ORACLE

Oracle Database Security Assessment Tool 4.2

Learn how secure your databases are with DBSAT

Angeline Dhanarani

Product Management

Oracle AI Database Security

March 2026

Risks to your databases can come from many directions

- Unauthorized data access
- Data leakage while training
- Data privacy

AI

Deployment

- Cloud
- Network, DMZ
- Hardware
- VM or OS
- Backup
- Unauthorized key access

- SQL injection attacks
- Sensitive data exposure
- Bypass app access control

Applications

Configuration

- 125+ parameters
- Unpatched CVEs
- Drift in configuration

- Data copies
- Data privacy
- Huge volume of data
- Admin access to data

Sensitive Data

Users

- Stolen or weak credentials
- Compromised insiders
- Overprivileged users
- Mistakes and errors
- Expired or shared accounts

Risks to your databases can come from many directions

- Unauthorized data access
- Data leakage while training
- Data privacy

AI

Deployment

- Cloud
- Network, DMZ
- Hardware
- VM or OS
- Backup
- Unauthorized key access

- SQL injection attacks
- Sensitive data exposure
- Bypass app access contr

Every database comes with its own flavors of risks

Risks become intractable with scale

125+ parameters
Unpatched CVEs
Drift in configuration

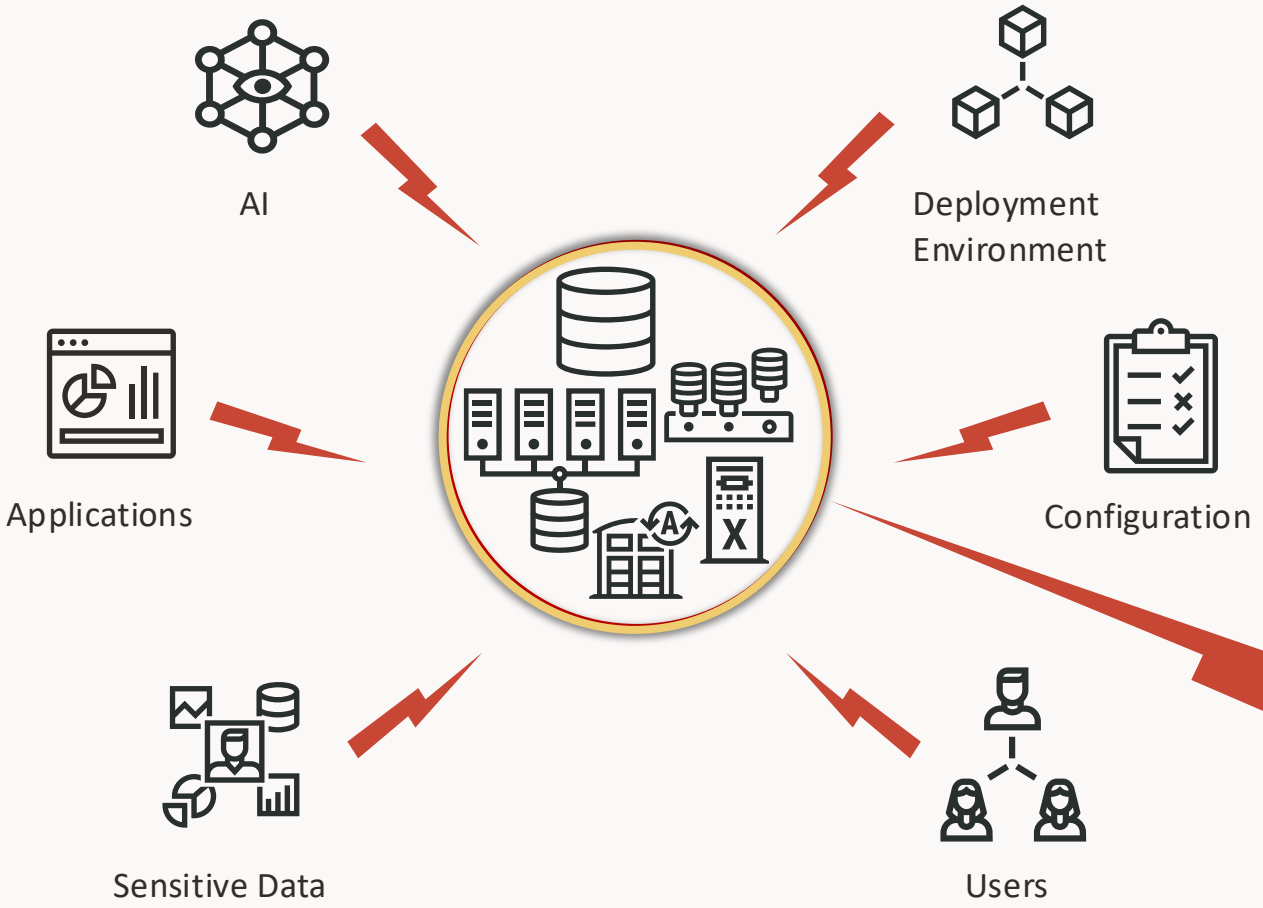
- Data copies
- Data privacy
- Huge volume of data
- Admin access to data

