Information section is followed by the User Accounts section.

Oracle Database Security Assessment Report — User Accounts

The Oracle Database Security Assessment Report — User Accounts section displays the following information:

Name	Finding ID	Description
User Accounts	-	Displays the user accounts and the following information about each account: • User Name — Displays the name of the user. • Profile — Displays the profile assigned to the account. • Status — Displays whether the account is, for example, Open, Locked, Expired, or in Rollover. • Authentication Type — Displays the type of authentication used. • Default Tablespace — Displays the default tablespace for the account. • Oracle Defined — Displays whether the user account is oracle maintained or not.
Users with DEFAULT Profile	USER.DEFAULTPROFILE	Displays the DEFAULT user profile password and resource parameters and the number of users in it.
Users with Default Passwords	USER.DEFPWD	Displays information about the user accounts with default passwords. Default account passwords for predefined Oracle accounts are well known. Active accounts with default passwords provide a trivial means of entry for attackers, but well-known passwords should be changed for locked accounts as well.
Users with Expired Passwords	USER.EXPIRED	Displays information about the user accounts with expired passwords. Password expiration is used to ensure that users change their passwords regularly. Unlocked accounts with an expired password can present a security risk, especially as those accounts age. Although the password is expired, because the account is unlocked, it can easily be used by anyone who knows the old password. You should investigate accounts that have been unused for an extended period to determine whether they should remain active.
Inactive Users	USER.INACTIVE	Displays information about the user accounts that are not in use and also accounts that are not configured to be locked when inactive. If a user account is no longer in use, it increases the attack surface of the system unnecessarily while providing no corresponding benefit. Furthermore, unauthorized use is less likely to be noticed when no one is regularly using the account. Accounts that have been unused for more than 30 days should be investigated to determine whether they should remain active. A solution is to set `INACTIVE_ACCOUNT_TIME` in the profiles assigned to users.

Name	Finding ID	Description
Sample Schemas	USER.SAMPLE	Displays information about the user accounts that use sample schemas such as SCOTT, HR, OE, SH, PM, IX, ADAMS, BLAKE, CLARK, and BI. 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.
Application Owner Account	USER.APPOWNER	Checks the database for the account that could be considered the application owner and for objects accessible by the application owner. Any user not "oracle maintained" that owns most objects in the database is considered the Application Owner. This check: • Lists application owners • Lists users who can login into database • Lists app owners and the objects owned by it along with the non-app owners who can access those objects
Shared Accounts	USER.SHARED	Displays users that have multiple administrative privileges and proxy users.
Users with Objects	USER.OBJOWNER	Displays application users who own objects and can grant access to those objects to other users
Users Authorized for Object Ownership	USER.OBJAUTHZ	Displays non-oracle maintained users who own objects
Users with Security Objects	USER.SECURITYOBJS	Displays users who own security objects
Users with Grant Option	USER.GRANTOPTION	Checks for users that have been granted privileges with WITH GRANT OPTION.
Users with Sensitive Data	USER.SENSITVEDATA	Displays users that own tables with columns marked as sensitive with TSDP and users that can access those tables. To ensure secure access to sensitive information, review these users. It is best to grant access to data through roles rather than directly to individual accounts.

Name	Finding ID	Description
User Schemas in SYSTEM or SYSAUX Tablespace	USER.TABLESPACE	Displays information about the regular user accounts that use the reserved Oracle-supplied tablespaces. The SYSTEM and SYSAUX tablespaces are reserved for Oracle-supplied user accounts. To avoid a possible denial of service caused by exhausting these resources, regular user accounts should not use these tablespaces. Prior to Oracle Database 12.2, the SYSTEM tablespace cannot be encrypted, and this is another reason to avoid user schemas in this tablespace.
Case-Sensitive Passwords	USER.PASSWORDCASE	Displays whether case-sensitive passwords are enabled. Case-sensitive passwords are recommended because including both upper and lower-case letters greatly increases the set of possible passwords that must be searched by an attacker who is attempting to guess a password by exhaustive search. Setting SEC_CASE_SENSITIVE_LOGON to TRUE ensures that the database distinguishes between upper and lower-case letters in passwords.

Note:

In 21c USER.PASSWORDCASE isn't expected to be shown as SEC_CASE_SENSITIVE_LOGON is desupported

Name	Finding ID	Description
Legacy Password Versions	USER.AUTHLEGACY	Displays information about the user accounts with obsolete password verifiers. For each user account, the database may store multiple verifiers, which are hashes of the user password. Each verifier supports a different version of the password authentication algorithm. Every user account should include a verifier for the latest password version supported by the database so that the user can be authenticated using the latest algorithm supported by the client. When all clients have been updated, the security of user accounts can be improved by removing the obsolete verifiers. HTTP password verifiers are used for XML Database authentication. Use the `ALTER USER` command to remove these verifiers from user accounts that do not require this access.
User Profiles	-	Displays information about the user profiles.
Users with no Password Complexity Requirements	USER.PASSWORDFUNCTION	Displays information about profiles with and without a password complexity verification function. Users not subject to password complexity verification are also displayed. 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, 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.
Account Locking after Failed Login Attempts	USER.NOLOCK	Displays information about user profile failed login attempt enforcement. Attackers sometimes attempt to guess a user's password by simply trying all possibilities from a set of common passwords. To defend against this attack, it is advisable to use the `FAILED_LOGIN_ATTEMPTS` and `PASSWORD_LOCK_TIME` profile resources to lock user accounts for a specified time when there are multiple failed login attempts without a successful login.

Name	Finding ID	Description
Users with Unlimited Password Lifetime	USER.NOEXPIRE	Displays information about user profile password expiration enforcement. Password expiration is used to ensure that users change their passwords on a regular basis. It also provides a mechanism to automatically disable temporary accounts. Passwords that never expire may remain unchanged for an extended period of time. When passwords do not have to be changed regularly, users are also more likely to use the same passwords for multiple accounts.
Users with Unlimited Concurrent Sessions	USER.SESSIONS	Displays all users that have a Profile Resource Limit for `SESSIONS_PER_USER` set to `UNLIMITED`. With `SESSIONS_PER_USER = UNLIMITED` users can have any number of concurrent sessions.
Unlimited Session Idle Time	USER.IDLETIME	This check lists users with UNLIMITED IDLE TIME
Users with Gradual Password Rollover	USER.PASSWORDROLLOVER	Displays information about the Gradual Password Rollover. Gradual Password Rollover allows administrators to change database passwords for applications without having to schedule downtime. Prior to the advent of 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 the minimum.
Temporary Users	USER.TEMP	Displays users associated with the DEFAULT profile. Users specifically created to execute temporary tasks should be on a profile tailored for that purpose.
Development Users in Production Databases	USER.DEV	There should not be developer accounts in production systems. Verify if such accounts exist in your database.

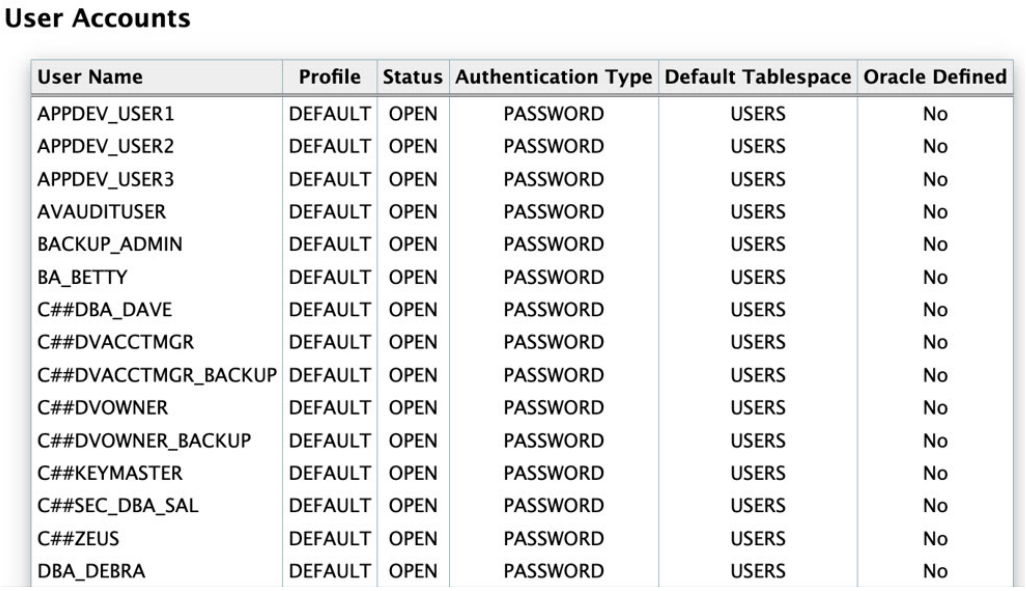
Name	Finding ID	Description
Advanced Replication Users	USER.REPCAT	Checks if Oracle Advanced Replication is being used and lists the dblinks used for replication. Checks to see if `enable_goldengate_replication` is set to `TRUE`. Also checks if `DBA_REPCAT%` views are present or `count(*) from DBA_REPCATLOG > 0`.
Minimum Client Authentication Version	USER.AUTHVERSION	Displays information about the user accounts that do not have minimum client version specified in the `ALLOWED_LOGON_VERSION_SERVER` parameter in the `sqlnet.ora` file. Over time, Oracle releases have added support for increasingly secure versions of the algorithm used for password authentication of user accounts. In order to remain compatible with older client software, the database continues to support previous password versions as well. The `sqlnet.ora` parameter `ALLOWED_LOGON_VERSION_SERVER` determines the minimum password version that the database will accept. For maximum security, this parameter should be set to the highest value supported by the database once all client systems have been upgraded.

Note:

Predefined Oracle accounts which are schema-only or locked are not included in this report. To include all user accounts, run the report with the `-a` option.

The following figure displays an example of the Oracle Database Security Assessment Report — User Accounts section.

Figure 1-5   Oracle Database Security Assessment Report — User Accounts



User Accounts

User Name	Profile	Status	Authentication Type	Default Tablespace	Oracle Defined
APPDEV_USER1	DEFAULT	OPEN	PASSWORD	USERS	No
APPDEV_USER2	DEFAULT	OPEN	PASSWORD	USERS	No
APPDEV_USER3	DEFAULT	OPEN	PASSWORD	USERS	No
AVAUDITUSER	DEFAULT	OPEN	PASSWORD	USERS	No
BACKUP_ADMIN	DEFAULT	OPEN	PASSWORD	USERS	No
BA_BETTY	DEFAULT	OPEN	PASSWORD	USERS	No
C##DBA_DAVE	DEFAULT	OPEN	PASSWORD	USERS	No
C##DVACCTMGR	DEFAULT	OPEN	PASSWORD	USERS	No
C##DVACCTMGR_BACKUP	DEFAULT	OPEN	PASSWORD	USERS	No
C##DVOWNER	DEFAULT	OPEN	PASSWORD	USERS	No
C##DVOWNER_BACKUP	DEFAULT	OPEN	PASSWORD	USERS	No
C##KEYMASTER	DEFAULT	OPEN	PASSWORD	USERS	No
C##SEC_DBA_SAL	DEFAULT	OPEN	PASSWORD	USERS	No
C##ZEUS	DEFAULT	OPEN	PASSWORD	USERS	No
DBA_DEBRA	DEFAULT	OPEN	PASSWORD	USERS	No

The User Accounts section is followed by the Privileges and Roles section.

Oracle Database Security Assessment Report — Privileges and Roles

The Oracle Database Security Assessment Report — Privileges and Roles section displays the following information:

Name	Finding ID	Description
Access to Password Verifier Tables	PRIV.ACCESSVERIFIERS	Displays access to password verifier tables granted to users. Users with these privileges can access objects that contain user password verifiers. The verifiers can be used in offline attacks to discover user passwords.
Users with Administrative Privileges SYS* Privileges	PRIV.SYSADMIN	Displays the administrative privileges granted to user accounts. Administrative 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, less powerful administrative privileges were introduced to allow users to perform common administrative tasks with less than full `SYSDBA` privileges. To achieve the benefit of this separation of duty, each of these administrative privileges should be granted to at least one user account.

Name	Finding ID	Description
Users with DBA Role	PRIV.DBA	Displays the user accounts that have been granted the DBA or PDB_DBA role. The DBA role is very powerful and can be used to bypass many security protections. It should be granted to only a small number of trusted administrators. Furthermore, each trusted user should have an individual account for accountability reasons. As with any powerful role, avoid granting the DBA role with admin option unless absolutely necessary.
Users with Powerful Roles	PRIV.BIGROLES	Displays the user accounts that have been granted roles with maximum data access privileges. Like the DBA role, these roles (AQ_ADMINISTRATOR_ROLE, EM_EXPRESS_ALL, EXP_FULL_DATABASE, IMP_FULL_DATABASE, SELECT_CATALOG_ROLE, EXECUTE_CATALOG_ROLE, DELETE_CATALOG_ROLE, OEM_MONITOR) contain powerful privileges that can be used to bypass security protections. They should be granted only to a small number of trusted administrators.
System Privilege Grants	PRIV.SYSTEM	Displays the system privileges granted to users. System privileges provide the ability to access data or perform administrative operations for the entire database. Consistent with the principle of least privilege, these privileges should be granted sparingly. System privileges should be granted with admin option only when the recipient needs the ability to grant the privilege to others. -g option reports all grants including common grants in a PDB. The report displays (*) for privileges being granted with admin option, (D) for privileges being granted directly, and (C) for privileges being granted commonly.
System Privileges Granted to PUBLIC	PRIV.SYSPUBLIC	Displays the system privileges granted to PUBLIC. Privileges granted to PUBLIC are available to all users. This generally should include few, if any, system privileges since these will not be needed by ordinary users who are not administrators.
Roles Granted to PUBLIC	PRIV.ROLEPUBLIC	Displays the roles granted to PUBLIC. Roles granted to PUBLIC are available to all users. Most roles contain privileges that are not appropriate for all users.
Column Privileges Granted to PUBLIC	PRIV.COLPUBLIC	Displays the column access privileges granted to PUBLIC. Privileges granted to PUBLIC are available to all users. This should include column privileges only for data that is intended to be accessible to everyone.

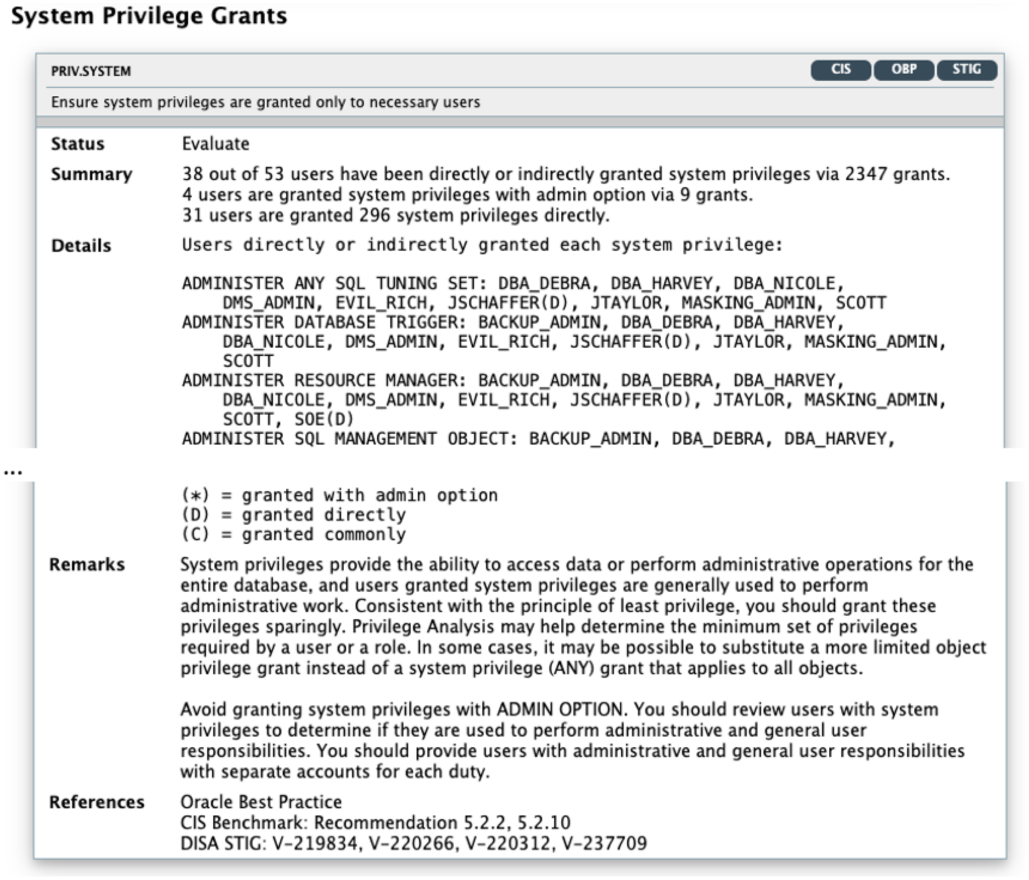
Name	Finding ID	Description
Objects Accessible by PUBLIC	PRIV.OBJPUBLIC	Displays objects that are accessible by PUBLIC.
Encryption Packages Granted to PUBLIC	PRIV.ENCRYPTPACKAGEPUBLIC	Displays DBMS_CRYPTO, DBMS_OBFUSCATION_TOOLKIT, and DBMS_RANDOM grants to PUBLIC.
Scheduler Job Packages Granted to PUBLIC	PRIV.JOBSCHPACKAGEPUBLIC	Display DBMS_SCHEDULER and DBMS_JOB EXECUTE grants to PUBLIC and Scheduler/Job system privileges (CREATE JOB, MANAGE SCHEDULER, CREATE EXTERNAL JOB, CREATE ANY JOB) grants to PUBLIC.
Credential Package Granted to PUBLIC	PRIV.CREDPACKAGEPUBLIC	Displays EXECUTE grant on DBMS_CREDENTIAL package to PUBLIC. Also checks for privilege grants of CREATE CREDENTIAL and CREATE ANY CREDENTIAL to users.
File System Packages Granted to PUBLIC	PRIV.FILESYSTEMPACKAGEPUBLIC	Displays EXECUTE grant on DBMS_LOB, UTL_FILE, and DBMS_ADVISOR packages to PUBLIC. Also checks for system privilege grants of CREATE ANY DIRECTORY and DROP ANY DIRECTORY to users.
Network Packages Granted to PUBLIC	PRIV.NETPACKAGEPUBLIC	Displays EXECUTE grant on DBMS_LDAP, UTL_HTTP, UTL_INADDR, UTL_SMTP, and UTL_TCP packages to PUBLIC. Also checks for users that are authorized to execute packages via ACLs.
SQL Packages Granted to PUBLIC	PRIV.QUERYPACKAGEPUBLIC	Displays EXECUTE grant on DBMS_XMLQUERY, DBMS_XMLSAVE, DBMS_XMLSTORE, DBMS_REDACT, DBMS_XMLGEN, and DBMS_SQL packages to PUBLIC.
JAVA Permissions Granted to PUBLIC	PRIV.JAVAPACKAGEPUBLIC	Displays EXECUTE grant on DBMS_JAVA and DBMS_JAVA_TEST packages to PUBLIC. Also checks for grants of JAVA_ADMIN role to users.
All Roles	PRIV.ALLROLES	Displays all roles granted to users. Roles are a convenient way to manage groups of related privileges, especially when the privileges are required for a particular task or job function. Beware of broadly defined roles, which may confer more privileges than an individual recipient requires. Roles should be granted with admin option only when the recipient needs the ability to modify the role or grant it to others.
Account Management Privileges	PRIV.ACCOUNTMGMT	Displays account management privileges granted to users. User management privileges (`ALTER USER`, `CREATE USER`, `DROP USER`) can be used to create and modify other user accounts, including changing passwords. This power can be abused to gain access to another user's account, which may have greater privileges.

Name	Finding ID	Description
Role and Privilege Management Privileges	PRIV.ROLEPRIVMGMT	Displays privilege management privileges granted to users. Users with privilege management privileges (ALTER ANY ROLE, CREATE ROLE, DROP ANY ROLE, GRANT ANY OBJECT PRIVILEGE, GRANT ANY PRIVILEGE, GRANT ANY ROLE) can change the set of privileges granted to themselves and other users. This ability should be granted sparingly, since it can be used to circumvent many security controls in the database.
Database Management Privileges	PRIV.DBMGMT	Displays database management privileges granted to users. Database management privileges (ALTER DATABASE, ALTER SYSTEM, CREATE ANY LIBRARY, CREATE LIBRARY) can be used to change the operation of the database and potentially bypass security protections. This ability should be granted only to trusted administrators.
Audit Management Package	PRIV.AUDITMGMTPKG	Displays audit management tool access granted to users. The DBMS_AUDIT_MGMT package allow for execution of Audit management tools. Access should be strictly limited and granted only to users with a legitimate need for this functionality.
Audit Management Privileges	PRIV.AUDITMGMT	Displays audit management privileges granted to users. Audit management privileges (AUDIT ANY, AUDIT SYSTEM) can be used to change the audit policies for the database. This ability should be granted sparingly, since it may be used to hide malicious activity.
Access to Audit Objects	PRIV.ACCESSAUDITOBJ	Displays access to audit objects granted to users. Users with these privileges can directly access and modify objects containing audit information. Access to these objects may allow a malicious user deduce privilege settings for other users and to manipulate the audit information by replacing or deleting audit records.
Access Control Exemption Privileges	PRIV.ACCESSEXEMPT	Displays access control exemption privileges that are enforced. Users with exemption privileges (EXEMPT ACCESS POLICY, EXEMPT REDACTION POLICY) can bypass the row and column access control policies enforced by Virtual Private Database and Data Redaction. Most administrative tasks do not require access to the data itself, so these privileges should be granted rarely even to administrators.

Name	Finding ID	Description
Write Access to Restricted Objects	PRIV.RESTRICTEDOBJ	Displays access to restricted objects granted to users. Users with these privileges can directly modify objects in the SYS, DVSYS, AUDSYS or LBACSYS schemas. Manipulating these system objects may allow security protections to be circumvented or otherwise interfere with normal operation of the database. Object permissions granted to PUBLIC must be restricted for objects in the SYS, DVSYS, AUDSYS or LBACSYS schemas.
Users Who Can Impersonate Other Users	PRIV.IMPERSONATEUSER	Displays the user accounts that have been granted rights to impersonate other users. The BECOME USER privilege and these PL/SQL packages (DBMS_AQADM_SYS, DBMS_AQADM_SYSCALLS, DBMS_IJOB, DBMS_PRVTAQIM, DBMS_REPCAT_SQL_UTL, DBMS_SCHEDULER, DBMS_STREAMS_ADM_UTL, DBMS_STREAMS_RPC, DBMS_SYS_SQL, INITJVMAUX, LTADM, WWV_DBMS_SQL, WWV_EXECUTE_IMMEDIATE) allow for execution of SQL code or external jobs using the identity of a different user. Access should be strictly limited and granted only to users with a legitimate need for this functionality.
Privilege for Data Exfiltration in Bulk	PRIV.EXFILTRATION	Displays the user accounts that have been granted rights to access or copy any data from a client or server. These PL/SQL packages (DBMS_BACKUP_RESTORE, UTL_DBWS, UTL_ORAMTS) can send data from the database using the network or file system. Access should be granted only to users with a legitimate need for this functionality.
Code Based Access Control	PRIV.CBAC	Displays all program units granted CBAC roles. Code Based Access Control(CBAC) can be used to grant additional privileges on program units. CBAC allows you to attach database roles to a PL/SQL function, procedure, or package. These database roles are enabled at run time, enabling the program unit to execute with the required privileges in the calling user's environment.
Java Permissions	PRIV.JAVAPERMISSIONS	Displays the user accounts that have been granted privileges to execute Java classes within the database. Java permission grants control the ability of database users to execute Java classes within the database server. A database user executing Java code must have both Java security permissions and database privileges to access resources within the database. These resources include database resources, such as tables and PL/SQL packages, operating system resources, such as files and sockets, Oracle JVM classes, and user-loaded classes. Make sure that these permissions are limited to the minimum required by each user.