Sensitive Data

Users

- Stolen or weak credentials
- Compromised insiders
- Overprivileged users
- Mistakes and errors
- Expired or shared accounts

ALL risks need to be mitigated or managed



Skipping a control or implementing controls inconsistently introduces risks, and opens an opportunity for the hacker

Hackers just need to find one hole to get in, but we need to **protect against all attack vectors** to keep the hackers out

What is DBSAT?

Assess your database security before hackers come knocking

Assess Configuration

Patches

Data Encryption

Auditing policies

OS file permissions

Database configuration

Listener configuration

Fine-grained access control

Identify Risky Users

Database accounts

User privileges

User roles

Discover Sensitive Data

What type, where, and how much?

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

Assessment Reports

Summary and detailed information

Prioritized, actionable and target specific recommendations

Mapping to EU GDPR, STIG and CIS Benchmark

Runs on 11g to 26ai Oracle Databases.

New in DBSAT 4.0

July 2025

Expanded Compliance

- Updated for STIG 19c V1R1. New STIG-related checks
- References updated to match new numbering scheme
- DISA highlights DBSAT's value in official Oracle Database 19c STIG

Improved User & Entitlement Assessment

- Identifies stale user accounts (no recent logins)
- Flags users with passwords expiring in 30 days
- Locally managed user checks
- Proxy users in DBA/PDB_DBA check
- Database Vault SoD and integrity checks
- Improved Data Redaction checks
- **Expanded Container Database Coverage**
- Checks for users with SET CONTAINER privilege
- Lists PDB lockdown profiles

Better CVE Visibility

- INFO.PATCH now covers unpatched CVEs

Smarter, Streamlined Findings

- Documentation links next to findings for Oracle Database 19c and 26ai assessments

Better Usability & Advanced Options

- Specify output format for DBSAT report [-f]
- Generate a log file for troubleshooting [-d]
- Limit number of rows collected [-r]

Discoverer Enhancements

- New JSON output
- Improved English pattern matching
- Report includes Views and View columns

DBSAT Extract

- New compression/encryption utility (no zip/unzip needed)

To learn more, please check the release notes.

New in DBSAT 4.1

Dec 2025

Support for Oracle AI Database 26ai

- DBSAT now supports Oracle AI Database 26ai and Oracle Autonomous AI Databases

Updated CVEs from Oct 2025 CPU

- INFO.PATCH now covers unpatched CVEs from Critical Patch Update - October 2025 for Oracle Database 19c, 21c, and 23ai

To learn more, please check the release notes.

New in DBSAT 4.2

March 2026

Updated CVEs from Jan 2026 CPU

- INFO.PATCH now covers unpatched CVEs from Critical Patch Update - January 2026 for Oracle Database 19c, 21c, and 26ai