The following figure displays an example of the Oracle Database Security Assessment Report — Privileges and Roles section.

Figure 1-6   Oracle Database Security Assessment Report — Privileges and Roles



System Privilege Grants

PRIV.SYSTEM

Ensure system privileges are granted only to necessary users

Status Evaluate

Summary 38 out of 53 users have been directly or indirectly granted system privileges via 2347 grants.
4 users are granted system privileges with admin option via 9 grants.
31 users are granted 296 system privileges directly.

Details

```
Users directly or indirectly granted each system privilege:

ADMINISTER ANY SQL TUNING SET: DBA_DEBRA, DBA_HARVEY, DBA_NICOLE,
    DMS_ADMIN, EVIL_RICH, JSCHAFFER(D), JTAYLOR, MASKING_ADMIN, SCOTT
ADMINISTER DATABASE TRIGGER: BACKUP_ADMIN, DBA_DEBRA, DBA_HARVEY,
    DBA_NICOLE, DMS_ADMIN, EVIL_RICH, JSCHAFFER(D), JTAYLOR, MASKING_ADMIN,
    SCOTT
ADMINISTER RESOURCE MANAGER: BACKUP_ADMIN, DBA_DEBRA, DBA_HARVEY,
    DBA_NICOLE, DMS_ADMIN, EVIL_RICH, JSCHAFFER(D), JTAYLOR, MASKING_ADMIN,
    SCOTT, SOE(D)
ADMINISTER SQL MANAGEMENT OBJECT: BACKUP_ADMIN, DBA_DEBRA, DBA_HARVEY,
...
(*) = granted with admin option
(D) = granted directly
(C) = granted commonly
```

Remarks System privileges provide the ability to access data or perform administrative operations for the entire database, and users granted system privileges are generally used to perform administrative work. Consistent with the principle of least privilege, you should grant these privileges sparingly. Privilege Analysis may help determine the minimum set of privileges required by a user or a role. In some cases, it may be possible to substitute a more limited object privilege grant instead of a system privilege (ANY) grant that applies to all objects.

Avoid granting system privileges with ADMIN OPTION. You should review users with system privileges to determine if they are used to perform administrative and general user responsibilities. You should provide users with administrative and general user responsibilities with separate accounts for each duty.

References Oracle Best Practice
CIS Benchmark: Recommendation 5.2.2, 5.2.10
DISA STIG: V-219834, V-220266, V-220312, V-237709

The Privileges and Roles section is followed by the Authorization Control section.

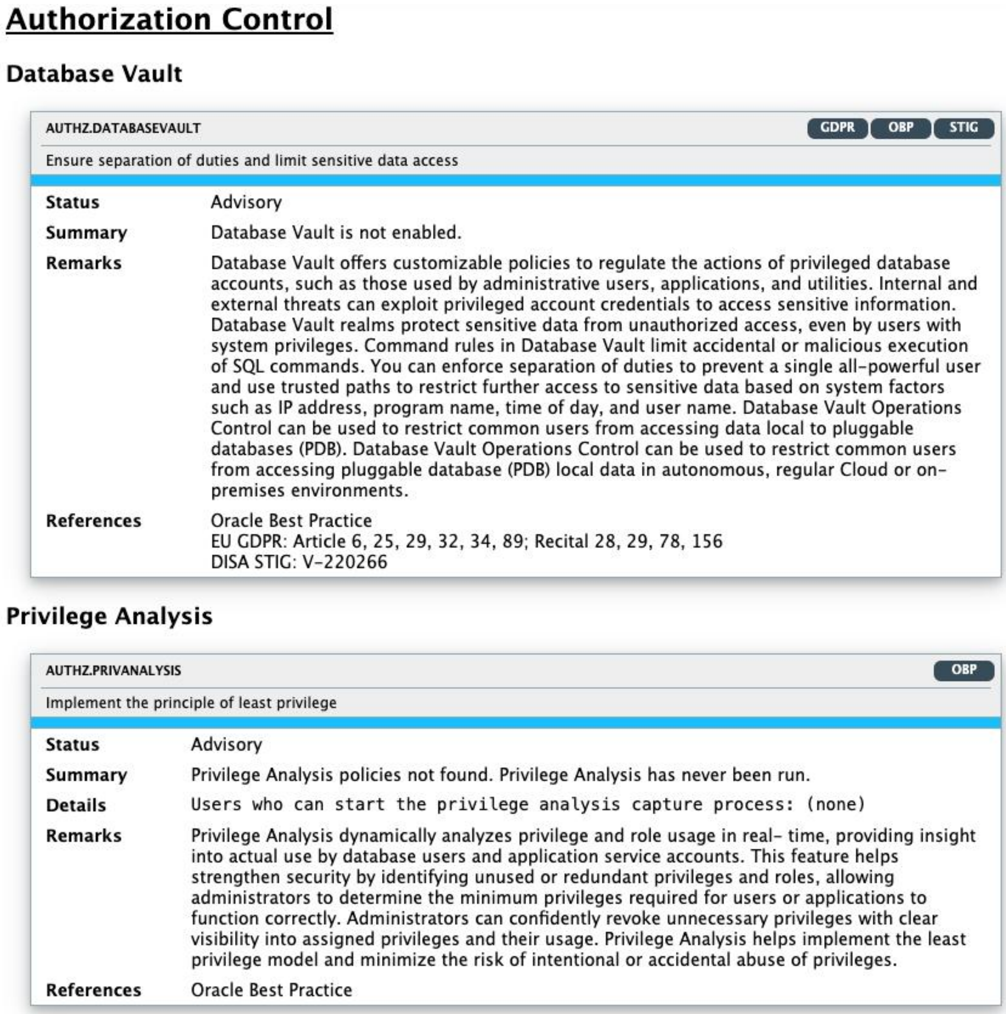
Oracle Database Security Assessment Report — Authorization Control

The Oracle Database Security Assessment Report — Authorization Control section displays the following information:

Name	Finding ID	Description
Database Vault	AUTHZ.DATABASEVAULT	Displays whether Oracle Database Vault is enabled and details existing protected objects, realms, command rules, and users granted Database Vault specific roles. Database Vault provides for configurable policies to control the actions of database accounts with elevated privileges such as those accounts used by administrative users, applications and utilities. Attacks (originating from external as well as internal sources) leverage privileged account credentials to access sensitive information. Database Vault realms prevent unauthorized access to sensitive data objects, even by user accounts with system privileges. Database Vault Command rules limit the accidental or malicious execution of SQL commands. You can use Database Vault to enforce separation of duties to prevent a single all powerful user. Also it provides trusted paths to further restrict access to sensitive data using system factors such as IP address, program name, time of day and user name. Database Vault operations control can be used to restrict common users from accessing pluggable database (PDB) local data in autonomous, regular Cloud, or on-premises environments.
Privilege Analysis	AUTHZ.PRIVANALYSIS	Displays Privilege Analysis policies and users with privileges to start the capture proces. Privilege Analysis records the privileges used during a real or simulated workload. After collecting data about the privileges that are actually used, this information can be used to revoke privilege grants that are no longer needed or to create roles with only the privileges that are used by the user or role. This helps implement Least Privilege Model and minimizes risk from intentional or accidental abuse of privileges.
Authentication for Client Scripts	AUTHZ.PASSWORDSCRIPTS	Lists password-authenticated users whose passwords can potentially be embedded in client scripts, jobs, and application source code to connect to the database server.
Data Masking	AUTHZ.DATAMASKING	Lists tables with sensitive data that should be masked when transferred to non-production systems. This check lists tables marked sensitive by TSDP or in `DBA_TABLES` and users that can transfer data via `DATAPUMP_EXP_FULL_DATABASE` or `DATAPUMP_IMP_FULL_DATABASE`.
PKI Based Authentication	AUTHZ.PKI	List user accounts identified externally where the authentication method is TCPS. This finding is targeting mostly customers looking for STIG compliance.

The following figure displays an example of the Oracle Database Security Assessment Report — Authorization Control section.

Figure 1-7 Oracle Database Security Assessment Report — Authorization Control



Authorization Control

Database Vault

AUTHZ.DATABASEVAULT

Ensure separation of duties and limit sensitive data access

Status	Advisory
Summary	Database Vault is not enabled.
Remarks	Database Vault offers customizable policies to regulate the actions of privileged database accounts, such as those used by administrative users, applications, and utilities. Internal and external threats can exploit privileged account credentials to access sensitive information. Database Vault realms protect sensitive data from unauthorized access, even by users with system privileges. Command rules in Database Vault limit accidental or malicious execution of SQL commands. You can enforce separation of duties to prevent a single all-powerful user and use trusted paths to restrict further access to sensitive data based on system factors such as IP address, program name, time of day, and user name. Database Vault Operations Control can be used to restrict common users from accessing data local to pluggable databases (PDB). Database Vault Operations Control can be used to restrict common users from accessing pluggable database (PDB) local data in autonomous, regular Cloud or on-premises environments.
References	Oracle Best Practice EU GDPR: Article 6, 25, 29, 32, 34, 89; Recital 28, 29, 78, 156 DISA STIG: V-220266

Privilege Analysis

AUTHZ.PRIVANALYSIS

Implement the principle of least privilege

Status	Advisory
Summary	Privilege Analysis policies not found. Privilege Analysis has never been run.
Details	`Users who can start the privilege analysis capture process: (none)`
Remarks	Privilege Analysis dynamically analyzes privilege and role usage in real- time, providing insight into actual use by database users and application service accounts. This feature helps strengthen security by identifying unused or redundant privileges and roles, allowing administrators to determine the minimum privileges required for users or applications to function correctly. Administrators can confidently revoke unnecessary privileges with clear visibility into assigned privileges and their usage. Privilege Analysis helps implement the least privilege model and minimize the risk of intentional or accidental abuse of privileges.
References	Oracle Best Practice

The Authorization Control section is followed by the Fine-Grained Access Control section.

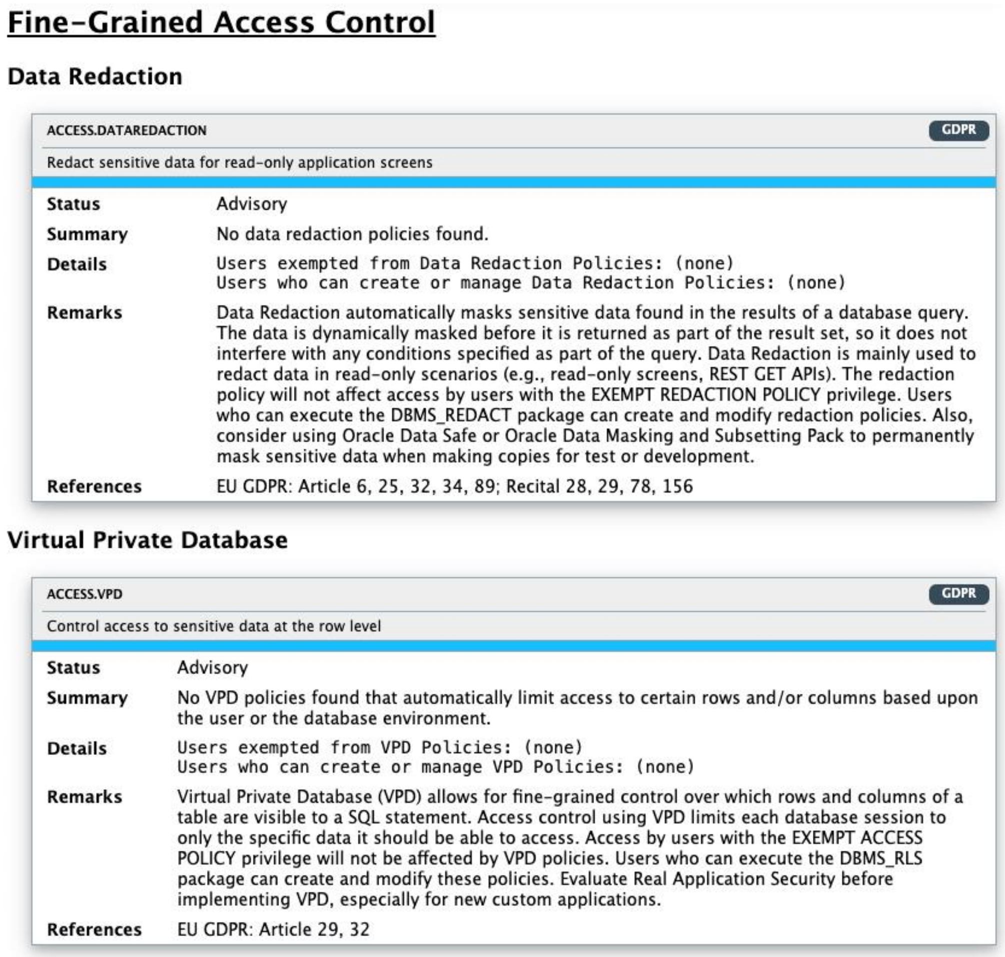
Oracle Database Security Assessment Report — Fine-Grained Access Control

The Oracle Database Security Assessment Report — Fine-Grained Access Control section displays the following information:

Name	Finding ID	Description
Data Redaction	ACCESS.DATAREDACTION	Displays information on Data Redaction policies, exempted users, and execute grants on the DBMS_REDACT package. Data Redaction automatically masks sensitive data found in the results of a database query.
Virtual Private Database	ACCESS.VPD	Displays information on Virtual Private Database policies, exempted users, and execute grants on the DBMS_RLS package. VPD allows for fine-grained control over the rows and columns of a table are visible to a SQL statement.
Real Application Security	ACCESS.RAS	Displays information on Real Application Security policies, exempted users, and users granted ADMIN_SEC_POLICY and APPLY_SEC_POLICY. Real Application Security (RAS) is a more modern, advanced version of Virtual Private Database and provides fine-grained control over the rows and columns of a table that are visible to a SQL statement.
Label Security	ACCESS.LABELSECURITY	Displays whether Oracle Label Security is enabled. Oracle Label Security provides the ability to tag data with a data label or a data classification. Access to sensitive data is controlled by comparing the data label with the requesting user's label or security clearance.
Transparent Sensitive Data Protection	ACCESS.TSDP	Displays information on Transparent Sensitive Data policies and the users that can manage it. TSDP was introduced in Oracle Database 12.1, and allows a data type to be associated with each column that contains sensitive data. TSDP can then apply various data security features to all instances of a particular type so that protection is uniform and consistent.

The following figure displays an example of the OracleDatabase Security Assessment Report — Fine-Grained Access Control section.

Figure 1-8   Oracle Database Security Assessment Report — Fine-Grained Access Control



Fine-Grained Access Control

Data Redaction

ACCESS.DATAREDACTION

Redact sensitive data for read-only application screens

Status	Advisory
Summary	No data redaction policies found.

Details	`Users exempted from Data Redaction Policies: (none)`
	`Users who can create or manage Data Redaction Policies: (none)`

Remarks	Data Redaction automatically masks sensitive data found in the results of a database query. The data is dynamically masked before it is returned as part of the result set, so it does not interfere with any conditions specified as part of the query. Data Redaction is mainly used to redact data in read-only scenarios (e.g., read-only screens, REST GET APIs). The redaction policy will not affect access by users with the EXEMPT REDACTION POLICY privilege. Users who can execute the DBMS_REDACT package can create and modify redaction policies. Also, consider using Oracle Data Safe or Oracle Data Masking and Subsetting Pack to permanently mask sensitive data when making copies for test or development.
References	EU GDPR: Article 6, 25, 32, 34, 89; Recital 28, 29, 78, 156

Virtual Private Database

ACCESS.VPD

Control access to sensitive data at the row level

Status	Advisory
Summary	No VPD policies found that automatically limit access to certain rows and/or columns based upon the user or the database environment.

Details	`Users exempted from VPD Policies: (none)`
	`Users who can create or manage VPD Policies: (none)`

Remarks	Virtual Private Database (VPD) allows for fine-grained control over which rows and columns of a table are visible to a SQL statement. Access control using VPD limits each database session to only the specific data it should be able to access. Access by users with the EXEMPT ACCESS POLICY privilege will not be affected by VPD policies. Users who can execute the DBMS_RLS package can create and modify these policies. Evaluate Real Application Security before implementing VPD, especially for new custom applications.
References	EU GDPR: Article 29, 32

The Fine-Grained Access Control section is followed by the Auditing section.

Oracle Database Security Assessment Report — Auditing

The Oracle Database Security Assessment Report — Auditing section displays the following information:

Name	Finding ID	Description
Audit Management Configuration Parameters	-	Displays information on audit management configuration parameters

Name	Finding ID	Description
Audit Records	AUDIT.ENABLED	Displays information about audit trails. Auditing is an essential component for securing any system. The audit trail allows for monitoring the activities of highly privileged users.
Unified Audit Policies	AUDIT.UNIFIEDPOLICIES	Displays whether unified audit policies are enabled. Unified Audit, available in Oracle Database 12.1 and later releases, combines multiple audit trails into a single unified view. It also introduces new syntax for specifying effective audit policies.
Fine Grained Audit	AUDIT.FGA	Displays whether fine grained audit policies are enabled. Fine Grained Audit policies can record highly specific activity, such as access to particular table columns or access that occurs under specified conditions. This is a useful way to monitor unexpected data access while avoiding unnecessary audit records that correspond to normal activity.
Audit Administrative (SYS*) Users	AUDIT.ADMINACTIONS	Displays whether the actions of the `SYS` user are audited by enabled audit policies. It is important to audit administrative actions performed by the `SYS` user. Traditional audit policies do not apply to `SYS`, so the `AUDIT_SYS_OPERATIONS` parameter must be set to record `SYS` actions to a separate audit trail.
Audit User Logon and Logoff	AUDIT.CONNECTIONS	Displays whether Database connections are audited by enabled audit policies. Successful user connections to the database should be audited to assist with future forensic analysis. Unsuccessful connection attempts can provide early warning of an attacker's attempt to gain access to the database.
Audit Database Management Activities	AUDIT.DBMGMT	Displays whether the actions related to database management are audited by enabled audit policies. Actions that affect the management of database features should always be audited. Each action or privilege listed should be included in at least one enabled audit policy.
Audit Account Management Activities	AUDIT.ACCOUNTMGMT	Displays whether account management activities are audited.
Audit System Privileges	AUDIT.SYSTEMPRIVS	Displays information on whether system privileges are audited by enabled audit policies.
Audit Roles with System Privileges	AUDIT.ROLESYSTEMPRIVS	Displays information about unified audit policies that audit roles with system privileges.
Audit Privilege Management	AUDIT.PRIVMGMT	Displays whether the actions related to privilege management are audited by enabled audit policies. Granting additional privileges to users or roles potentially affects most security protections and should be audited. Each action or privilege listed should be included in at least one enabled audit policy.

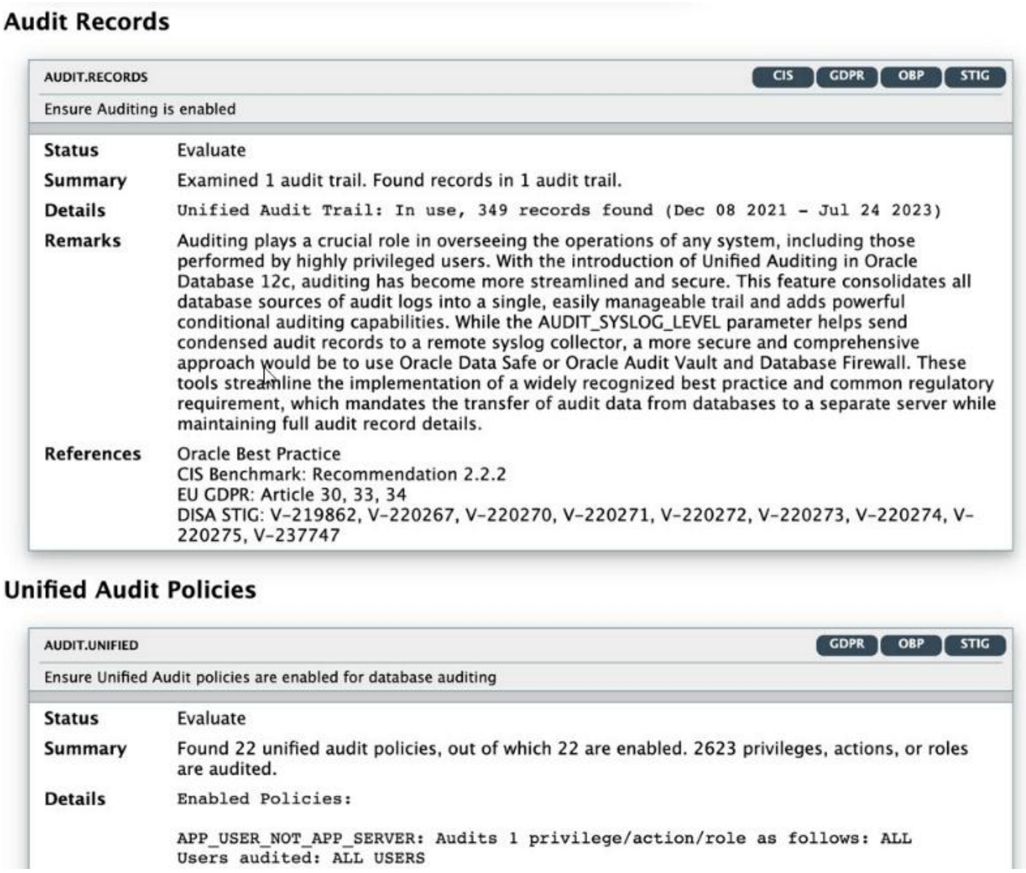
Name	Finding ID	Description
Audit SQL Statements	AUDIT.STATEMENT	Displays information about SQL statements audited by enabled audit policies. Applies to targets with Traditional Auditing policies.
Audit Object Actions	AUDIT.SENSITIVEOBJS	Displays information about the object access audited by enabled audit policies.
Audit Synonym Management Activities	AUDIT.SYNONYMS	Displays information on whether synonym management activities (CREATE ANY SYNONYM, CREATE PUBLIC SYNONYM, CREATE SYNONYM, DROP PUBLIC SYNONYM, DROP SYNONYM) are audited.
Audit Conditions	AUDIT.CONDITION	Lists all audit policies with conditions and, if enabled, lists users/roles it's enabled for.
Audit Shared Accounts	AUDIT.SHAREDPROXY	Checks to see if users listed in USER.SHARED are being audited.
Audit Storage	AUDIT.TABLESPACE	Displays information about tablespaces used by different audit trails. Checks include: • Audit trail is SYSTEM • Audit trail is SYSAUX • Tablespace is non-autoextensible & 80% or more full (MEDIUM) • Tablespace is non-autoextensible & 90% or more full (HIGH)
Audit Trail Cleanup	AUDIT.CLEANUPJOBS	Lists enabled jobs that cleanup audit trails and checks cleanup jobs that are not present
Audit Data Pump	AUDIT.DATAPUMP	Displays whether data pump exports and imports are being audited.
Audit STIG Actions	AUDIT.STIGPOLICY	Oracle provides out-of-the-box audit policies that aim to answer DoD- auditable events requirements - `ORA_STIG_RECOMMENDATIONS`, `ORA_ALL_TOPLEVEL_ACTIONS` and `ORA_LOGON_LOGOFF`. This check will validate if these policies are audited.
Audit Database Vault	AUDIT.DATABASEVAULT	Displays users that can administer Database Vault but are not audited and lists policies enabled to audit Database Vault actions
Audit Oracle Label Security	AUDIT.LABELSECURITY	Displays information regarding enabled audit policies used to audit OLS. • Checks to see if Oracle Label Security (OLS) is enabled and no audit policy is found with OLS action • Reports if OLS is enabled and audit policies were found for OLS actions

Note:

The details of the audit findings can vary depending on whether the database has unified audit or traditional audit in place. Starting in Oracle Database 12.2, the best practice is to use Unified Audit.

The following figure displays an example of the Oracle Database Security Assessment Report — Auditing section.

Figure 1-9   Oracle Database Security Assessment Report — Auditing



Audit Records

AUDIT.RECORDS

Ensure Auditing is enabled

Status	Evaluate
Summary	Examined 1 audit trail. Found records in 1 audit trail.
Details	`Unified Audit Trail: In use, 349 records found (Dec 08 2021 - Jul 24 2023)`
Remarks	Auditing plays a crucial role in overseeing the operations of any system, including those performed by highly privileged users. With the introduction of Unified Auditing in Oracle Database 12c, auditing has become more streamlined and secure. This feature consolidates all database sources of audit logs into a single, easily manageable trail and adds powerful conditional auditing capabilities. While the AUDIT_SYSLOG_LEVEL parameter helps send condensed audit records to a remote syslog collector, a more secure and comprehensive approach would be to use Oracle Data Safe or Oracle Audit Vault and Database Firewall. These tools streamline the implementation of a widely recognized best practice and common regulatory requirement, which mandates the transfer of audit data from databases to a separate server while maintaining full audit record details.
References	Oracle Best Practice CIS Benchmark: Recommendation 2.2.2 EU GDPR: Article 30, 33, 34 DISA STIG: V-219862, V-220267, V-220270, V-220271, V-220272, V-220273, V-220274, V-220275, V-237747

Unified Audit Policies

AUDIT.UNIFIED

Ensure Unified Audit policies are enabled for database auditing

Status	Evaluate
Summary	Found 22 unified audit policies, out of which 22 are enabled. 2623 privileges, actions, or roles are audited.

Details	`Enabled Policies:`
	
	`APP_USER_NOT_APP_SERVER: Audits 1 privilege/action/role as follows: ALL`
	`Users audited: ALL USERS`

The Auditing section is followed by the Encryption section.

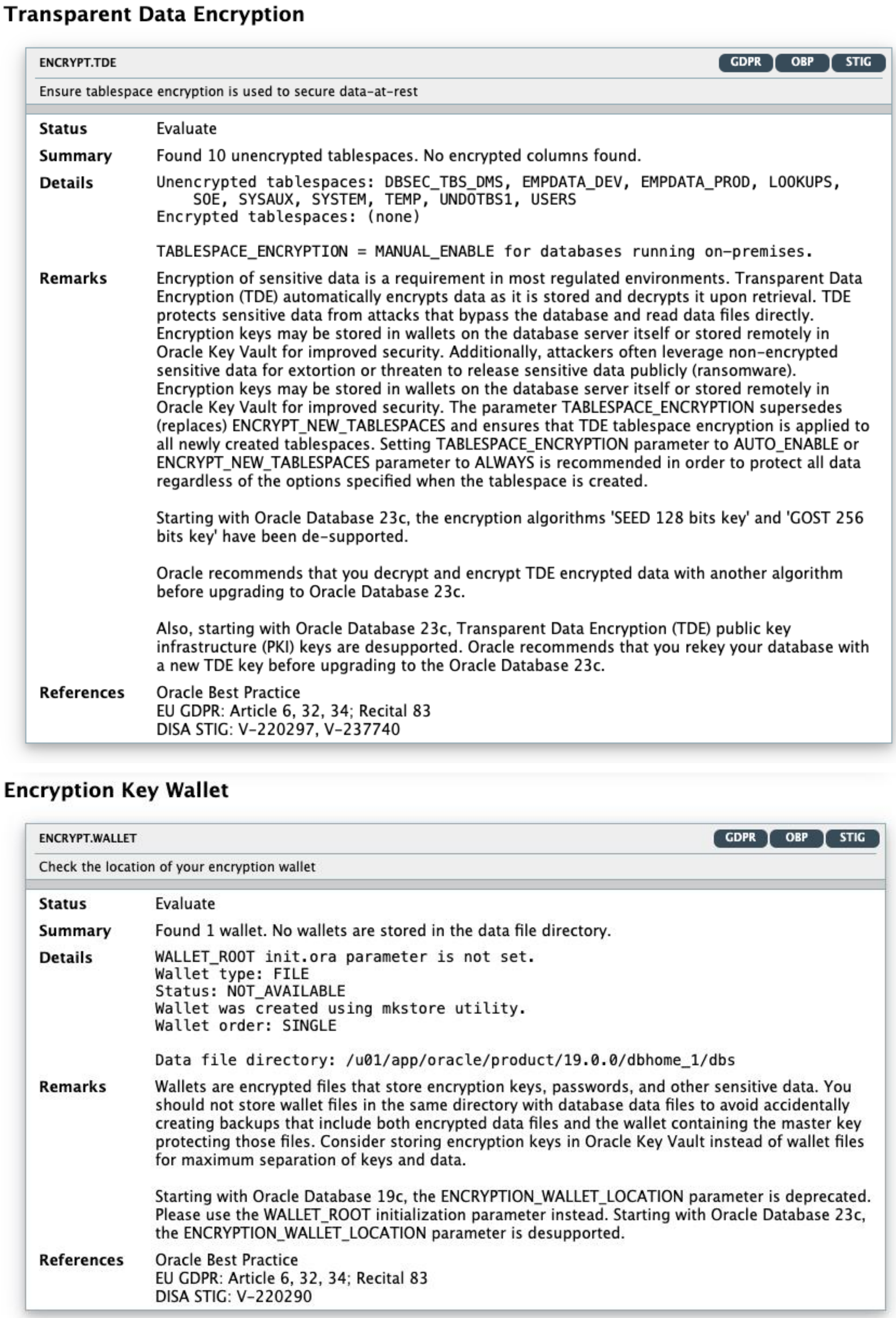
Oracle Database Security Assessment Report — Encryption

The Oracle Database Security Assessment Report — Encryption section displays the following information:

Name	Finding ID	Description
Transparent Data Encryption	ENCRYPT.TDE	Displays whether column or tablespace encryption is in use. Also, shows encrypted and unencrypted tablespaces along with the number of days since the master encryption key was last rotated. Encryption of sensitive data is a requirement in most regulated environments. Transparent Data Encryption automatically encrypts data as it is stored and decrypts it upon retrieval. This protects sensitive data from attacks that bypass the database and read data files directly.
Encryption Key Wallet	ENCRYPT.WALLET	Displays wallet information. Wallets are encrypted files used to store encryption keys, passwords, and other sensitive data. Wallet files should not be stored in the same directory with database data files, to avoid accidentally creating backups that include both encrypted data files and the wallet containing the master key protecting those files. For maximum separation of keys and data, consider storing encryption keys in Oracle Key Vault instead of wallet files.
FIPS Mode for TDE and DBMS_CRYPTO	ENCRYPT.DBFIPS	Displays information whether TDE and DBMS_CRYPTYO run in a FIPS-compliant mode. Federal Information Processing Standard (140-2) is a U.S. government security standard that specifies security requirements. It is used to approve cryptographic modules. Setting parameter DBFIPS_140 = TRUE enables Transparent Data Encryption (TDE) and DBMS_CRYPTO PL/SQL package program units to run in a FIPS-compliant mode. FIPS mode is mostly used by departments and agencies of the United States federal government looking to meet FIPS and/or STIG compliance. Be aware that this setting and thus using the underlying FIPS-certified library incurs a slight amount of overhead when the library is first loaded. This is due to the verification of the library signature and the execution of the self-test.
FIPS mode for TLS	ENCRYPT.TLSFIPS	Federal Information Processing Standard (140-2) is a U.S. government security standard that specifies security requirements. The SSLFIPS_140 parameter configures the Transport Layer Security (TLS) adapter to run in FIPS mode. SSLFIPS_LIB sets the location of the FIPS library.

The following figure displays an example of the Oracle Database Security Assessment Report — Encryption section.

Figure 1-10 Oracle Database Security Assessment Report — Encryption and Encryption Key Wallets



Transparent Data Encryption

ENCRYPT.TDE

Ensure tablespace encryption is used to secure data-at-rest

Status Evaluate

Summary Found 10 unencrypted tablespaces. No encrypted columns found.

Details

```
Unencrypted tablespaces: DBSEC_TBS_DMS, EMPDATA_DEV, EMPDATA_PROD, LOOKUPS,
    SOE, SYSAUX, SYSTEM, TEMP, UNDOTBS1, USERS
Encrypted tablespaces: (none)

TABLESPACE_ENCRYPTION = MANUAL_ENABLE for databases running on-premises.
```

Remarks Encryption of sensitive data is a requirement in most regulated environments. Transparent Data Encryption (TDE) automatically encrypts data as it is stored and decrypts it upon retrieval. TDE protects sensitive data from attacks that bypass the database and read data files directly. Encryption keys may be stored in wallets on the database server itself or stored remotely in Oracle Key Vault for improved security. Additionally, attackers often leverage non-encrypted sensitive data for extortion or threaten to release sensitive data publicly (ransomware). Encryption keys may be stored in wallets on the database server itself or stored remotely in Oracle Key Vault for improved security. The parameter TABLESPACE_ENCRYPTION supersedes (replaces) ENCRYPT_NEW_TABLESPACES and ensures that TDE tablespace encryption is applied to all newly created tablespaces. Setting TABLESPACE_ENCRYPTION parameter to AUTO_ENABLE or ENCRYPT_NEW_TABLESPACES parameter to ALWAYS is recommended in order to protect all data regardless of the options specified when the tablespace is created.

Starting with Oracle Database 23c, the encryption algorithms 'SEED 128 bits key' and 'GOST 256 bits key' have been de-supported.

Oracle recommends that you decrypt and encrypt TDE encrypted data with another algorithm before upgrading to Oracle Database 23c.

Also, starting with Oracle Database 23c, Transparent Data Encryption (TDE) public key infrastructure (PKI) keys are desupported. Oracle recommends that you rekey your database with a new TDE key before upgrading to the Oracle Database 23c.

References Oracle Best Practice
EU GDPR: Article 6, 32, 34; Recital 83
DISA STIG: V-220297, V-237740

Encryption Key Wallet

ENCRYPT.WALLET

Check the location of your encryption wallet

Status Evaluate

Summary Found 1 wallet. No wallets are stored in the data file directory.

Details

```
WALLET_ROOT init.ora parameter is not set.
Wallet type: FILE
Status: NOT_AVAILABLE
Wallet was created using mkstore utility.
Wallet order: SINGLE

Data file directory: /u01/app/oracle/product/19.0.0/dbhome_1/dbs
```

Remarks Wallets are encrypted files that store encryption keys, passwords, and other sensitive data. You should not store wallet files in the same directory with database data files to avoid accidentally creating backups that include both encrypted data files and the wallet containing the master key protecting those files. Consider storing encryption keys in Oracle Key Vault instead of wallet files for maximum separation of keys and data.

Starting with Oracle Database 19c, the ENCRYPTION_WALLET_LOCATION parameter is deprecated. Please use the WALLET_ROOT initialization parameter instead. Starting with Oracle Database 23c, the ENCRYPTION_WALLET_LOCATION parameter is desupported.

References Oracle Best Practice
EU GDPR: Article 6, 32, 34; Recital 83
DISA STIG: V-220290

The Encryption section is followed by the Database Configuration section.

Oracle Database Security Assessment Report — Database Configuration

The Oracle Database Security Assessment Report — Database Configuration section displays the following information:

Name	Finding ID	Description
Initialization Parameters for Security	-	Displays security related Database initialization parameters and their values.
Pre-Authenticated Request URL	CONF.PREAUTHREQUESTURL	Displays pre-authenticated URL information for Autonomous Database Serverless databases including who can manage them via the DBMS_DATA_ACCESS package.
Authentication Configuration	CONF.AUTHN	Displays information about the user account initialization parameters. SEC_MAX_FAILED_LOGIN_ATTEMPTS configures the maximum number of failed login attempts in a single session before the connection is closed. This is independent of the user profile parameter FAILED_LOGIN_ATTEMPTS, which controls locking the user account after multiple failed login attempts. RESOURCE_LIMIT should be set to TRUE to enable enforcement of any resource constraints set in user profiles.
PDB OS User	CONF.DEFAULTPDBOSUSER	Checks if the highly privileged Oracle OS user is set for the PDB_OS_CREDENTIAL parameter.
Control Files	CONF.CONTROLFILES	Checks if control files are multiplexed and lists all the control file locations. The REMOTE_LOGIN_PASSWORDFILE set to EXCLUSIVE, allows passwords to be updated using the ALTER USER command.
PDB OS User	CONF.DEFAULTPDBOSUSER	Checks if the highly privileged Oracle OS user is set for the PDB_OS_CREDENTIAL parameter.
Redo Log Files	CONF.REDOLOGS	Checks if the defined redo log files follow best practices and lists their location. Redo logs should be multiplexed and stored on different physical disks.
Archive Log Mode	CONF.ARCHIVELOG	Checks if the database is in ARCHIVELOG or NOARCHIVELOG mode. If set, also displays the archive_log_destination or the recovery_file_destination. Also displays the archive_log_destination or the recovery_file_destination for the standalone databases.

Name	Finding ID	Description
Database Backup	CONF.BACKUP	Displays information about Database backup records. Database should be backed up regularly to prevent loss of data in the event of a system failure. Oracle Recovery Manager (RMAN) allows performing backup and recovery tasks on your databases. Unencrypted backup data should not be transported on tape or disk to offsite storage for safekeeping.
Instance Name Check	CONF.INSTANCENAME	Displays whether the instance name contains the Database version number. Instance names should not contain Oracle version numbers. Service names may be discovered by unauthenticated users. If the service name includes version numbers or other database product information, a malicious user may use that information to develop a targeted attack.
SQL Firewall	CONF.SQLFIREWALL	Checks if SQL Firewall is enabled and displays the users that are affected by the policy and whether the policy is in observing, blocking, or enforcing mode. Also, details if the SQL and context allow-lists are in enforcement mode or not. Only applicable to Oracle Database versions >=23ai.
Read-only ORACLE_HOME	CONF.READONLYHOME	Checks if the ORACLE_HOME is read-only. Only applicable to Oracle Database versions >=18c.
Access to Dictionary Objects	CONF.SYSOBJ	Displays whether access to dictionary objects is properly limited. When O7_DICTIONARY_ACCESSIBILITY is set to FALSE, tables owned by SYS are not affected by the ANY TABLE system privileges. This parameter should always be set to FALSE because tables owned by SYS control the overall state of the database and should not be subject to manipulation by users with ANY TABLE privileges.
Inference of Table Data	CONF.SQL92SECURITY	Displays whether data inference attacks are properly blocked. When SQL92_SECURITY is set to TRUE, UPDATE and DELETE statements that refer to a column in their WHERE clauses will succeed only when the user has the privilege to SELECT from the same column. This parameter should be set to TRUE so that this requirement is enforced in order to prevent users from inferring the value of a column which they do not have the privilege to view.
Access to Password File	CONF.PASSWORDFILE	Displays whether the password file is configured correctly. The REMOTE_LOGIN_PASSWORDFILE set to EXCLUSIVE allows the password file to contain distinct entries for each administrative user allowing them to be individually audited and tracked for their actions. It also allows passwords to be updated using the ALTER USER command.

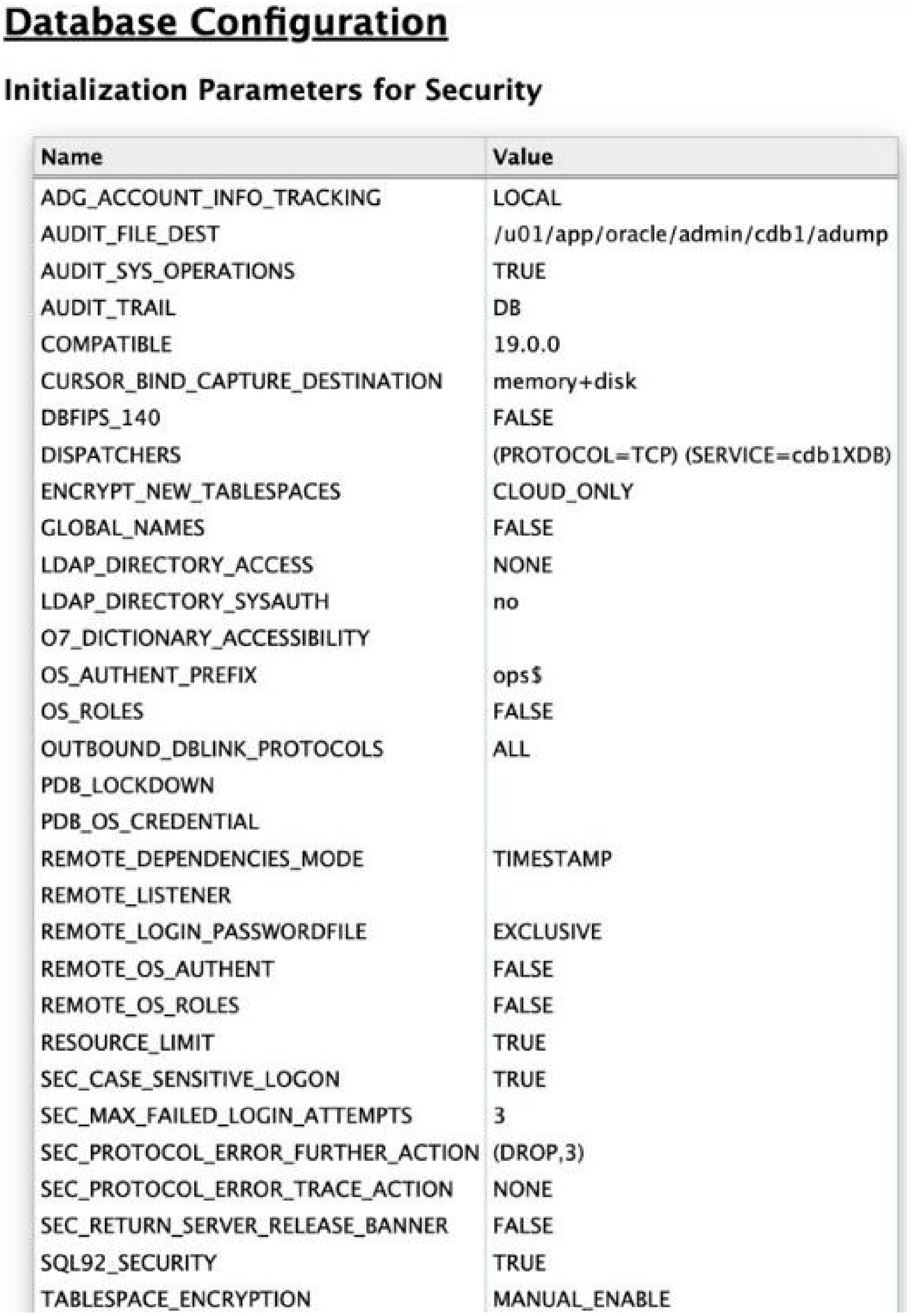
Name	Finding ID	Description
Network Communication	CONF.NETWORK	Displays information about initialization parameters that determine the database server response to malformed packets. Also, includes details on usage of a remote listener and if database server version information is hidden from unauthenticated client requests. `REMOTE_LISTENER` allows a network listener running on another system to be used. This parameter should normally be unset to ensure that the local listener is used. The `SEC_PROTOCOL_ERROR` parameters control the database server's response when it receives malformed network packets from a client. Because these malformed packets may indicate an attempted attack by a malicious client, the parameters should be set to log the incident and terminate the connection. `SEC_RETURN_SERVER_RELEASE_BANNER` should be set to `FALSE` to limit the information that is returned to an unauthenticated client, which could be used to help determine the server's vulnerability to a remote attack.
External OS Authentication	CONF.EXTERNALOSAUTH	Displays whether the Oracle Database roles are defined and managed by the database itself or by the host operating system (for local and remote authentication). The `OS_ROLES` parameter determines whether roles granted to users are controlled by `GRANT` statements in the database or by the database server's operating system. `REMOTE_OS_AUTHENT` and `REMOTE_OS_ROLES` allow the client operating system to set the database user and roles. All of these parameters should be set to `FALSE` so that the authorizations of database users are managed by the database itself.
Unused Components	CONF.DBCOMPONENTS	Checks to see if components like XOQ, CONTEXT, SDO, DV, OLS are installed/enabled and not being used.
Job Details	CONF.JOBS	Checks the scheduled database jobs and users who can administer them. Checks include: • Users who can create database jobs • Jobs that can use privileges of DBA/PDB_DBA
Triggers	CONF.TRIGGERS	Displays information about logon triggers. A trigger is code that executes whenever a specific event occurs, such as inserting data in a table or connecting to the database. Disabled triggers are a potential cause for concern because whatever protection or monitoring they may be expected to provide is not active.
Disabled Constraints	CONF.CONSTRAINTS	Displays information about disabled constraints. Constraints are used to enforce and guarantee specific relationships between data items stored in the database. Disabled constraints are a potential cause for concern because the conditions they ensure are not enforced.