Oracle recommends using a more secure authentication method when invoking DBSAT

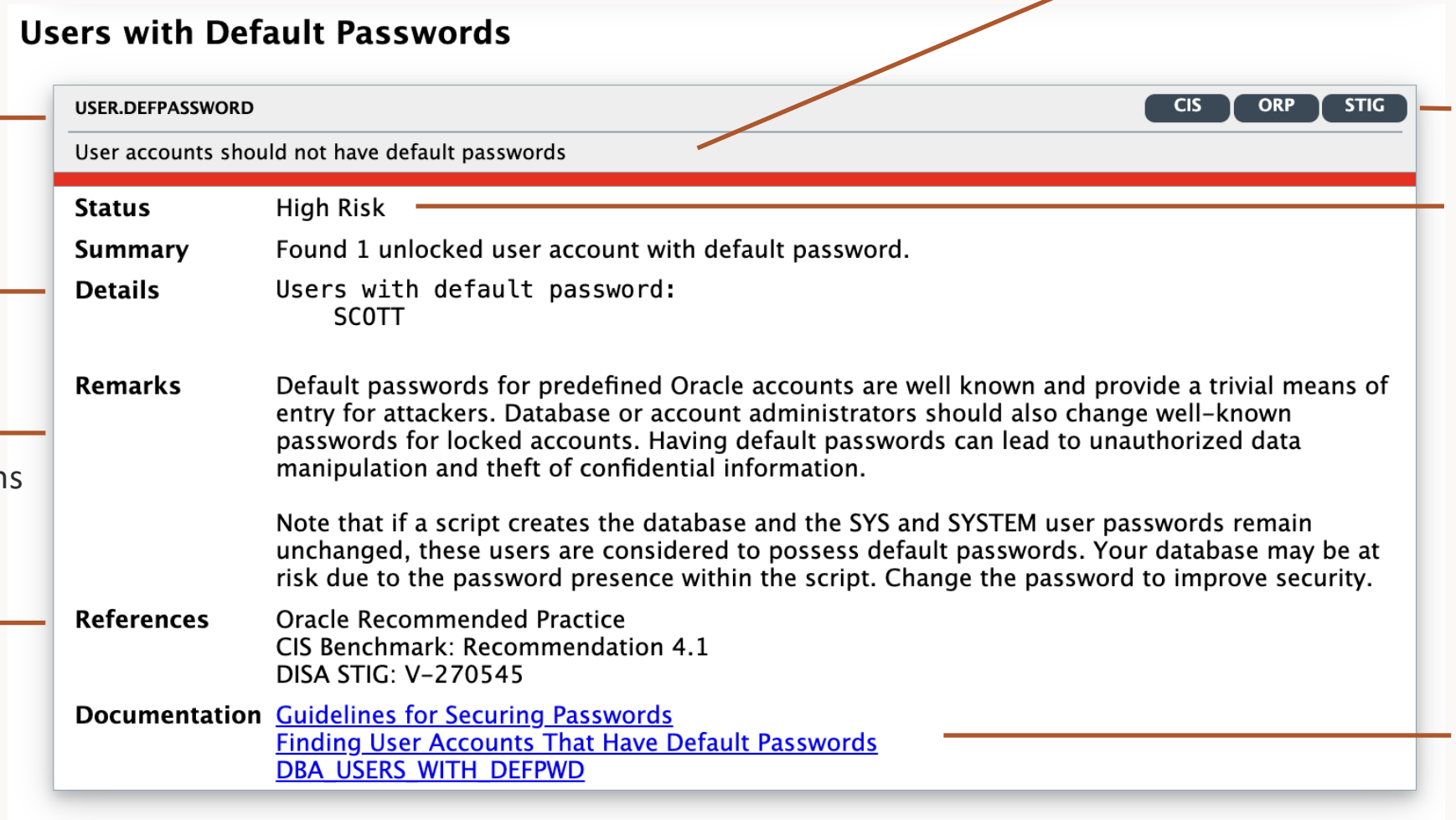
- Supplying the password on the command line is deprecated and will be unsupported in a future release.
- DBSAT now displays a warning advising to adopt a more secure authentication approach.