Name	Finding ID	Description
External Procedures	CONF.EXTERNALPROCS	Displays information about external procedures and services. External procedures allow code written in other languages to be executed from PL/SQL. Note that modifications to external code cannot be controlled by the database. Be careful to ensure that only trusted code libraries are available to be executed. Although the database can spawn its own process to execute the external procedure, it is advisable to configure a listener service for this purpose so that the external code can run as a less-privileged OS user. The listener configuration should set `EXTPROC_DLLS` to identify the specific shared library code that can be executed rather than using the default value `ANY`.
Source Code Analysis	CONF.SOURCEANALYSIS	Checks `DBA_SOURCE` for non-oracle maintained procedures and functions using `RAISE_APPLICATION_ERROR` and `DBMS_OUTPUT.PUT_LINE`.
Directory Objects	CONF.DIRECTORYOBJ	Displays information about directory objects. Directory objects allow access to the server's file system from PL/SQL code within the database. Access to files that are used by the database kernel itself should not be permitted, as this may alter the operation of the database and bypass its access controls.
Database Links	CONF.DATABASELINKS	Displays information about database links. Database links allow users to execute SQL statements that access tables in other databases. This allows for both querying and storing data on the remote database. It is advisable to set `GLOBAL_NAMES` to `TRUE` in order to ensure that link names match the databases they access.
Network Access Control	CONF.NETWORKACL	Displays information about Network Access Control Lists (ACLs). Network ACLs control the external servers that database users can access using network packages such as UTL_TCP and UTL_HTTP. Specifically, a database user needs the connect privilege to an external network host computer if he or she is connecting using the `UTL_TCP`, `UTL_HTTP`, `UTL_SMTP`, and `UTL_MAIL` utility packages. To convert between a host name and its IP address using the `UTL_INADDR` package, the `Resolve` privilege is required. Make sure that these permissions are limited to the minimum required by each user.

Name	Finding ID	Description
XML Database Access Control	CONF.XMLACL	Displays information about XML Database Access Control Lists (ACLs). XML ACLs control access to database resources using the XML DB feature. Every resource in the Oracle XML DB Repository hierarchy has an associated ACL. The ACL mechanism specifies a privilege-based access control for resources to principals, which are database users or roles. Whenever a resource is accessed, a security check is performed, and the ACL determines if the requesting user has sufficient privileges to access the resource. Make sure that these privileges are limited to the minimum required by each user.
File System Access	CONF.FILESYS	Checks for `UTL_FILE_DIR` for older database versions where the parameter is not deprecated.
Trace Files	CONF.TRACEFILELIMIT	Displays information about the initialization parameters for trace files. The hidden parameter `_TRACE_FILES_PUBLIC` determines whether trace files generated by the database should be accessible to all OS users. Since these files may contain sensitive information, access should be limited by setting this parameter to `FALSE`.

The following figure displays an example of the Oracle Database Security Assessment Report — Database Configuration section.

Figure 1-11 Oracle Database Security Assessment Report — Database Configuration



Database Configuration

Initialization Parameters for Security

Name	Value
ADG_ACCOUNT_INFO_TRACKING	LOCAL
AUDIT_FILE_DEST	/u01/app/oracle/admin/cdb1/adump
AUDIT_SYS_OPERATIONS	TRUE
AUDIT_TRAIL	DB
COMPATIBLE	19.0.0
CURSOR_BIND_CAPTURE_DESTINATION	memory+disk
DBFIPS_140	FALSE
DISPATCHERS	(PROTOCOL=TCP) (SERVICE=cdb1XDB)
ENCRYPT_NEW_TABLESPACES	CLOUD_ONLY
GLOBAL_NAMES	FALSE
LDAP_DIRECTORY_ACCESS	NONE
LDAP_DIRECTORY_SYSAUTH	no
O7_DICTIONARY_ACCESSIBILITY	
OS_AUTHENT_PREFIX	ops$
OS_ROLES	FALSE
OUTBOUND_DBLINK_PROTOCOLS	ALL
PDB_LOCKDOWN	
PDB_OS_CREDENTIAL	
REMOTE_DEPENDENCIES_MODE	TIMESTAMP
REMOTE_LISTENER	
REMOTE_LOGIN_PASSWORDFILE	EXCLUSIVE
REMOTE_OS_AUTHENT	FALSE
REMOTE_OS_ROLES	FALSE
RESOURCE_LIMIT	TRUE
SEC_CASE_SENSITIVE_LOGON	TRUE
SEC_MAX_FAILED_LOGIN_ATTEMPTS	3
SEC_PROTOCOL_ERROR_FURTHER_ACTION	(DROP,3)
SEC_PROTOCOL_ERROR_TRACE_ACTION	NONE
SEC_RETURN_SERVER_RELEASE_BANNER	FALSE
SQL92_SECURITY	TRUE
TABLESPACE_ENCRYPTION	MANUAL_ENABLE

The Database Configuration section is followed by the Network Configuration section.

Oracle Database Security Assessment Report — Network Configuration

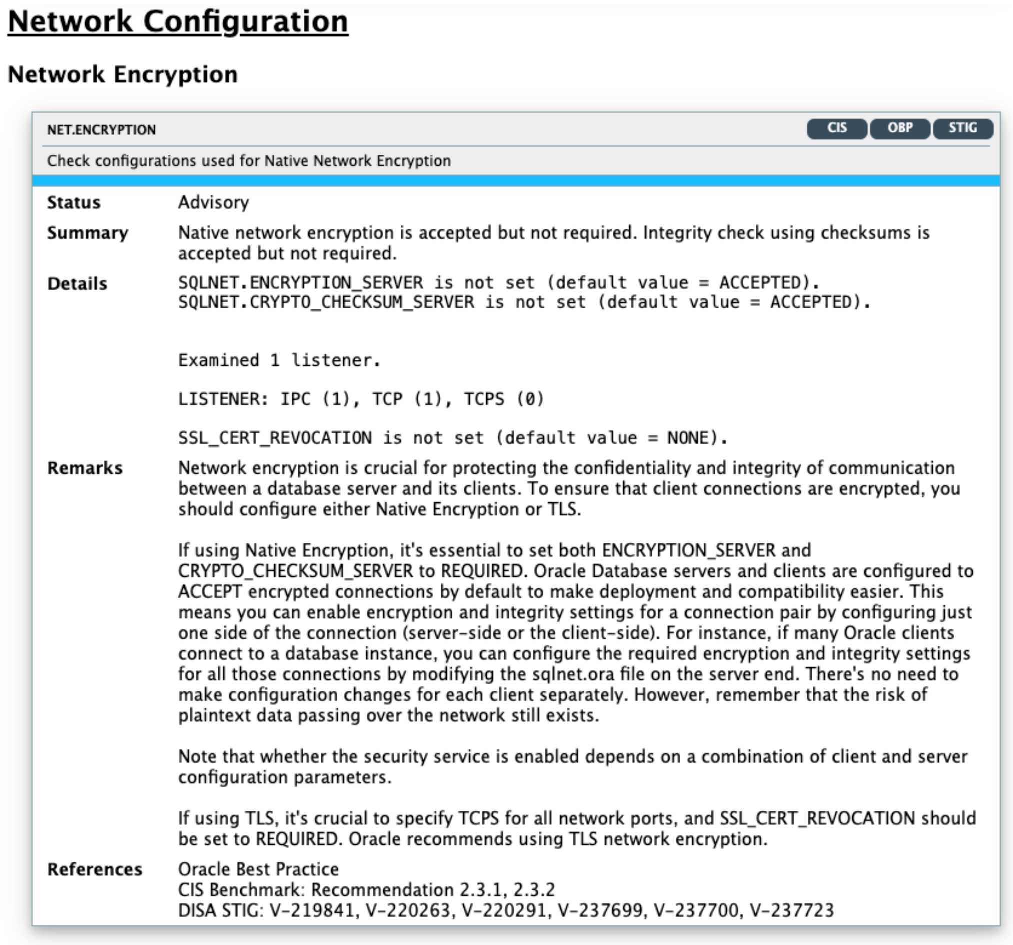
The Oracle Database Security Assessment Report — Network Configuration section displays the following information:

Name	Finding ID	Description
Network Encryption	NET.ENCRYPTION	Displays information about network encryption. Network encryption protects the confidentiality and integrity of communication between the database server and its clients. Either Native Encryption or TLS should be enabled. For Native Encryption, both `ENCRYPTION_SERVER` and `CRYPTO_CHECKSUM_SERVER` should be set to `REQUIRED`. If TLS is used, TCPS should be specified for all network ports and `SSL_CERT_REVOCATION` should be set to `REQUIRED`.
Client Nodes	NET.INVITEDNODES	Displays whether the database accepts connections from any client. `TCP.VALIDNODE_CHECKING` should be enabled to control which client nodes can connect to the database server. Either an allowlist of client nodes allowed to connect (`TCP.INVITED_NODES`) or a blocklist of nodes that are not allowed (`TCP.EXCLUDED_NODES`) may be specified. Configuring both lists is an error; only the invited node list will be used in this case.
Connection Limits Configuration	NET.CONNECTIONLIMITS	Check value of parameters governing termination of unauthenticated connections: • SQLNET.INBOUND_CONNECT_TIMEOUT • INBOUND_CONNECT_TIMEOUT_LISTENER • SQLNET.EXPIRE_TIME
Network Listener Configuration	NET.LISTENERCONFIG	Displays information about network listener configuration. These parameters are used to limit changes to the network listener configuration. `ADMIN_RESTRICTIONS` should be enabled to prevent parameter changes to the running listener. One of the following restrictions on service registration should be implemented: • Prevent changes by disabling `DYNAMIC_REGISTRATION` • Limit the nodes that can make changes by enabling `VALID_NODE_CHECKING_REGISTRATION` • Limit the network sources for changes using the `COST` parameters `SECURE_PROTOCOL`, `SECURE_CONTROL`, and `SECURE_REGISTER`. `CONNECTION_RATE` determines rate enforced across all the endpoints that are rate limited

Name	Finding ID	Description
Listener Logging Control	NET.LISTENERLOG	Displays information about network listener logging configuration. The `LOGGING_LISTENER` parameter enables logging of listener activity. Log information can be useful for troubleshooting and to provide early warning of attempted attacks.

The following figure displays an example of the Oracle Database Security Assessment Report — Network Configuration section.

Figure 1-12 Oracle Database Security Assessment Report — Network Configuration



Network Configuration

Network Encryption

NET.ENCRYPTION

Check configurations used for Native Network Encryption

Status	Advisory
Summary	Native network encryption is accepted but not required. Integrity check using checksums is accepted but not required.
Details	SQLNET.ENCRYPTION_SERVER is not set (default value = ACCEPTED). SQLNET.CRYPTO_CHECKSUM_SERVER is not set (default value = ACCEPTED). Examined 1 listener. LISTENER: IPC (1), TCP (1), TCPS (0) SSL_CERT_REVOCATION is not set (default value = NONE).
Remarks	Network encryption is crucial for protecting the confidentiality and integrity of communication between a database server and its clients. To ensure that client connections are encrypted, you should configure either Native Encryption or TLS. If using Native Encryption, it's essential to set both ENCRYPTION_SERVER and CRYPTO_CHECKSUM_SERVER to REQUIRED. Oracle Database servers and clients are configured to ACCEPT encrypted connections by default to make deployment and compatibility easier. This means you can enable encryption and integrity settings for a connection pair by configuring just one side of the connection (server-side or the client-side). For instance, if many Oracle clients connect to a database instance, you can configure the required encryption and integrity settings for all those connections by modifying the sqlnet.ora file on the server end. There's no need to make configuration changes for each client separately. However, remember that the risk of plaintext data passing over the network still exists. Note that whether the security service is enabled depends on a combination of client and server configuration parameters. If using TLS, it's crucial to specify TCPS for all network ports, and SSL_CERT_REVOCATION should be set to REQUIRED. Oracle recommends using TLS network encryption.
References	Oracle Best Practice CIS Benchmark: Recommendation 2.3.1, 2.3.2 DISA STIG: V-219841, V-220263, V-220291, V-237699, V-237700, V-237723

The Network Configuration section is followed by the Operating System section.

Oracle Database Security Assessment Report — Operating System

The Oracle Database Security Assessment Report — Operating System section displays the following information:

Name	Finding ID	Description
Installation Account	OS.INSTALLATIONUSER	This check specifies the Oracle installation owner.
OS Authentication	OS.AUTH	Displays information about operating system group names and users that can exercise administrative privileges. OS authentication allows operating system users within the specified user group to connect to the database with administrative privileges. This shows the OS group names and users that can exercise each administrative privilege. OS users with administrative privileges should be reviewed to prevent any unauthorized, malicious or unintentional access to the database.
Segregation of Production and Development Databases	OS.MULTIDB	Checks for databases/instances running on the same server. If there are multiple databases/instances running on the same server ensure that it is not hosting production and test/development databases.
Process Monitor Processes	OS.PMON	Displays whether Process Monitor (PMON) processes are running under the `ORACLE_HOME` owner account. The PMON process monitors user processes and frees resources when they terminate. This process should run with the user ID of the `ORACLE_HOME` owner.
Agent Processes	OS.AGENT	Displays whether Agent processes owners overlap with Listener or Process Monitor (PMON) process owners. Agent processes should run with a user ID separate from the database and listener processes. These processes should run under a user ID separate from the database and listener processes.
Listener Processes	OS.LISTENER	Displays whether Listener process owners overlap with Agent or Process Monitor (PMON) process owners. Listener processes accept incoming network connections and connect them to the appropriate database server process. These processes should run with a user ID separate from the database and agent processes. These processes should be administered only through local OS authentication.
CMAN Remote Admin	OS.CMANLOCAL	Checks if Oracle Connection Manager is installed in the server and if yes, if CMAN remote administration is configured.

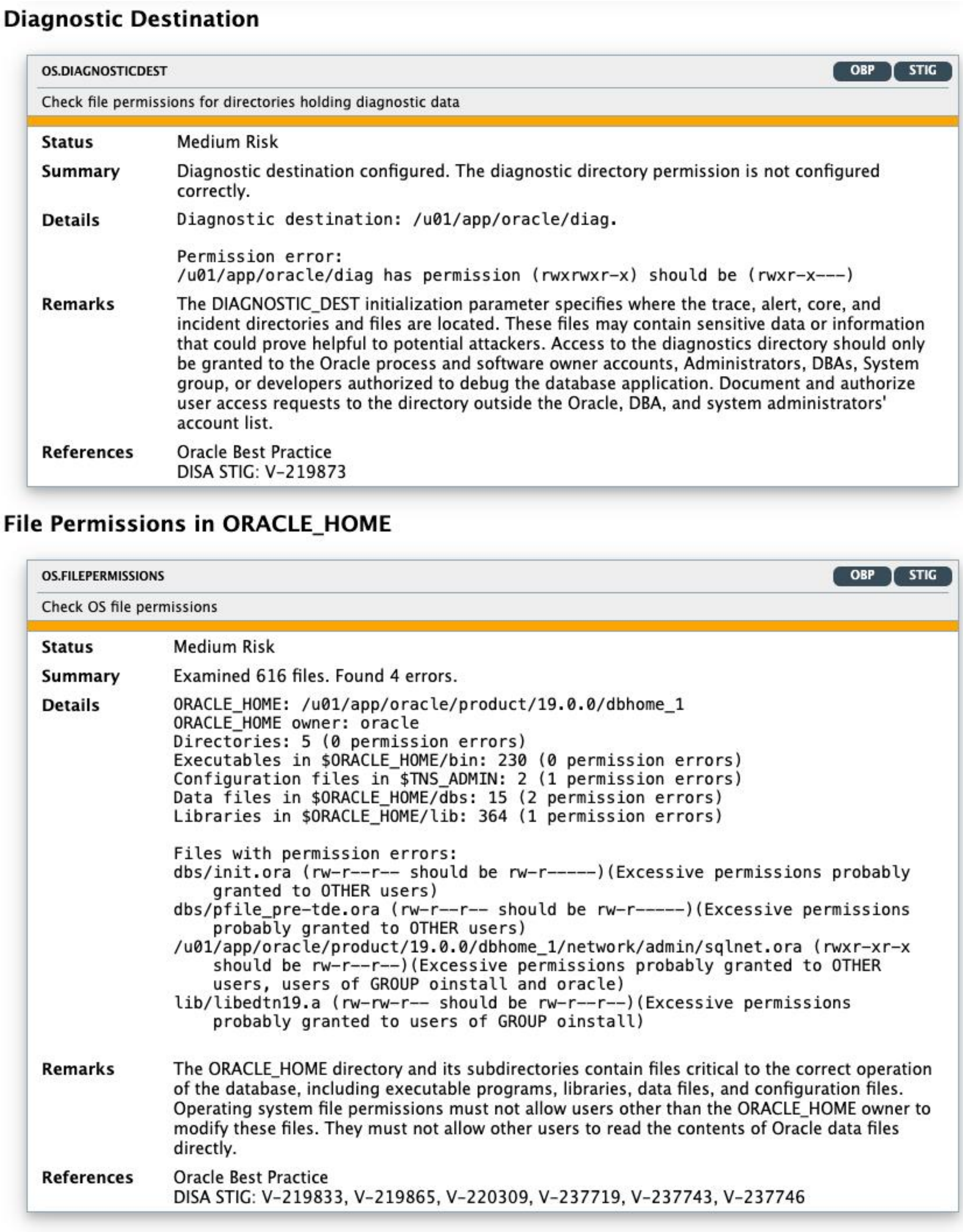
Name	Finding ID	Description
Diagnostic Destination	OS.DIAGNOSTICDEST	Checks permissions of DIAGONSTIC_DEST: - Checks file permissions if DIAGNOSTIC_DEST is set and is either ORACLE_HOME/rdbms/log or ORACLE_BASE <= 750 - Checks file permissions if DIAGNOSTIC_DEST is set and is either ORACLE_HOME/rdbms/log or ORACLE_BASE > 750 - Checks if the value of DIAGNOSTIC_DEST is not equal to ORACLE_HOME/rdbms/log nor ORACLE_BASE
File Permissions in ORACLE_HOME	OS.FILEPERMISSIONS	Displays information about file permissions errors in the ORACLE_HOME. The ORACLE_HOME directory and its subdirectories contain files that are critical to the correct operation of the database, including executable programs, libraries, data files, and configuration files. Operating system file permissions must not allow these files to be modified by users other than the ORACLE_HOME owner and must not allow other users to directly read the contents of Oracle data files.

Note:

On Windows, the DBSAT Collector collects data only from SQL queries. Since the data from the operating system commands is missing, the DBSAT Reporter runs a subset of rules on this data. Operating System findings are not available for databases running on Windows platform.

The following figure displays an example of the Oracle Database Security Assessment Report — Operating System section.

Figure 1-13   Oracle Database Security Assessment Report — Operating System



Diagnostic Destination

OS.DIAGNOSTICDEST

Check file permissions for directories holding diagnostic data

Status Medium Risk

Summary Diagnostic destination configured. The diagnostic directory permission is not configured correctly.

Details

```
Diagnostic destination: /u01/app/oracle/diag.

Permission error:
/u01/app/oracle/diag has permission (rwxrwxr-x) should be (rwxr-x---)
```

Remarks The DIAGNOSTIC_DEST initialization parameter specifies where the trace, alert, core, and incident directories and files are located. These files may contain sensitive data or information that could prove helpful to potential attackers. Access to the diagnostics directory should only be granted to the Oracle process and software owner accounts, Administrators, DBAs, System group, or developers authorized to debug the database application. Document and authorize user access requests to the directory outside the Oracle, DBA, and system administrators' account list.

References Oracle Best Practice
DISA STIG: V-219873

File Permissions in ORACLE_HOME

OS.FILEPERMISSIONS

Check OS file permissions

Status Medium Risk

Summary Examined 616 files. Found 4 errors.

Details

```
ORACLE_HOME: /u01/app/oracle/product/19.0.0/dbhome_1
ORACLE_HOME owner: oracle
Directories: 5 (0 permission errors)
Executables in $ORACLE_HOME/bin: 230 (0 permission errors)
Configuration files in $TNS_ADMIN: 2 (1 permission errors)
Data files in $ORACLE_HOME/dbs: 15 (2 permission errors)
Libraries in $ORACLE_HOME/lib: 364 (1 permission errors)

Files with permission errors:
dbs/init.ora (rw-r--r-- should be rw-r-----)(Excessive permissions probably
    granted to OTHER users)
dbs/pfile_pre-tde.ora (rw-r--r-- should be rw-r-----)(Excessive permissions
    probably granted to OTHER users)
/u01/app/oracle/product/19.0.0/dbhome_1/network/admin/sqlnet.ora (rwxr-xr-x
    should be rw-r--r--)(Excessive permissions probably granted to OTHER
    users, users of GROUP oinstall and oracle)
lib/libedtn19.a (rw-rw-r-- should be rw-r--r--)(Excessive permissions
    probably granted to users of GROUP oinstall)
```

Remarks The ORACLE_HOME directory and its subdirectories contain files critical to the correct operation of the database, including executable programs, libraries, data files, and configuration files. Operating system file permissions must not allow users other than the ORACLE_HOME owner to modify these files. They must not allow other users to read the contents of Oracle data files directly.

References Oracle Best Practice
DISA STIG: V-219833, V-219865, V-220309, V-237719, V-237743, V-237746

The Operating System section is followed by the Diagnostics section.

Oracle Database Security Assessment Report — Diagnostics

The Diagnostics section displays the checks which could not be executed.

Note:

This report provides information and recommendations that may be helpful in securing your Oracle database system. These recommendations reflect best practices for database security and should be part of any strategy for Data Protection by Design and by Default. These practices may help in addressing Articles 25 and 32 of the EU General Data Protection Regulation as well as other data privacy regulations. Technical controls alone are not sufficient for compliance. Passing all findings does not guarantee compliance.

Oracle Database Vault, Oracle Advanced Security, Oracle Label Security, Oracle Data Masking and Subsetting Pack are database licensed options. Oracle Key Vault and Oracle Audit Vault and Database Firewall require separate licensing as well.

The report provides a view on the current status. The results shown are provided for informational purposes only and should not be used as a substitute for a thorough analysis or interpreted to contain any legal or regulatory advice or guidance.

You are solely responsible for your system, and the data and information gathered during the production of this report. You are also solely responsible for the execution of software to produce this report, and for the effect and results of the execution of any mitigating actions identified herein.

Oracle provides this analysis on an "as is" basis without warranty of any kind and Oracle hereby disclaims all warranties and conditions whether express, implied or statutory.

Using the Discoverer

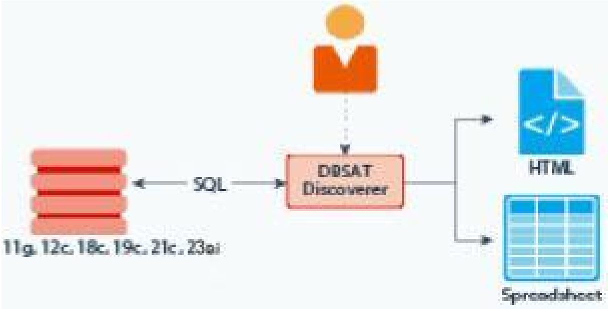
You can generate the Oracle Database Sensitive Data Assessment Report with the Discoverer component.

Oracle Database Sensitive Data Assessment Report

The Discoverer component is used to generate the Oracle Database Sensitive Data Assessment Report. The Discoverer executes SQL queries and collects data from the system to be assessed, based on the settings specified in the configuration and pattern files.

The following figure shows the components and architecture of the Discoverer.

Figure 1-14   Discoverer Components and Architecture



Configuring the Discoverer

Configuring dbsat.config

The settings in the configuration file determine the behavior of the Discoverer.

To configure the Discoverer, do the following:

1. Access the directory where DBSAT is installed.
2. Navigate to the `Discover/conf` directory. Make a copy of the `sample_dbsat.config` file and rename the file to match your site–specific requirements. For example, you can rename the file to `custom_dbsat.config`.

   > **Note:**
   >
   > Creating a duplicate file ensures that your custom settings are not overwritten during reinstallation.

3. Open `custom_dbsat.config`.

   The following are the contents of the configuration file:

   ```
   [Database]
           TNS_ADMIN =
           NET_SERVICE_NAME =
           WALLET_LOCATION =

           DB_HOSTNAME = localhost
           DB_PORT = 1521
           DB_SERVICE_NAME =

           SSL_ENABLED = FALSE
           SSL_TRUSTSTORE =
           SSL_TRUSTSTORE_TYPE =
           SSL_KEYSTORE =
           SSL_KEYSTORE_TYPE =
   ```

```
        SSL_DN =
        SSL_VERSION =
        SSL_CIPHER_SUITES =

[Discovery Parameters]
        sensitive_pattern_files = sensitive_en.ini
        schema_scope = ALL
        minrows = 1
        exclusion_list_file =

[Sensitive Categories]
        Identification Info - National IDs = High Risk
        Identification Info - Personal IDs = High Risk
        Identification Info - Public IDs = High Risk
        Biographic Info - Address = High Risk
        Biographic Info - Family Data = High Risk
        Biographic Info - Extended PII = High Risk
        Biographic Info - Restricted Data = High Risk
        IT Info - User Data = High Risk
        IT Info - Device Data = Medium Risk
        Financial Info - Card Data = High Risk
        Financial Info - Bank Data = High Risk
        Health Info - Insurance Data = High Risk
        Health Info - Provider Data = Medium Risk
        Health Info - Medical Data = Medium Risk
        Job Info - Employee Data = High Risk
        Job Info - Org Data = Low Risk
        Job Info - Compensation Data = High Risk
        Academic Info - Student Data = High Risk
        Academic Info - Institution Data = Medium Risk
        Academic Info - Performance Data = Low Risk
```

> **Note:**
>
> Keep the `[Database]`, `[Discovery Parameters]`, and `[Sensitive Categories]` entries for the sections. If you remove these lines, DBSAT discoverer will fail to execute.

4. Configure the settings. For more information about the configuration settings, see Configuration Settings.
5. Save and close the configuration file.

Section	Key	Value	Description
[Database]	`TNS_ADMIN`	`<network service name location>`	Location from where network service names needs to be read
-	`NET_SERVICE_NAME`	`<net_service_name>`	Network Service name to be used to make connection
-	`WALLET_LOCATION`	`<SSL wallet location> | <SEPS wallet location>`	Location of wallets for secured connections via SSL or SEPS (Secure External Password Store)
-	`DB_HOSTNAME`	`<hostname> | <ip_address>`	Hostname or IP Address of the target database server
-	`DB_PORT`	`<portnumber>` The default is 1521.	Listener port number for the target database. If a port number is not specified, the default port 1521 is used.
-	`DB_SERVICE_NAME`	`<service_name>`	Service name for the target database
-	`SSL_ENABLED`	`TRUE | FALSE` The default is `FALSE`.	Specifies if SSL is enabled or disabled when connecting to the Database Server. This is an optional argument. It is recommended that the `SSL_ENABLED` value is set to `TRUE`. Retain the default `FALSE` value if you do not require an SSL connection to the Database Server. If `SSL_ENABLED = TRUE`, then `SSL_TRUSTSTORE` is mandatory.
-	`SSL_TRUSTSTORE`	`<Absolute path to the TrustStore/TrustStore filename>` **Example:** `/opt/oracle/wallets/truststore.jks`	Specifies the absolute path to the TrustStore, and the TrustStore file name. Mandatory if `SSL_ENABLED = TRUE`.

Section	Key	Value	Description
-	`SSL_TRUSTSTORE_TYPE`	`PKCS12 | JKS | SSO`	Specifies the type of TrustStore. Use `PKCS12` if the Truststore is a Wallet. Use `JKS` if the Truststore is a Java KeyStore. Use `SSO` if the Truststore is an auto-login SSO Wallet.
-	`SSL_KEYSTORE`	`<Absolute path to the KeyStore/KeyStore filename>` **Example:** `/opt/oracle/wallets/keystore.jks`	Specifies the absolute path to the KeyStore, and the KeyStore file name. If `SSL_KEYSTORE` is not specified, the value specified in `SSL_TRUSTSTORE` is used. Mandatory if the Database server requires client authentication.
-	`SSL_KEYSTORE_TYPE`	`PKCS12 | JKS | SSO`	Specifies the type of KeyStore. Use `PKCS12` if the KeyStore is a Wallet. Use `JKS` if the KeyStore is a Java KeyStore. Use `SSO` if the KeyStore is an auto-login SSO Wallet.
-	`SSL_DN`	`<distinguished_name>`	Distinguished Name (DN) of the target Database server. Specify the DN if the server’s DN needs to be checked. This is an optional argument.

Section	Key	Value	Description
-	SSL_VERSION	1.0 | 1.1 | 1.2 The default is 1.2.	Specifies the version of the SSL protocol to use when connecting to the Database Server. This is an optional argument. Use 1.0 for SSL version TLSv1.0. Use 1.1 for SSL version TLSv1.1. Use 1.2 for SSL version TLSv1.2.
-	SSL_CIPHER_SUITES	<cipher_suite1>,<cipher_suite2> **Example:** TLS_RSA_WITH_AES_256_CBC_SHA256 , SSL_RSA_WITH_RC4_128_MD5	Specifies the Cryptographic Algorithms to be used. Multiple entries can be specified as a comma-separated list. This is an optional argument. For information about supported cryptographic suites, see https://docs.oracle.com/javase/8/docs/technotes/guides/security/SunProviders.html.
[Discovery Parameters]	SENSITIVE_PATTERN_FILES	<file_name> | <file_name1>, <file_name2> The default is sensitive_en.ini.	Specifies the pattern files to be used. Multiple files can be specified as a comma-separated list. The limit is 10 files. For more information about configuring the Sensitive Data Type pattern file, see Pattern File Configuration (Optional).
-	SCHEMA_SCOPE	ALL | <schema1>,<schema2> The default is ALL.	Specifies the schemas to be scanned. Multiple schemas can be specified as a comma-separated list.

Section	Key	Value	Description
-	MINROWS	<numerical value> The default is 1.	Specifies the minimum number of rows in a table for that table to be scanned. Tables with a number of rows less than what is specified in the minrows parameter are excluded from the scan.
-	EXCLUSION_LIST_FILE	<exclusion_list_filename>.ini	Specifies the file to be used to exclude schemas, tables, or columns from the scan. For more information about configuring the Exclusion List file, see Configuring the Exclusion List File (Optional).
[Sensitive Categories]			The **[Sensitive Categories]** section defines which Sensitive Categories are used. Valid risk levels are: • Low Risk • Medium Risk • High Risk The types of sensitive data are defined in the Sensitive Data Type pattern file. For more information about configuring the Sensitive Data Type pattern file, see Pattern File Configuration (Optional).

Pattern File Configuration (Optional)

The Oracle Database Security Assessment Tool searches for the types of sensitive data defined in the Pattern file(s).

About Sensitive Types

Pattern files contain the patterns to search for. A Pattern file is grouped into sections, defined by the section heading format `[SENSITIVE_TYPE_NAME]`. Each section constitutes a Sensitive Type.

The following example shows a sample Sensitive Type section for `FULL NAME`.

```
[FULL NAME]
COL_NAME_PATTERN = ^(?!.*(ITEM|TAX|BALANCE)).*(FULL.*NAME)|(^|[_-])
(CUSTOMER|CUST|CLIENT|PATIENT|PERSON).?(NAME|NM)($|[_-])
COL_COMMENT_PATTERN = ^(?!.*(ITEM|TAX|BALANCE)).*(FULL.?NAME)|
(CUSTOMER|CUST|CLIENT|PATIENT|PERSON).?NAME
SENSITIVE_CATEGORY = Identification Info - Public IDs
```

The Sensitive Type name `[SENSITIVE_TYPE_NAME]` is displayed in the Sensitive Type column of the Database Sensitive Data Assessment Report — Sensitive Column Details section. For more information about the Database Sensitive Data Assessment Report, see Oracle Database Sensitive Data Assessment Report.

Each Sensitive Type is defined by the following three parameters: `COL_NAME_PATTERN`, `COL_COMMENT_PATTERN`, and `SENSITIVE_CATEGORY`.

COL_NAME_PATTERN

The `COL_NAME_PATTERN` parameter specifies the text to search for in the Regular Expression (`RegExp`) patterns of the database column names.

```
(^LNAME$)|((LAST|FAMILY|SUR|PATERNAL).*NAME$)
```

In the example above, the following text will be searched for in the `RegExp` patterns of the database column names:

- `(^LNAME$)` — Searches for a column titled `LNAME`.
- `((LAST|FAMILY|SUR|PATERNAL).*NAME$)` — Searches for column names that contain `LAST`, `FAMILY`, `SUR`, or `PATERNAL`, followed by any characters and ending with `NAME`. For example, `LAST_NAME` or `CUSTOMER_SURNAME`.

COL_COMMENT_PATTERN

The `COL_COMMENT_PATTERN` parameter specifies the text to search for in the Regular Expression (`RegExp`) patterns of the database column comments.

SENSITIVE_CATEGORY

The `SENSITIVE_CATEGORY` parameter specifies the type of sensitive data. The risk levels associated with exposing types of sensitive data are specified in the `sample_dbsat.config` file. The risk levels are:

- `Low Risk`
- `Medium Risk`

- `High Risk`

For more information about configuring the `sample_dbsat.config` file, see Configuration Settings.

Customizing the Pattern File

To customize the Pattern file, do the following:

1. Access the directory where DBSAT is installed.
2. Navigate to the `Discover/conf` directory. Make a copy of the `sensitive_en.ini` file and rename the file `my_sensitive_en.ini`.

   > **Note:**
   >
   > The `Discover/conf` directory also contains the following language-specific `.ini` files to help discover sensitive data in data dictionaries in major European languages (filename - country, language):
   >
   > - `sensitive_de.ini` - German, Germany.
   > - `sensitive_el.ini` - Greek, Greece.
   > - `sensitive_es.ini` - Spanish, Spain.
   > - `sensitive_fr.ini` - French, France.
   > - `sensitive_it.ini` - Italian, Italy.
   > - `sensitive_nl.ini` - Dutch, Netherlands.
   > - `sensitive_pt.ini` - Portuguese, Portugal.

3. Open `my_sensitive_en.ini`.
4. Customize the settings by adding new Sensitive Types and modifying existing Sensitive Types.

   For more information about adding new Sensitive Types and Sensitive Categories to the Pattern file, see About Sensitive Types and Configuration Settings.
5. Save and close `my_sensitive_en.ini`.

   The Pattern file is configured.
6. Include `my_sensitive_en.ini` in the Discoverer scan by adding a reference to the file in the `custom_dbsat.config` file.

   ```
   sensitive_pattern_files = my_sensitive_en.ini
   ```

For more information about referencing the Pattern file in the `custom_dbsat.config` file, see Configuring dbsat.config.

About Regular Expressions

The search parameters use regular expressions, sets of strings based on common characteristics shared by each string in the set. Regular expressions vary in complexity, but once you understand the basics of how they are constructed, you can decipher or create any regular expression. You can use character classes, capturing groups, quantifiers, boundary matchers, and logical operators to define regular expressions.

String Literals

The most basic form of pattern matching is the match of a string literal. For example, if the regular expression is `EMP` and the input string is `EMP`, the match succeeds because the strings are identical. This regular expression also matches any string containing `EMP`, such as `EMPLOYEE`, `TEMP`, and `TEMPERATURE`.

Metacharacters

You can also use some special characters that affect the way a pattern is matched. One of the most common ones is the dot (`.`) symbol, which matches any character. For example, `EMPLOYEE.ID` matches `EMPLOYEE_ID` and `EMPLOYEE-ID`, but not `EMPLOYEE_VERIFICATION_ID`. Here, the dot is a metacharacter — a character with special meaning interpreted by the matcher.

Some other metacharacters are: `^ $ ? + * \ - [ ] ( ) { }`.

If you want a metacharacter to be treated literally (as an ordinary character), you can use a backslash (`\`) to escape it. For example, the regular expression `9\+9` matches `9+9`.

Character Classes

A character class is a set of characters enclosed within square brackets. It specifies the characters that successfully match a single character from a given input string.

The following table describes some common regular expression constructs.

Construct	Description
`[abc]`	Matches one of the characters mentioned within square brackets. Example: `EMPLOYE[ER]` matches `EMPLOYEE` and `EMPLOYER`.
`[^abc]`	Matches any character except the ones mentioned within square brackets. Example: `[^BC]AT` matches `RAT` and `HAT`, but does not match `BAT` and `CAT`.
`[A-Z0-9]`	Matches any character in the range mentioned within square brackets. To specify a range, simply insert the dash metacharacter "-" between the first and last character to be matched; for example, `[1-5]` or `[A-M]`. You can also place different ranges beside each other within the class to further expand the match possibilities. Example: `[B-F]AT` matches `BAT`, `CAT`, `DAT`, `EAT`, and `FAT`, but does not match `AAT` and `GAT`.

See Also:

- Character Classes
- Predefined Character Classes

Capturing Groups

You can use capturing groups to treat multiple characters as a single unit. A capturing group is created by placing the characters to be grouped inside a set of parentheses. For example, the regular expression `(SSN)` creates a single group containing the letters `S`, `S`, and `N`.

See Also:

Capturing Groups

Quantifiers

You can use quantifiers to specify the number of occurrences to match against.

The following table describes some common quantifiers.

Quantifier	Description
`X?`	Matches zero or one occurrence of the specified character or group of characters. Example: `SSN_NUMBERS?` matches strings `SSN_NUMBER` and `SSN_NUMBERS`.
`X*`	Matches zero or more occurrences of the specified character or group of characters. Example: `TERM.*DATE` matches strings like `TERMDATE`, `TERM_DATE` and `LAST_TERMINATION_DATE`.
`X+`	Matches one or more occurrences of the specified character or group of characters. Example: `TERM.+DATE` matches strings like `TERM_DATE` and `TERMINATION_DATE`, but not `TERMDATE`.
`X{n}`	Matches the specified character or group of characters exactly `n` times. Example: `9{3}` matches `999`, but not `99`.
`X{n,}`	Matches the specified character or group of characters at least `n` times. Example: `9{3,}` matches `999`, `9999`, and `99999`, but not `99`.
`X{n,m}`	Matches the specified character or group of characters at least `n` times but not more than m times. Example: `9{3,4}` matches `999` and `9999`, but not `99`.

An example of regular expression using character class is SSN[0-9]+, which matches strings like SSN0, SSN1, and SSN12. Here, [0-9] is a character class and is allowed one or more times. The regular expression however, does not match SSN.

See Also:

Quantifiers

Boundary Matchers

You can use boundary matchers to make pattern matching more precise by specifying where in the string the match should take place. For example, you might be interested in finding a particular word, but only if it appears at the beginning or end of an input string.

The following table describes common boundary matchers.

Boundary Construct	Description
^	Matches the specified character or group of characters at the beginning of a string (starts with search). Example: ^VISA matches strings beginning with VISA.
$	Matches the specified character or group of characters at the end of a string (ends with search). Example: NUMBER$ matches strings ending with NUMBER.
\b	Marks a word boundary. Matches the character or group of characters specified between a pair of \b only if it is a separate word (as opposed to substring within a longer string). Example: \bAGE\b matches strings like EMPLOYEE AGE and PATIENT AGE INFORMATION, but does not match strings like AGEING and EMPLOYEEAGE.

If no boundary matcher is specified, a contains search is performed. For example, ELECTORAL matches strings containing ELECTORAL, such as ELECTORAL_ID, ID_ELECTORAL, and ELECTORALID.

An exact match search can be performed by using ^ and $ together. For example, ^ADDRESS$ searches for the exact string ADDRESS. It matches the string ADDRESS, but does not match strings like PRIMARY_ADDRESS and ADDRESS_HOME.

See Also:

Boundary Matchers

Logical Operators

You can use the pipe or vertical bar character (|) if you want to match any one of the characters (or group of characters) separated by pipe. For example, EMPLOY(EE|ER)_ID matches EMPLOYEE_ID and EMPLOYER_ID.

Examples

^JOB.*(TITLE|PROFILE|POSITION)$ matches strings beginning with JOB, followed by zero or more occurrences of any character, and ending with TITLE, PROFILE, or POSITION.

^[A-Z]{3}[0-9]{2}[A-Z0-9]$ matches strings beginning with three letters, followed by two digits, and ending with a letter or digit.

BIRTH.?(COUNTRY|PLACE)|(COUNTRY|PLACE).*BIRTH matches strings such as BIRTH COUNTRY, PATIENT_BIRTH_PLACE, PLACE_OF_BIRTH, and EMPLOYEE'S COUNTRY OF BIRTH.

> **See Also:**
>
> Regular Expressions

Configuring the Exclusion List File (Optional)

You can specify schemas, tables, or columns to exclude from the scan in the Exclusion List file.

This is an optional step but often required to fine tune the Discoverer to exclude false positives.

To create an Exclusion List file, do the following:

1. Create an Exclusion List file, and save it in the Discover/conf directory as myexclusion_list.
2. Specify the schemas, tables, or columns to exclude from the Discoverer scan.

   The following is a sample of the contents of the Exclusion List file.

   ```
   PAYROLL
   IT.ENTITLEMENTS
   HR.EMPLOYEE.MARITAL_STATUS
   HR.JOB.CANDIDATE
   ```

   Specify the schemas, tables, or columns to exclude using the format SchemaName.TableName.ColumnName. Type each exclusion entry on a new line.

   In the example above, PAYROLL excludes the PAYROLL schema from the discovery scan; IT.ENTITLEMENTS excludes the ENTITLEMENTS table in IT schema; HR.EMPLOYEE.MARITAL_STATUS excludes column MARITAL_STATUS from the HR.EMPLOYEE table. Similarly, HR.JOB.CANDIDATE excludes column CANDIDATE from HR.JOB table.

Tip:

The Discoverer CSV report includes a column with the fully qualified column names (FULLY_QUALIFIED_COLUMN_NAME). This column can be used to create the exclusion list file contents and speed up the removal of unwanted columns or false positives from the report in a subsequent run.

3. Save and close the Exclusion List file.
4. Update the `exclusion_list_file` entry in your `custom_dbsat.config` file to `exclusion_list_file = myexclusion_list`

For more information about referencing the Exclusion List file, see Configuring dbsat.config.

Configuring Certificates and Wallets (Optional)

The Discoverer allows usage of Secure External Password Store to retrieve login credentials stored a wallet while connecting. Secure External Password Store can be used to connect to Database without entering the username and password. Secure External Password Store improves the security and allows automation of the execution of the Discoverer.

For increased security, Oracle Database provides Secure Sockets Layer (SSL) support to encrypt the connection between clients and the server. If SSL (TLS) encryption is configured on the Database Server, the Discoverer needs to be configured in order to connect and discover data. Configuration parameters for SSL can be found in the `dbsat.config` file.

To establish an SSL connection with the Discoverer, the Database Server sends its certificate, which is stored in its wallet. The client may or may not need a certificate or wallet, depending on the server configuration.

Note:

Configuring certificates and wallets is an optional step and needs to be performed only when using SSL to connect to the Oracle Database server.

For more information about configuring certificates and wallets, see Support for SSL in the *Oracle Database JDBC Developer's Guide*.

Running the Discoverer

To run the Discoverer, do the following:

1. Specify the arguments to run the Discoverer:

   ```
   $ dbsat discover [-n] -c <config_file> <output_file>
   ```

   The `dbsat discover` command has the following options and arguments:

   - *`-n`*

     Specifies that there is no encryption for output.

   - *`-c`*

     Specifies the name of the configuration file used for discoverer. For more information about the *`config_file`* file, see Configuring dbsat.config.

   - *`output_file`*

     Specifies the full or relative path name to create the `.zip` file. Do not add an extension.

     Example: `/home/oracle/dbsat/PDB1`

2. Run the Discoverer.

   ```
   $ ./dbsat discover -c Discover/conf/custom_dbsat.config PDB1
   ```

   The following output is displayed:

   ```
   DBSAT Discover ran successfully.
   Calling /usr/bin/zip to encrypt the generated reports...
   Enter password:
   Verify password:
     adding: PDB1_discover.html (deflated 86%)
     adding: PDB1_discover.csv (deflated 86%)
   Zip completed successfully.
   $
   ```

3. Specify a password to encrypt the `.zip` file.

   A zip file named `<destination>_report.zip` is created. If the file `<destination>_report.zip` exists, the discovery results are added to the existing zip file.

   > **Note:**
   >
   > The `.zip` file is used for Reporter and Discoverer output. To avoid confusion, it is recommended that you use the same password while creating both outputs.

4. Extract the contents of the `.zip` file to access the Database Sensitive Data Assessment Report. When prompted, enter the password to decrypt the `.zip` file specified in Step *3*.

The contents of the `.zip` file are extracted.

5. Use the appropriate tools to read the Database Sensitive Data Assessment Report.

   Example: Use a browser to display the `.html` file.

   Example: Use a spreadsheet reader like `OpenOffice Calc` or `Excel` to open the `.csv` file.

Oracle Database Sensitive Data Assessment Report

The Discoverer component is used to generate the Oracle Database Sensitive Data Assessment Report in HTML and CSV formats.

The HTML report is the main report and contains the discovered sensitive data and its categories along with target database information and Discoverer parameters.

The CSV report can be loaded into Oracle Audit Vault and Database Firewall to add sensitive data context to the new Data Privacy reports. For more information about this functionality, see Importing Sensitive Data Into AVDF Repository in the *Oracle Audit Vault and Database Firewall Auditor's Guide*.

Oracle Database Sensitive Data Assessment Report — High-Level Summary

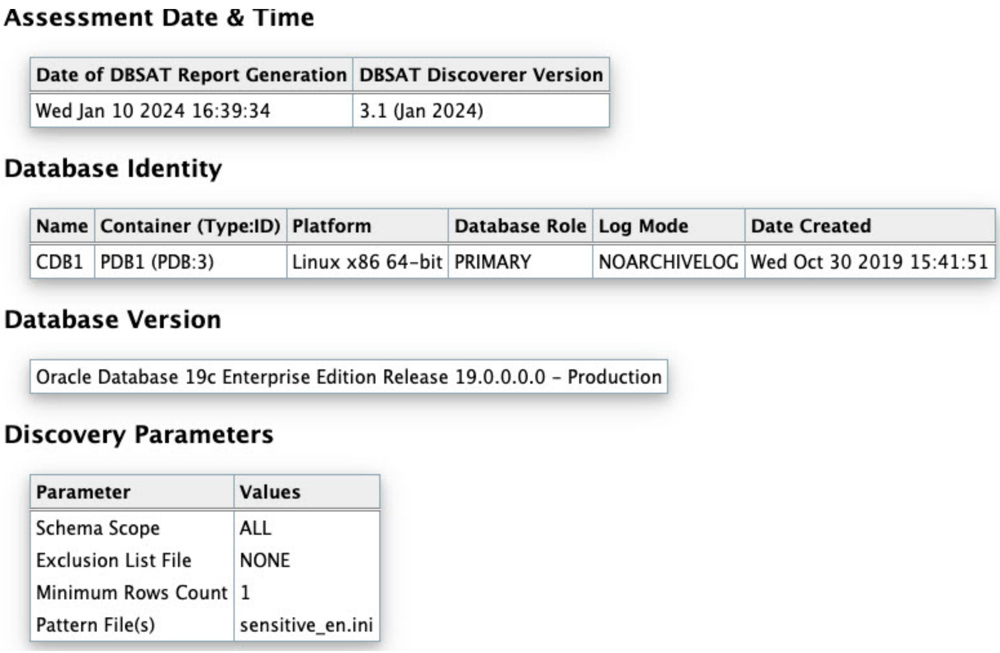
The Oracle Database Sensitive Data Assessment Report — High-Level Summary section contains the following information:

Table 1-1 Oracle Database Sensitive Data Assessment Report — High-Level Summary

Section	Description
Assessment Time & Date	Displays when the Sensitive Data Assessment report was generated. The DBSAT Discoverer version is also displayed.
Database Identity	Displays the details of the database assessed by the Discoverer.
Database Version	Displays the version of the database assessed by the Discoverer.
Discovery Parameters	Displays the Discovery Parameters specified in the configuration file. For more information about Discovery Parameters, see Configuration Settings.

The following figure displays the first four tables of the Oracle Database Sensitive Data Assessment Report — High-Level Summary section.

Figure 1-15   Oracle Database Sensitive Data Assessment Report — High-Level Summary



Assessment Date & Time

Date of DBSAT Report Generation	DBSAT Discoverer Version
Wed Jan 10 2024 16:39:34	3.1 (Jan 2024)

Database Identity

Name	Container (Type:ID)	Platform	Database Role	Log Mode	Date Created
CDB1	PDB1 (PDB:3)	Linux x86 64-bit	PRIMARY	NOARCHIVELOG	Wed Oct 30 2019 15:41:51

Database Version

Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production

Discovery Parameters

Parameter	Values
Schema Scope	ALL
Exclusion List File	NONE
Minimum Rows Count	1
Pattern File(s)	sensitive_en.ini

The High-Level Summary section is followed by the Summary section.

Oracle Database Sensitive Data Assessment Report — Summary

The Oracle Database Sensitive Data Assessment Report — Summary section displays information about the number of tables, columns, and rows identified as sensitive data, grouped by Sensitive Category.

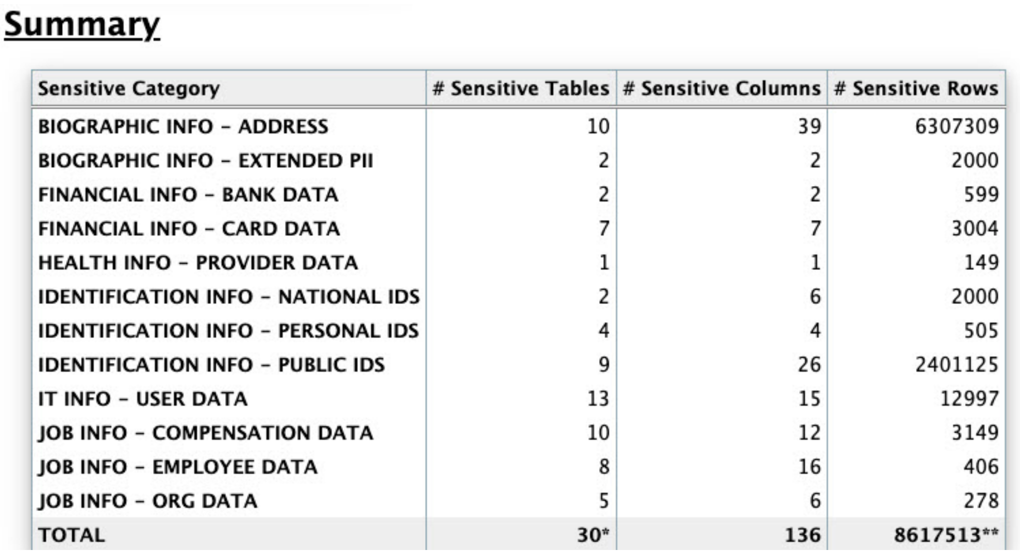
The Database Sensitive Data Assessment Report — Summary section contains the following columns:

Table 1-2   Oracle Database Sensitive Data Assessment Report — Summary

Column Name	Description
Sensitive Category	Displays the name of the Sensitive Category
# Sensitive Tables	Displays the number of tables detected that contain sensitive data
# Sensitive Columns	Displays the number of columns detected in the tables that contain sensitive data
# Sensitive Rows	Displays the number of rows detected in the tables that contain sensitive data

The following figure displays the information displayed in the Oracle Database Sensitive Data Assessment Report — Summary section:

Figure 1-16   Oracle Database Sensitive Data Assessment Report — Summary



Summary

Sensitive Category	# Sensitive Tables	# Sensitive Columns	# Sensitive Rows
BIOGRAPHIC INFO - ADDRESS	10	39	6307309
BIOGRAPHIC INFO - EXTENDED PII	2	2	2000
FINANCIAL INFO - BANK DATA	2	2	599
FINANCIAL INFO - CARD DATA	7	7	3004
HEALTH INFO - PROVIDER DATA	1	1	149
IDENTIFICATION INFO - NATIONAL IDS	2	6	2000
IDENTIFICATION INFO - PERSONAL IDS	4	4	505
IDENTIFICATION INFO - PUBLIC IDS	9	26	2401125
IT INFO - USER DATA	13	15	12997
JOB INFO - COMPENSATION DATA	10	12	3149
JOB INFO - EMPLOYEE DATA	8	16	406
JOB INFO - ORG DATA	5	6	278
TOTAL	30*	136	8617513**

> **Note:**
>
> A single database table could contain columns or column comments that match more than one Sensitive Category, causing a higher number to be displayed in the `# Sensitive Tables` and `# Sensitive Rows` columns. However, the `Total` row displays the unique number of tables and rows identified as sensitive data.

For more information about configuring Sensitive Categories, see Pattern File Configuration (Optional).

The Summary section is followed by the Sensitive Data section.

Oracle Database Sensitive Data Assessment Report — Sensitive Data

The Oracle Database Sensitive Data Assessment Report — Sensitive Data section displays information about the schemas containing sensitive data.

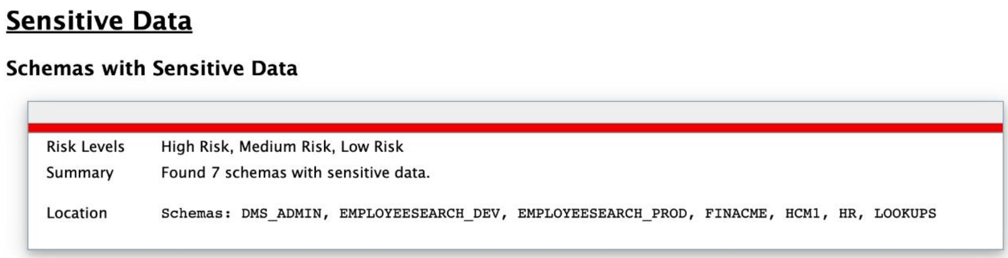
The Oracle Database Sensitive Data Assessment Report — Sensitive Data section contains the following information:

Table 1-3 Oracle Database Sensitive Data Assessment Report — Sensitive Data

Section	Description
Risk Level(s)	Displays the Risk Level(s) of the sensitive data identified in the schema of the database assessed by the Discoverer.
Summary	Displays a summary of the occurrence of sensitive data in the schema.
Location	Displays the names of the schemas containing sensitive data.

The following figure shows the information displayed in the Oracle Database Sensitive Data Assessment Report — Sensitive Data section.

Figure 1-17 Oracle Database Sensitive Data Assessment Report — Sensitive Data



Sensitive Data

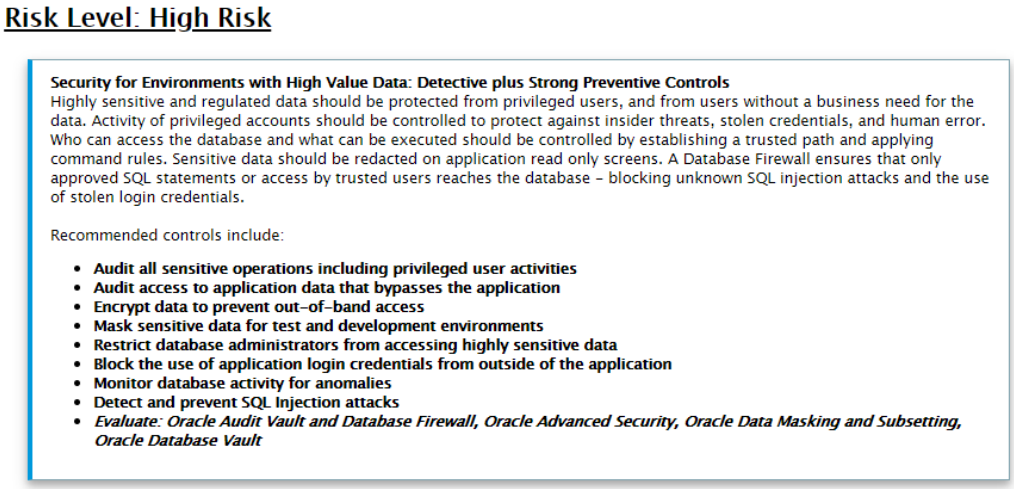
Schemas with Sensitive Data

Risk Levels	High Risk, Medium Risk, Low Risk
Summary	Found 7 schemas with sensitive data.
Location	Schemas: DMS_ADMIN, EMPLOYEESEARCH_DEV, EMPLOYEESEARCH_PROD, FINACME, HCM1, HR, LOOKUPS

Findings belonging to each risk level are followed by a set of recommendations to secure the sensitive data. These recommendations lists various controls based on the Risk Levels, namely HIGH, MEDIUM, and LOW.

The following figure shows the information displayed in the Risk Level: High Risk section.

Figure 1-18 Sensitive categories grouped by Risk Level



Risk Level: High Risk

Security for Environments with High Value Data: Detective plus Strong Preventive Controls
Highly sensitive and regulated data should be protected from privileged users, and from users without a business need for the data. Activity of privileged accounts should be controlled to protect against insider threats, stolen credentials, and human error. Who can access the database and what can be executed should be controlled by establishing a trusted path and applying command rules. Sensitive data should be redacted on application read only screens. A Database Firewall ensures that only approved SQL statements or access by trusted users reaches the database – blocking unknown SQL injection attacks and the use of stolen login credentials.

Recommended controls include:

- **Audit all sensitive operations including privileged user activities**
- **Audit access to application data that bypasses the application**
- **Encrypt data to prevent out–of–band access**
- **Mask sensitive data for test and development environments**
- **Restrict database administrators from accessing highly sensitive data**
- **Block the use of application login credentials from outside of the application**
- **Monitor database activity for anomalies**
- **Detect and prevent SQL Injection attacks**
- ***Evaluate: Oracle Audit Vault and Database Firewall, Oracle Advanced Security, Oracle Data Masking and Subsetting, Oracle Database Vault***

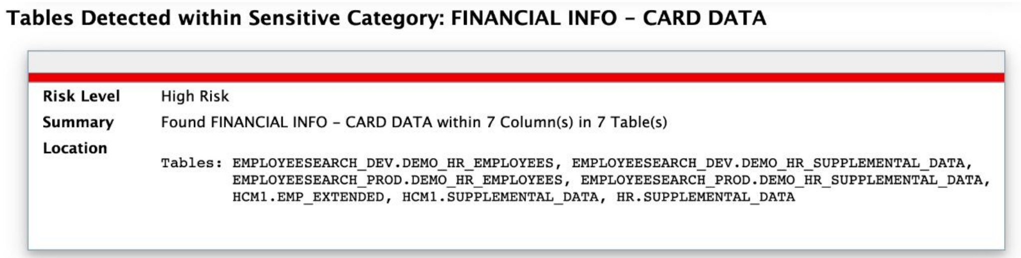
Each Risk Level section is followed by a list of the tables detected that contain sensitive data. The following information is displayed:

Table 1-4 Tables Detected within Sensitive Category: <Sensitive Category Name>

Name	Description
Risk Level	Displays the Risk Level
Summary	Displays a summary of the sensitive category data detected
Location	Displays the names of the tables that contain sensitive data

The following figure shows the information displayed in the Tables Detected within each Sensitive Category: <Sensitive Category Name> subsection.

Figure 1-19 Tables Detected within Sensitive Category: <Sensitive Category Name>



Tables Detected within Sensitive Category: FINANCIAL INFO – CARD DATA

Risk Level	High Risk
Summary	Found FINANCIAL INFO – CARD DATA within 7 Column(s) in 7 Table(s)
Location	`Tables: EMPLOYEESEARCH_DEV.DEMO_HR_EMPLOYEES, EMPLOYEESEARCH_DEV.DEMO_HR_SUPPLEMENTAL_DATA, EMPLOYEESEARCH_PROD.DEMO_HR_EMPLOYEES, EMPLOYEESEARCH_PROD.DEMO_HR_SUPPLEMENTAL_DATA, HCM1.EMP_EXTENDED, HCM1.SUPPLEMENTAL_DATA, HR.SUPPLEMENTAL_DATA`

The Sensitive Data section is followed by the Schema View section.

Oracle Database Sensitive Data Assessment Report — Schema View

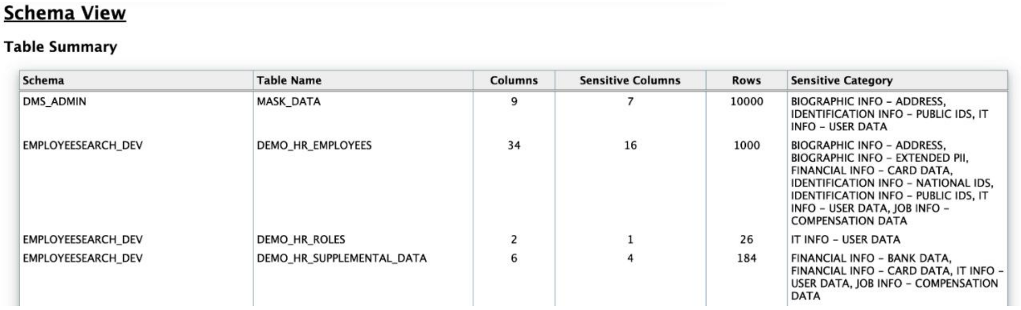
The Oracle Database Sensitive Data Assessment Report — Schema View section displays information about the schemas, tables, columns, and rows containing sensitive data. The Sensitive Category is also displayed.

The Oracle Database Sensitive Data Assessment Report — Summary section contains the following columns:

Column Name	Description
Schema	Displays the name of the schema
Table Name	Displays the name of the table
Columns	Displays the number of columns in the table
Sensitive Columns	Displays the number of columns detected that contain sensitive data
Rows	Displays the number of rows in the table
Sensitive Category	Displays the category of sensitive data detected in each column

The following figure highlights the information displayed in the Oracle Database Sensitive Data Assessment Report — Schema View section:

Figure 1-20   Oracle Database Sensitive Data Assessment Report — Schema View



Schema View

Table Summary

Schema	Table Name	Columns	Sensitive Columns	Rows	Sensitive Category
DMS_ADMIN	MASK_DATA	9	7	10000	BIOGRAPHIC INFO – ADDRESS, IDENTIFICATION INFO – PUBLIC IDS, IT INFO – USER DATA
EMPLOYEESEARCH_DEV	DEMO_HR_EMPLOYEES	34	16	1000	BIOGRAPHIC INFO – ADDRESS, BIOGRAPHIC INFO – EXTENDED PII, FINANCIAL INFO – CARD DATA, IDENTIFICATION INFO – NATIONAL IDS, IDENTIFICATION INFO – PUBLIC IDS, IT INFO – USER DATA, JOB INFO – COMPENSATION DATA
EMPLOYEESEARCH_DEV	DEMO_HR_ROLES	2	1	26	IT INFO – USER DATA
EMPLOYEESEARCH_DEV	DEMO_HR_SUPPLEMENTAL_DATA	6	4	184	FINANCIAL INFO – BANK DATA, FINANCIAL INFO – CARD DATA, IT INFO – USER DATA, JOB INFO – COMPENSATION DATA

The Schema View section is followed by the Sensitive Column Details section.

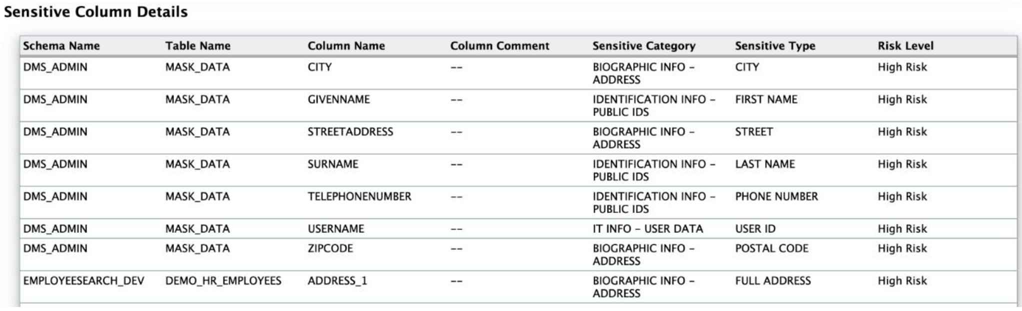
Oracle Database Sensitive Data Assessment Report — Sensitive Column Details

The Oracle Database Sensitive Data Assessment Report — Sensitive Column Details section displays information about the columns containing sensitive data. The Sensitive Category and Type are also displayed.

Column Name	Description
Schema Name	Displays the name of the schema
Table Name	Displays the name of the table
Column Name	Displays the name of the column
Column Comment	Displays the column comment
Sensitive Category	Displays the category of sensitive data detected in each column
Sensitive Type	Displays the type of sensitive data detected in each column
Risk Level	Displays the risk level

The following figure displays the information displayed in the Oracle Database Sensitive Data Assessment Report — Sensitive Column Details section.

Figure 1-21   Oracle Database Sensitive Data Assessment Report — Sensitive Column Details



Sensitive Column Details

Schema Name	Table Name	Column Name	Column Comment	Sensitive Category	Sensitive Type	Risk Level
DMS_ADMIN	MASK_DATA	CITY	--	BIOGRAPHIC INFO – ADDRESS	CITY	High Risk
DMS_ADMIN	MASK_DATA	GIVENNAME	--	IDENTIFICATION INFO – PUBLIC IDS	FIRST NAME	High Risk
DMS_ADMIN	MASK_DATA	STREETADDRESS	--	BIOGRAPHIC INFO – ADDRESS	STREET	High Risk
DMS_ADMIN	MASK_DATA	SURNAME	--	IDENTIFICATION INFO – PUBLIC IDS	LAST NAME	High Risk
DMS_ADMIN	MASK_DATA	TELEPHONENUMBER	--	IDENTIFICATION INFO – PUBLIC IDS	PHONE NUMBER	High Risk
DMS_ADMIN	MASK_DATA	USERNAME	--	IT INFO – USER DATA	USER ID	High Risk
DMS_ADMIN	MASK_DATA	ZIPCODE	--	BIOGRAPHIC INFO – ADDRESS	POSTAL CODE	High Risk
EMPLOYEESEARCH_DEV	DEMO_HR_EMPLOYEES	ADDRESS_1	--	BIOGRAPHIC INFO – ADDRESS	FULL ADDRESS	High Risk

Best Practices

Collector - OS Commands

As a general best practice, you should not put username/password credentials in cleartext in an application or file. When you provide the password on the command line while executing `dbsat collect`, someone can retrieve credentials, either using history or executing the `ps` Unix command or any similar Windows command. Therefore, Oracle recommends that you enter the password when prompted.

Collector - Database User Account

It's advisable that you run DBSAT collect and discoverer with a user that has the minimum set of privileges required to execute the assessments. The user shall also have a strong password. This will help reduce the attack surface and the potential impact of stolen DBSAT user account credentials, account misuse, and human error.

You can create a user with the required minimum privileges to run the Oracle Database Security Assessment Tool with the script provided in the pre-requisites section.

Securing DBSAT Output Files

By default, DBSAT produces password-protected zip files. As DBSAT output can contain sensitive information, it is recommended not to override the default. Mishandling of assessment information can introduce risk.

Excluding Sensitive User Accounts

DBSAT allows you to exclude users from the security assessment report. If there are critical users that you do not want to show in the report, you can exclude them by using the -u option in dbsat report execution.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

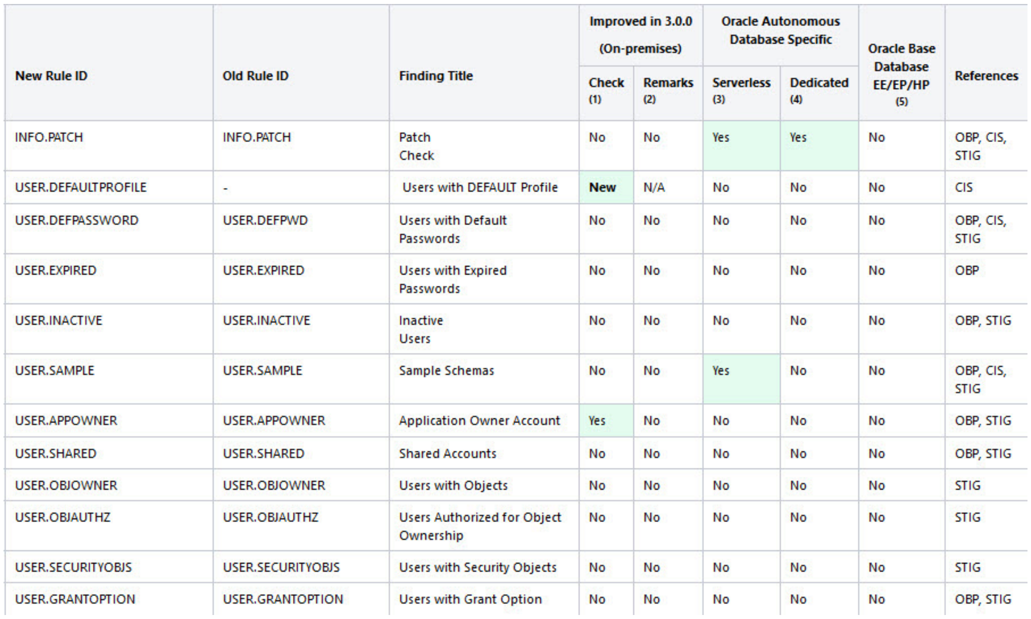
Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Appendix A

Improved DBSAT Target Specific Checks and Recommendations

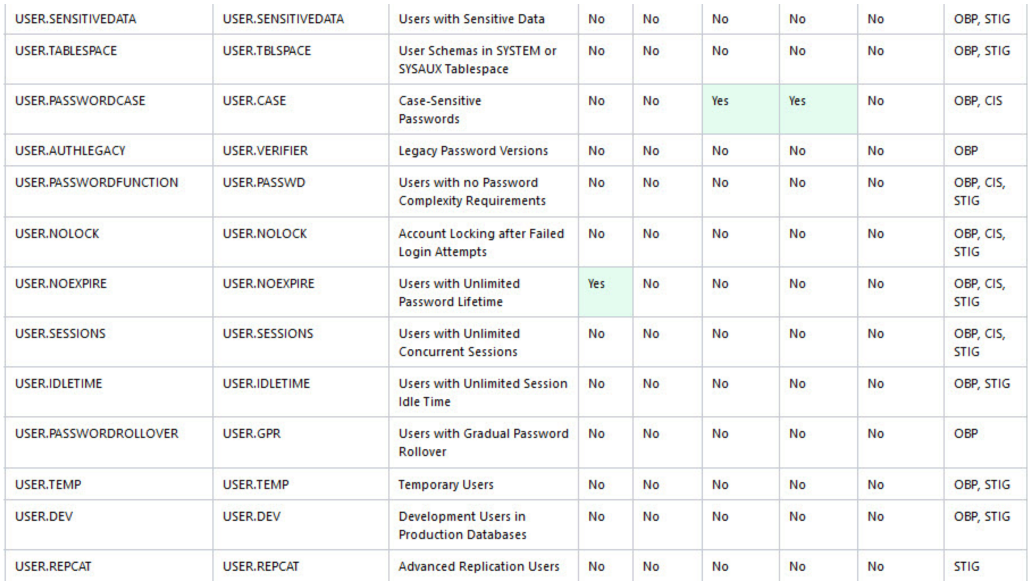
DBSAT can be run against on-premises databases, Autonomous Databases (Serverless and Dedicated) and Oracle Cloud DBCS (DBSystems EE/HP/EP). Some findings will execute different checks and provide specific recommendations for these databases. The table below highlights which findings were improved.

Figure 1-22 DBSAT Target Specific Checks and Recommendations



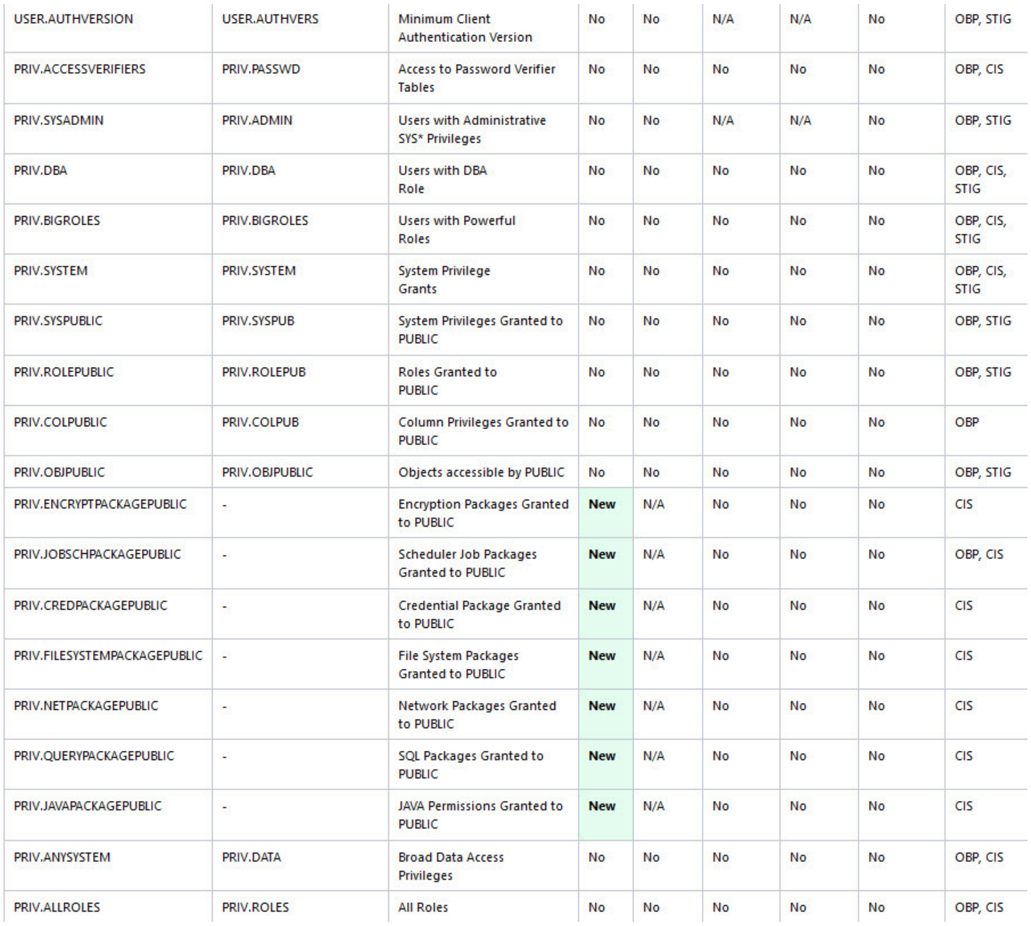
New Rule ID	Old Rule ID	Finding Title	Improved in 3.0.0 (On-premises)		Oracle Autonomous Database Specific		Oracle Base Database EE/EP/HP (5)	References
			Check (1)	Remarks (2)	Serverless (3)	Dedicated (4)		
INFO.PATCH	INFO.PATCH	Patch Check	No	No	Yes	Yes	No	OBP, CIS, STIG
USER.DEFAULTPROFILE	-	Users with DEFAULT Profile	**New**	N/A	No	No	No	CIS
USER.DEFPASSWORD	USER.DEFPWD	Users with Default Passwords	No	No	No	No	No	OBP, CIS, STIG
USER.EXPIRED	USER.EXPIRED	Users with Expired Passwords	No	No	No	No	No	OBP
USER.INACTIVE	USER.INACTIVE	Inactive Users	No	No	No	No	No	OBP, STIG
USER.SAMPLE	USER.SAMPLE	Sample Schemas	No	No	Yes	No	No	OBP, CIS, STIG
USER.APPOWNER	USER.APPOWNER	Application Owner Account	Yes	No	No	No	No	OBP, STIG
USER.SHARED	USER.SHARED	Shared Accounts	No	No	No	No	No	OBP, STIG
USER.OBJOWNER	USER.OBJOWNER	Users with Objects	No	No	No	No	No	STIG
USER.OBJAUTHZ	USER.OBJAUTHZ	Users Authorized for Object Ownership	No	No	No	No	No	STIG
USER.SECURITYOBJS	USER.SECURITYOBJS	Users with Security Objects	No	No	No	No	No	STIG
USER.GRANTOPTION	USER.GRANTOPTION	Users with Grant Option	No	No	No	No	No	OBP, STIG

Figure 1-23 DBSAT Target Specific Checks and Recommendations (continued)



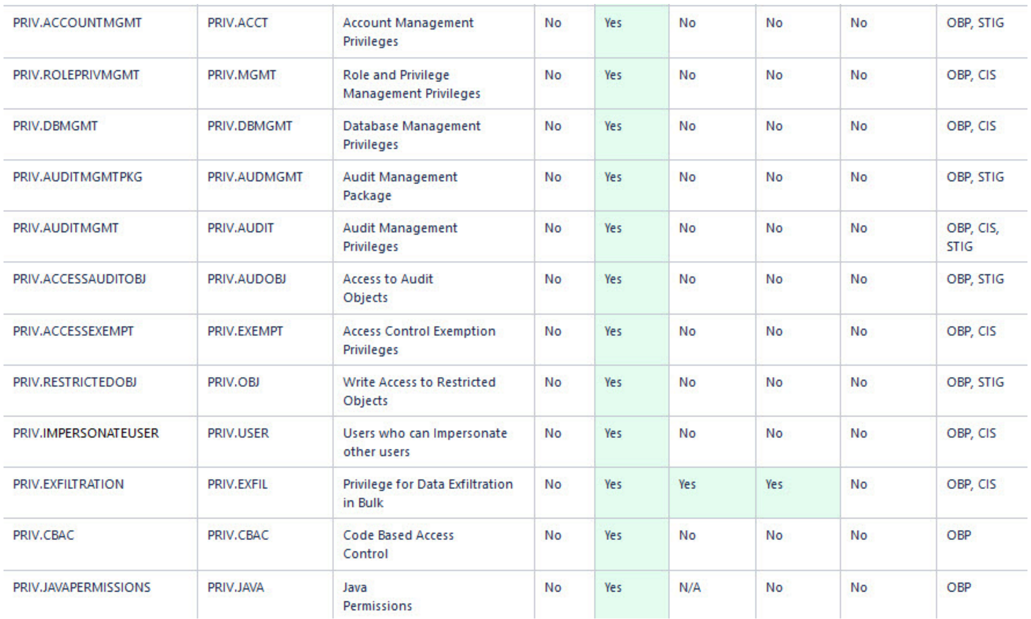
USER.SENSITIVEDATA	USER.SENSITIVEDATA	Users with Sensitive Data	No	No	No	No	No	OBP, STIG
USER.TABLESPACE	USER.TBLSPACE	User Schemas in SYSTEM or SYSAUX Tablespace	No	No	No	No	No	OBP, STIG
USER.PASSWORDCASE	USER.CASE	Case-Sensitive Passwords	No	No	Yes	Yes	No	OBP, CIS
USER.AUTHLEGACY	USER.VERIFIER	Legacy Password Versions	No	No	No	No	No	OBP
USER.PASSWORDFUNCTION	USER.PASSWD	Users with no Password Complexity Requirements	No	No	No	No	No	OBP, CIS, STIG
USER.NOLOCK	USER.NOLOCK	Account Locking after Failed Login Attempts	No	No	No	No	No	OBP, CIS, STIG
USER.NOEXPIRE	USER.NOEXPIRE	Users with Unlimited Password Lifetime	Yes	No	No	No	No	OBP, CIS, STIG
USER.SESSIONS	USER.SESSIONS	Users with Unlimited Concurrent Sessions	No	No	No	No	No	OBP, CIS, STIG
USER.IDLETIME	USER.IDLETIME	Users with Unlimited Session Idle Time	No	No	No	No	No	OBP, STIG
USER.PASSWORDROLLOVER	USER.GPR	Users with Gradual Password Rollover	No	No	No	No	No	OBP
USER.TEMP	USER.TEMP	Temporary Users	No	No	No	No	No	OBP, STIG
USER.DEV	USER.DEV	Development Users in Production Databases	No	No	No	No	No	OBP, STIG
USER.REPCAT	USER.REPCAT	Advanced Replication Users	No	No	No	No	No	STIG

Figure 1-24   DBSAT Target Specific Checks and Recommendations (continued)



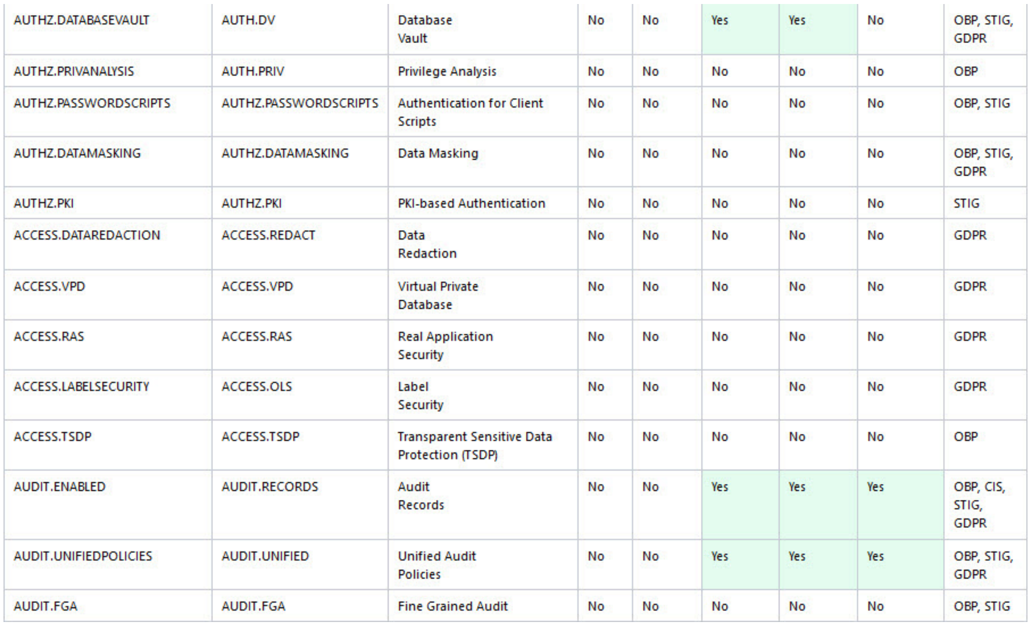
USER.AUTHVERSION	USER.AUTHVERS	Minimum Client Authentication Version	No	No	N/A	N/A	No	OBP, STIG
PRIV.ACCESSVERIFIERS	PRIV.PASSWD	Access to Password Verifier Tables	No	No	No	No	No	OBP, CIS
PRIV.SYSADMIN	PRIV.ADMIN	Users with Administrative SYS* Privileges	No	No	N/A	N/A	No	OBP, STIG
PRIV.DBA	PRIV.DBA	Users with DBA Role	No	No	No	No	No	OBP, CIS, STIG
PRIV.BIGROLES	PRIV.BIGROLES	Users with Powerful Roles	No	No	No	No	No	OBP, CIS, STIG
PRIV.SYSTEM	PRIV.SYSTEM	System Privilege Grants	No	No	No	No	No	OBP, CIS, STIG
PRIV.SYSPUBLIC	PRIV.SYSPUB	System Privileges Granted to PUBLIC	No	No	No	No	No	OBP, STIG
PRIV.ROLEPUBLIC	PRIV.ROLEPUB	Roles Granted to PUBLIC	No	No	No	No	No	OBP, STIG
PRIV.COLPUBLIC	PRIV.COLPUB	Column Privileges Granted to PUBLIC	No	No	No	No	No	OBP
PRIV.OBJPUBLIC	PRIV.OBJPUBLIC	Objects accessible by PUBLIC	No	No	No	No	No	OBP, STIG
PRIV.ENCRYPTPACKAGEPUBLIC	-	Encryption Packages Granted to PUBLIC	**New**	N/A	No	No	No	CIS
PRIV.JOBSCHPACKAGEPUBLIC	-	Scheduler Job Packages Granted to PUBLIC	**New**	N/A	No	No	No	OBP, CIS
PRIV.CREDPACKAGEPUBLIC	-	Credential Package Granted to PUBLIC	**New**	N/A	No	No	No	CIS
PRIV.FILESYSTEMPACKAGEPUBLIC	-	File System Packages Granted to PUBLIC	**New**	N/A	No	No	No	CIS
PRIV.NETPACKAGEPUBLIC	-	Network Packages Granted to PUBLIC	**New**	N/A	No	No	No	CIS
PRIV.QUERYPACKAGEPUBLIC	-	SQL Packages Granted to PUBLIC	**New**	N/A	No	No	No	CIS
PRIV.JAVAPACKAGEPUBLIC	-	JAVA Permissions Granted to PUBLIC	**New**	N/A	No	No	No	CIS
PRIV.ANYSYSTEM	PRIV.DATA	Broad Data Access Privileges	No	No	No	No	No	OBP, CIS
PRIV.ALLROLES	PRIV.ROLES	All Roles	No	No	No	No	No	OBP, CIS

Figure 1-25   DBSAT Target Specific Checks and Recommendations (continued)



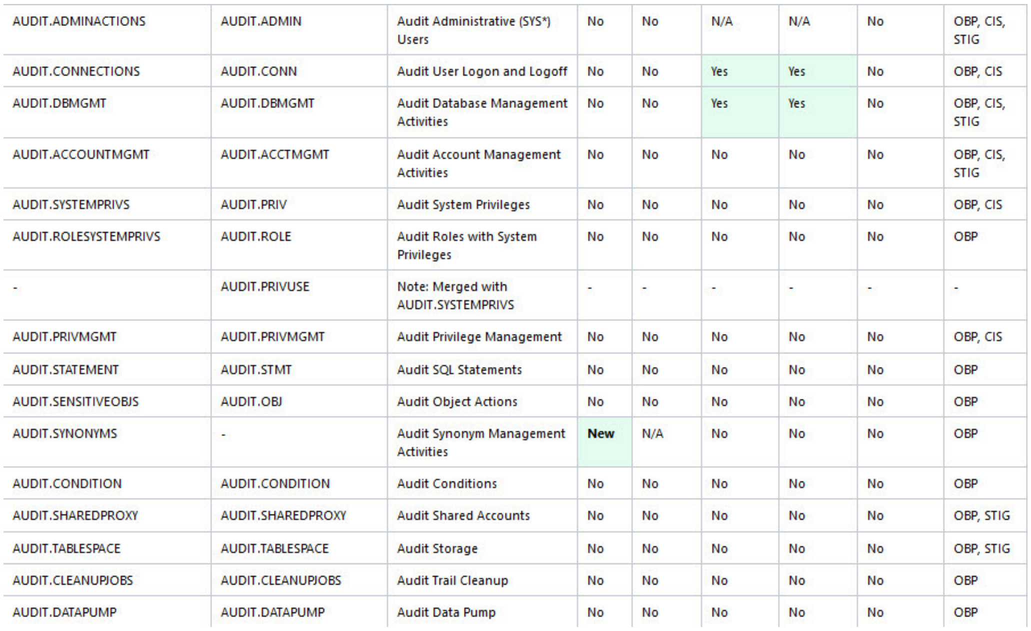
PRIV.ACCOUNTMGMT	PRIV.ACCT	Account Management Privileges	No	Yes	No	No	No	OBP, STIG
PRIV.ROLEPRIVMGMT	PRIV.MGMT	Role and Privilege Management Privileges	No	Yes	No	No	No	OBP, CIS
PRIV.DBMGMT	PRIV.DBMGMT	Database Management Privileges	No	Yes	No	No	No	OBP, CIS
PRIV.AUDITMGMTPKG	PRIV.AUDMGMT	Audit Management Package	No	Yes	No	No	No	OBP, STIG
PRIV.AUDITMGMT	PRIV.AUDIT	Audit Management Privileges	No	Yes	No	No	No	OBP, CIS, STIG
PRIV.ACCESSAUDITOBJ	PRIV.AUDOBJ	Access to Audit Objects	No	Yes	No	No	No	OBP, STIG
PRIV.ACCESSEXEMPT	PRIV.EXEMPT	Access Control Exemption Privileges	No	Yes	No	No	No	OBP, CIS
PRIV.RESTRICTEDOBJ	PRIV.OBJ	Write Access to Restricted Objects	No	Yes	No	No	No	OBP, STIG
PRIV.IMPERSONATEUSER	PRIV.USER	Users who can Impersonate other users	No	Yes	No	No	No	OBP, CIS
PRIV.EXFILTRATION	PRIV.EXFIL	Privilege for Data Exfiltration in Bulk	No	Yes	Yes	Yes	No	OBP, CIS
PRIV.CBAC	PRIV.CBAC	Code Based Access Control	No	Yes	No	No	No	OBP
PRIV.JAVAPERMISSIONS	PRIV.JAVA	Java Permissions	No	Yes	N/A	No	No	OBP

Figure 1-26   DBSAT Target Specific Checks and Recommendations (continued)



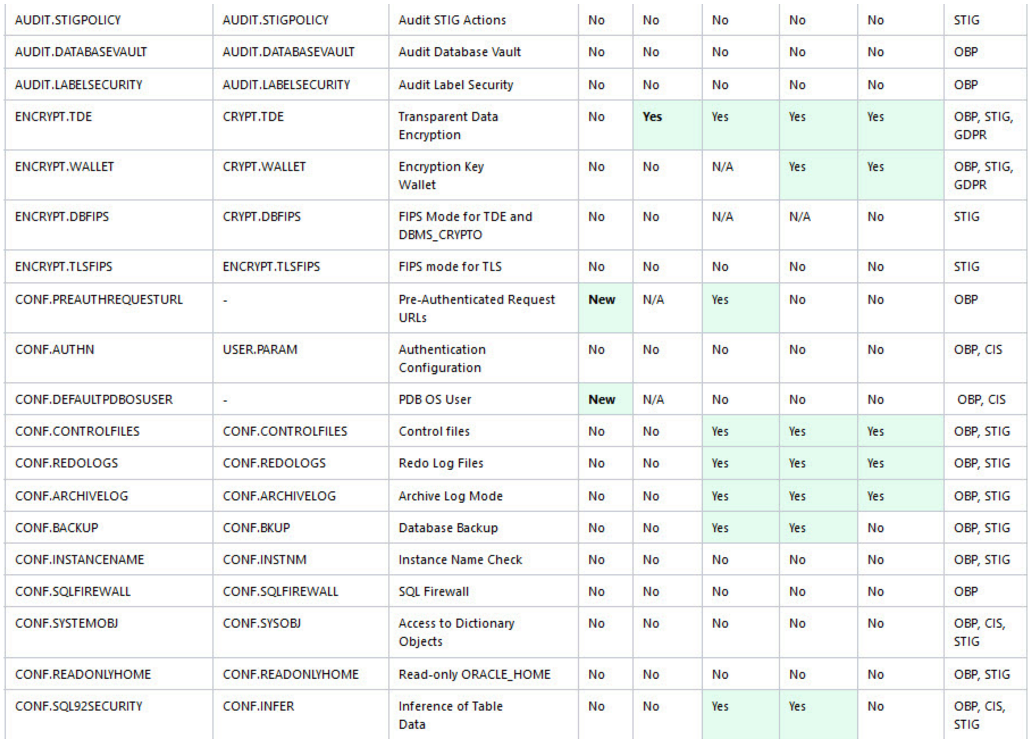
AUTHZ.DATABASEVAULT	AUTH.DV	Database Vault	No	No	Yes	Yes	No	OBP, STIG, GDPR
AUTHZ.PRIVANALYSIS	AUTH.PRIV	Privilege Analysis	No	No	No	No	No	OBP
AUTHZ.PASSWORDSCRIPTS	AUTHZ.PASSWORDSCRIPTS	Authentication for Client Scripts	No	No	No	No	No	OBP, STIG
AUTHZ.DATAMASKING	AUTHZ.DATAMASKING	Data Masking	No	No	No	No	No	OBP, STIG, GDPR
AUTHZ.PKI	AUTHZ.PKI	PKI-based Authentication	No	No	No	No	No	STIG
ACCESS.DATAREDACTION	ACCESS.REDACT	Data Redaction	No	No	No	No	No	GDPR
ACCESS.VPD	ACCESS.VPD	Virtual Private Database	No	No	No	No	No	GDPR
ACCESS.RAS	ACCESS.RAS	Real Application Security	No	No	No	No	No	GDPR
ACCESS.LABELSECURITY	ACCESS.OLS	Label Security	No	No	No	No	No	GDPR
ACCESS.TSDP	ACCESS.TSDP	Transparent Sensitive Data Protection (TSDP)	No	No	No	No	No	OBP
AUDIT.ENABLED	AUDIT.RECORDS	Audit Records	No	No	Yes	Yes	Yes	OBP, CIS, STIG, GDPR
AUDIT.UNIFIEDPOLICIES	AUDIT.UNIFIED	Unified Audit Policies	No	No	Yes	Yes	Yes	OBP, STIG, GDPR
AUDIT.FGA	AUDIT.FGA	Fine Grained Audit	No	No	No	No	No	OBP, STIG

Figure 1-27   DBSAT Target Specific Checks and Recommendations (continued)



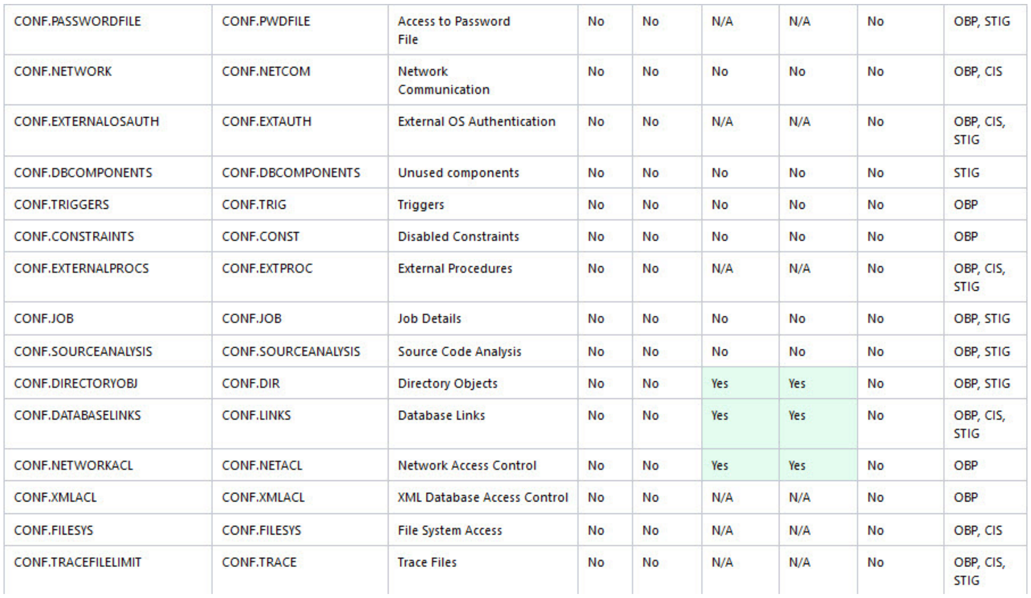
AUDIT.ADMINACTIONS	AUDIT.ADMIN	Audit Administrative (SYS*) Users	No	No	N/A	N/A	No	OBP, CIS, STIG
AUDIT.CONNECTIONS	AUDIT.CONN	Audit User Logon and Logoff	No	No	Yes	Yes	No	OBP, CIS
AUDIT.DBMGMT	AUDIT.DBMGMT	Audit Database Management Activities	No	No	Yes	Yes	No	OBP, CIS, STIG
AUDIT.ACCOUNTMGMT	AUDIT.ACCTMGMT	Audit Account Management Activities	No	No	No	No	No	OBP, CIS, STIG
AUDIT.SYSTEMPRIVS	AUDIT.PRIV	Audit System Privileges	No	No	No	No	No	OBP, CIS
AUDIT.ROLESYSTEMPRIVS	AUDIT.ROLE	Audit Roles with System Privileges	No	No	No	No	No	OBP
-	AUDIT.PRIVUSE	Note: Merged with AUDIT.SYSTEMPRIVS	-	-	-	-	-	-
AUDIT.PRIVMGMT	AUDIT.PRIVMGMT	Audit Privilege Management	No	No	No	No	No	OBP, CIS
AUDIT.STATEMENT	AUDIT.STMT	Audit SQL Statements	No	No	No	No	No	OBP
AUDIT.SENSITIVEOBJS	AUDIT.OBJ	Audit Object Actions	No	No	No	No	No	OBP
AUDIT.SYNONYMS	-	Audit Synonym Management Activities	**New**	N/A	No	No	No	OBP
AUDIT.CONDITION	AUDIT.CONDITION	Audit Conditions	No	No	No	No	No	OBP
AUDIT.SHAREDPROXY	AUDIT.SHAREDPROXY	Audit Shared Accounts	No	No	No	No	No	OBP, STIG
AUDIT.TABLESPACE	AUDIT.TABLESPACE	Audit Storage	No	No	No	No	No	OBP, STIG
AUDIT.CLEANUPJOBS	AUDIT.CLEANUPJOBS	Audit Trail Cleanup	No	No	No	No	No	OBP
AUDIT.DATAPUMP	AUDIT.DATAPUMP	Audit Data Pump	No	No	No	No	No	OBP

Figure 1-28   DBSAT Target Specific Checks and Recommendations (continued)



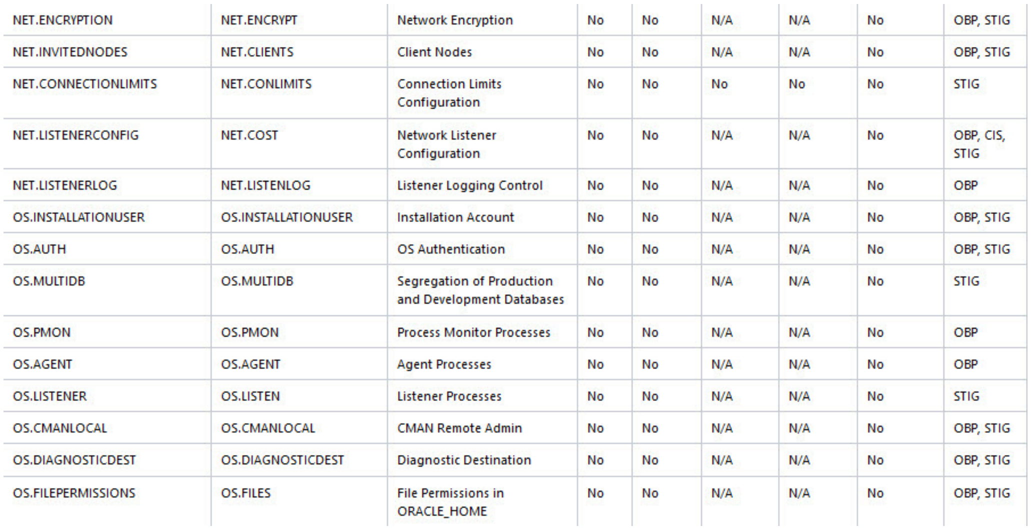
AUDIT.STIGPOLICY	AUDIT.STIGPOLICY	Audit STIG Actions	No	No	No	No	No	STIG
AUDIT.DATABASEVAULT	AUDIT.DATABASEVAULT	Audit Database Vault	No	No	No	No	No	OBP
AUDIT.LABELSECURITY	AUDIT.LABELSECURITY	Audit Label Security	No	No	No	No	No	OBP
ENCRYPT.TDE	CRYPT.TDE	Transparent Data Encryption	No	**Yes**	Yes	Yes	Yes	OBP, STIG, GDPR
ENCRYPT.WALLET	CRYPT.WALLET	Encryption Key Wallet	No	No	N/A	Yes	Yes	OBP, STIG, GDPR
ENCRYPT.DBFIPS	CRYPT.DBFIPS	FIPS Mode for TDE and DBMS_CRYPTO	No	No	N/A	N/A	No	STIG
ENCRYPT.TLSFIPS	ENCRYPT.TLSFIPS	FIPS mode for TLS	No	No	No	No	No	STIG
CONF.PREAUTHREQUESTURL	-	Pre-Authenticated Request URLs	**New**	N/A	Yes	No	No	OBP
CONF.AUTHN	USER.PARAM	Authentication Configuration	No	No	No	No	No	OBP, CIS
CONF.DEFAULTPDBOSUSER	-	PDB OS User	**New**	N/A	No	No	No	OBP, CIS
CONF.CONTROLFILES	CONF.CONTROLFILES	Control files	No	No	Yes	Yes	Yes	OBP, STIG
CONF.REDOLOGS	CONF.REDOLOGS	Redo Log Files	No	No	Yes	Yes	Yes	OBP, STIG
CONF.ARCHIVELOG	CONF.ARCHIVELOG	Archive Log Mode	No	No	Yes	Yes	Yes	OBP, STIG
CONF.BACKUP	CONF.BKUP	Database Backup	No	No	Yes	Yes	No	OBP, STIG
CONF.INSTANCENAME	CONF.INSTNM	Instance Name Check	No	No	No	No	No	OBP, STIG
CONF.SQLFIREWALL	CONF.SQLFIREWALL	SQL Firewall	No	No	No	No	No	OBP
CONF.SYSTEMOBJ	CONF.SYSOBJ	Access to Dictionary Objects	No	No	No	No	No	OBP, CIS, STIG
CONF.READONLYHOME	CONF.READONLYHOME	Read-only ORACLE_HOME	No	No	No	No	No	OBP, STIG
CONF.SQL92SECURITY	CONF.INFER	Inference of Table Data	No	No	Yes	Yes	No	OBP, CIS, STIG

Figure 1-29   DBSAT Target Specific Checks and Recommendations (continued)



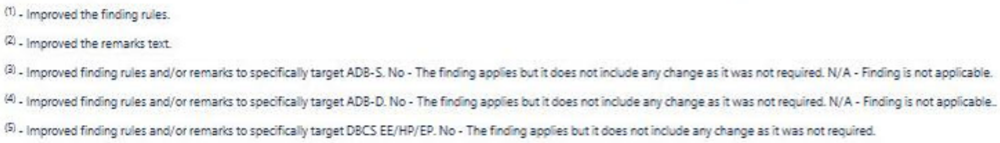
CONF.PASSWORDFILE	CONF.PWDFILE	Access to Password File	No	No	N/A	N/A	No	OBP, STIG
CONF.NETWORK	CONF.NETCOM	Network Communication	No	No	No	No	No	OBP, CIS
CONF.EXTERNALOSAUTH	CONF.EXTAUTH	External OS Authentication	No	No	N/A	N/A	No	OBP, CIS, STIG
CONF.DBCOMPONENTS	CONF.DBCOMPONENTS	Unused components	No	No	No	No	No	STIG
CONF.TRIGGERS	CONF.TRIG	Triggers	No	No	No	No	No	OBP
CONF.CONSTRAINTS	CONF.CONST	Disabled Constraints	No	No	No	No	No	OBP
CONF.EXTERNALPROCS	CONF.EXTPROC	External Procedures	No	No	N/A	N/A	No	OBP, CIS, STIG
CONF.JOB	CONF.JOB	Job Details	No	No	No	No	No	OBP, STIG
CONF.SOURCEANALYSIS	CONF.SOURCEANALYSIS	Source Code Analysis	No	No	No	No	No	OBP, STIG
CONF.DIRECTORYOBJ	CONF.DIR	Directory Objects	No	No	Yes	Yes	No	OBP, STIG
CONF.DATABASELINKS	CONF.LINKS	Database Links	No	No	Yes	Yes	No	OBP, CIS, STIG
CONF.NETWORKACL	CONF.NETACL	Network Access Control	No	No	Yes	Yes	No	OBP
CONF.XMLACL	CONF.XMLACL	XML Database Access Control	No	No	N/A	N/A	No	OBP
CONF.FILESYS	CONF.FILESYS	File System Access	No	No	N/A	N/A	No	OBP, CIS
CONF.TRACEFILELIMIT	CONF.TRACE	Trace Files	No	No	N/A	N/A	No	OBP, CIS, STIG

Figure 1-30   DBSAT Target Specific Checks and Recommendations (continued)



NET.ENCRYPTION	NET.ENCRYPT	Network Encryption	No	No	N/A	N/A	No	OBP, STIG
NET.INVITEDNODES	NET.CLIENTS	Client Nodes	No	No	N/A	N/A	No	OBP, STIG
NET.CONNECTIONLIMITS	NET.CONLIMITS	Connection Limits Configuration	No	No	No	No	No	STIG
NET.LISTENERCONFIG	NET.COST	Network Listener Configuration	No	No	N/A	N/A	No	OBP, CIS, STIG
NET.LISTENERLOG	NET.LISTENLOG	Listener Logging Control	No	No	N/A	N/A	No	OBP
OS.INSTALLATIONUSER	OS.INSTALLATIONUSER	Installation Account	No	No	N/A	N/A	No	OBP, STIG
OS.AUTH	OS.AUTH	OS Authentication	No	No	N/A	N/A	No	OBP, STIG
OS.MULTIDB	OS.MULTIDB	Segregation of Production and Development Databases	No	No	N/A	N/A	No	STIG
OS.PMON	OS.PMON	Process Monitor Processes	No	No	N/A	N/A	No	OBP
OS.AGENT	OS.AGENT	Agent Processes	No	No	N/A	N/A	No	OBP
OS.LISTENER	OS.LISTEN	Listener Processes	No	No	N/A	N/A	No	STIG
OS.CMANLOCAL	OS.CMANLOCAL	CMAN Remote Admin	No	No	N/A	N/A	No	OBP, STIG
OS.DIAGNOSTICDEST	OS.DIAGNOSTICDEST	Diagnostic Destination	No	No	N/A	N/A	No	OBP, STIG
OS.FILEPERMISSIONS	OS.FILES	File Permissions in ORACLE_HOME	No	No	N/A	N/A	No	OBP, STIG

Figure 1-31   DBSAT Target Specific Checks and Recommendations (continued)



[1] - Improved the finding rules.

[2] - Improved the remarks text.

[3] - Improved finding rules and/or remarks to specifically target ADB-S. No - The finding applies but it does not include any change as it was not required. N/A - Finding is not applicable.

[4] - Improved finding rules and/or remarks to specifically target ADB-D. No - The finding applies but it does not include any change as it was not required. N/A - Finding is not applicable..

[5] - Improved finding rules and/or remarks to specifically target DBCS EE/HP/EP. No - The finding applies but it does not include any change as it was not required.

Appendix B

You can troubleshoot Oracle Database Security Assessment Tool by using diagnostics and log files.

B.1 Enabling DBSAT Diagnostics to diagnose Oracle Database Security Assessment Tool Errors

Output diagnostics, which the DBSAT generates, capture vital information to help you debug errors.

By default, DBSAT suppresses errors that do not impact the report execution. To find details on errors that might affect your report generation, please run dbsat report with the `-d` option.

Example of a run with `-d`:

```
$ ./dbsat report -n -d orcl

Database Security Assessment Tool version 3.1 (Mar 2023)

This tool is intended to assist you in securing your Oracle database
system. You are solely responsible for your system and the effect and
results of the execution of this tool (including, without limitation,
any damage or data loss). Further, the output generated by this tool
may include potentially sensitive system configuration data and
information that could be used by a skilled attacker to penetrate your
system. You are solely responsible for ensuring that the output of
this tool, including any generated reports, is handled in accordance
with your company’s policies.

Traceback (most recent call last): File “<iostream>“, line 11865, in
<module> File “<iostream>“, line 1161, in sec_feature_usage
IndexError: index out of range: 1

DBSAT Reporter ran successfully.
```

Example of a standard run:

```
$ ./dbsat report -n orcl

Database Security Assessment Tool version 3.0

This tool is intended to assist you in securing your Oracle database
system. You are solely responsible for your system and the effect and
results of the execution of this tool (including, without limitation,
any damage or data loss). Further, the output generated by this tool
may include potentially sensitive system configuration data and
```

```
information that could be used by a skilled attacker to penetrate your
system. You are solely responsible for ensuring that

the output of this tool, including any generated reports, is handled
in accordance with your company’s policies.

DBSAT Reporter ran successfully.
```

B.2 DBSAT Reporter Fails With "No JSON object could be decoded"

If execute on package `SYS.DBMS_SQL` was revoked from `PUBLIC` you can encounter this issue.

```
$ ./dbsat report -a -n orcl

Database Security Assessment Tool version 3.0

This tool is intended to assist in you in securing your Oracle
database system. You are solely responsible for your system and the
effect and results of the execution of this tool (including, without
limitation, any damage or data loss). Further, the output generated by
this tool may include potentially sensitive system configuration data
and information that could be used by a skilled attacker to penetrate
your system. You are solely responsible for ensuring that the output
of this tool, including any generated reports, is handled in
accordance with yourcompany's policies.

... Unable to process input file: orcl.json No JSON object could be
decoded Error: Unexpected error occurred while running DBSAT Reporter.
```

To avoid this error, grant execute privilege on `DBMS_SQL` to the DBSAT database user (and not use PUBLIC privilege) used in `dbsat collect` *`<user>@<service_name> <output-file>`*

```
SQL> grant execute on sys.dbms_sql to <user> ;
```

Run `dbsat collect` again to ensure the data is collected appropriately and then run the report.

```
./dbsat collect <user>@<service_name> <output-file>

./dbsat report <output-file>
```

Note: make sure JSON is not invalid or corrupt. Review the json file and/or run the collector.

B.3 DBSAT Reporter Fails – Generic

Occasionally, the source of the issue affecting the DBSAT report's successful execution is present in the collector-generated file. As a troubleshooting step, you can open the file (extract from the zip file) generated by DBSAT collect and search the file for errors.

B.4 Issues running DBSAT on AIX platforms

AIX default shell is the Korn shell (`ksh`). DBSAT needs to run under the bash shell. You can either change it to `bash` or install it. DBSAT fails to run under other shells. As an example, if you do not have `bash` shell installed on AIX, and you try to run DBSAT, you can encounter the following:

```
oraprod>./dbsat

ksh: ./dbsat: not found

oraprod>pwd

/home/oraprod/dbsat300
```

At this point, you can install `bash` on AIX or run DBSAT collect remotely. You can execute DBSAT from another server with `bash` (e.g., a linux server), reaching the database running on AIX:

```
./dbsat collect <user>@<service_name> <output-file>
```

When collecting from a remote server, DBSAT will not include Operating System-related findings.

Appendix C

Attribution for Third-Party Licenses

For third party technology that you receive from Oracle in binary form which is licensed under an open source license that gives you the right to receive the source code for that binary, you can obtain a copy of the applicable source code from this page. If the source code for the technology was not provided to you with the binary, you can also receive a copy of the source code on physical media by submitting a written request to:

```
Oracle America, Inc.
Attn: Associate General Counsel
Development and Engineering Legal
500 Oracle Parkway, 10th Floor
Redwood Shores, CA 94065
```

Or, you may send an email to Oracle using this form. Your request should include:

```
The name of the component or binary file(s) for which you are requesting the
source code
The name and version number of the Oracle product
The date you received the Oracle product
Your name
Your company name (if applicable)
Your return mailing address and email
A telephone number in the event we need to reach you
```

We may charge you a fee to cover the cost of physical media and processing. Your request must be sent (i) within three (3) years of the date you received the Oracle product that included the component or binary file(s) that are the subject of your request, or (ii) in the case of code licensed under the GPL v3, for as long as Oracle offers spare parts or customer support for that product model

XlsxWriter, Version: 2.0

Copyright (c) 2013-2020, John McNamara <`jmcnamara@cpan.org`>

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the FreeBSD Project.

TERMS AND CONDITIONS FOR ACCESSING OR OTHERWISE USING JYTHON

PYTHON SOFTWARE FOUNDATION LICENSE VERSION 2

1. This LICENSE AGREEMENT is between the Python Software Foundation ("PSF"), and the Individual or Organization ("Licensee") accessing and otherwise using this software ("Jython") in source or binary form and its associated documentation.
2. Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Jython alone or in any derivative version, provided, however, that

PSF's License Agreement and PSF's notice of copyright, i.e., "Copyright (c) 2007 Python Software Foundation; All Rights Reserved" are retained in Jython alone or in any derivative version prepared by Licensee.

3. In the event Licensee prepares a derivative work that is based on or incorporates Jython or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Jython.
   The following changes were made:
   - Updated the Third Party package guava@31.0.1-jre to guava@32.1.2-jre
   - Removed pip@19.1 and setuptools@41.0.1 from binary distribution.
4. PSF is making Jython available to Licensee on an "AS IS" basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF JYTHON WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.
5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF JYTHON FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING JYTHON, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.
6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.
7. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSF trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.
8. By copying, installing or otherwise using Jython, Licensee agrees to be bound by the terms and conditions of this License Agreement.

PYTHON SOFTWARE FOUNDATION LICENSE VERSION 2.1

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Jython Developers nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

Note:

JPython version 1.1.x

1. This LICENSE AGREEMENT is between the Corporation for National Research Initiatives, having an office at 1895 Preston White Drive, Reston, VA 20191 ("CNRI"), and the Individual or Organization ("Licensee") accessing and using JPython version 1.1.x in source or binary form and its associated documentation as provided herein ("Software").
2. Subject to the terms and conditions of this License Agreement, CNRI hereby grants Licensee a non-exclusive, non-transferable, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use the Software alone or in any derivative version, provided, however, that CNRI's License Agreement and CNRI's notice of copyright, i.e., "Copyright (c)1996-1999 Corporation for National Research Initiatives; All Rights Reserved" are both retained in the Software, alone or in any derivative version prepared by Licensee.
   Subject to the terms and conditions of this License Agreement, CNRI hereby grants Licensee a non-exclusive, non-transferable, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use the Software alone or in any derivative version, provided, however, that CNRI's License Agreement and CNRI's notice of copyright, i.e., "Copyright (c)1996-1999 Corporation for National Research Initiatives; All Rights Reserved" are both retained in the Software, alone or in any derivative version prepared by Licensee.
3. In the event Licensee prepares a derivative work that is based on or incorporates the Software or any part thereof, and wants to make the derivative work available to the public as provided herein, then Licensee hereby agrees to indicate in any such work, in a prominently visible way, the nature of the modifications made to CNRI's Software.
4. Licensee may not use CNRI trademarks or trade name, including JPython or CNRI, in a trademark sense to endorse or promote products or services of Licensee, or any third party. Licensee may use the mark JPython in connection

with Licensee's derivative versions that are based on or incorporate the Software, but only in the form "JPython-based ___________________," or equivalent.

5. CNRI is making the Software available to Licensee on an "AS IS" basis. CNRI MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, CNRI MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.
6. CNRI SHALL NOT BE LIABLE TO LICENSEE OR OTHER USERS OF THE SOFTWARE FOR ANY INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THE SOFTWARE, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY SO THE ABOVE DISCLAIMER MAY NOT APPLY TO LICENSEE.
7. This License Agreement may be terminated by CNRI (i) immediately upon written notice from CNRI of any material breach by the Licensee, if the nature of the breach is such that it cannot be promptly remedied; or (ii) sixty (60) days following notice from CNRI to Licensee of a material remediable breach, if Licensee has not remedied such breach within that sixty-day period.
8. This License Agreement shall be governed by and interpreted in all respects by the law of the State of Virginia, excluding conflict of law provisions. Nothing in this Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between CNRI and Licensee.
9. By clicking on the "ACCEPT" button where indicated, or by installing, copying or otherwise using the Software, Licensee agrees to be bound by the terms and conditions of this License Agreement.

Oracle Database Database Security Assessment Tool User Guide, Release 3.1.0
F90720-05

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.