> *Warning: Including passwords in connection strings is deprecated and will be desupported in future releases. Refer to the Oracle Database Security Assessment Tool User Guide for secure ways to run the Collector.*

- For interactive prompt with no password in command line, use the format:

  $ dbsat collect <username>@<service_name> <dest-file>

Sample finding



Sentence outlining the recommended action

Rule ID

Tag with applicable standards

Can be High risk, Medium risk, Low risk, Pass Advisory, or Evaluate

Detail of the Finding

Rationale and Recommendations

Mapping to Regulations

NEW

Documentation links

New STIG checks in DBSAT (1/5)

NEW in 4.0

Locally Managed Accounts

USER.LOCALAUTH — STIG

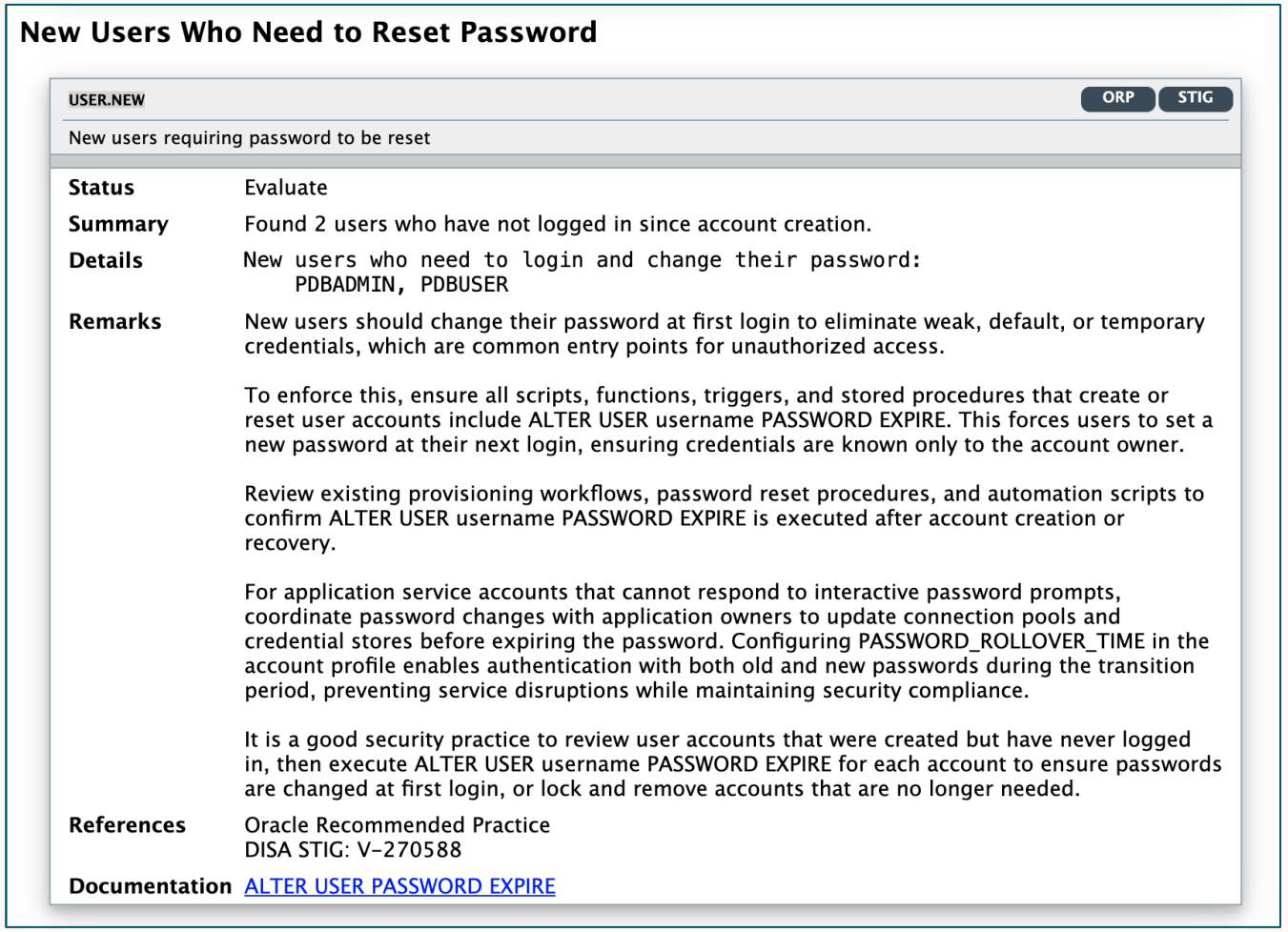
Locally managed users

Status	Evaluate
Summary	Found 3 accounts managed locally by the Oracle Database.
Details	`Locally managed accounts:` `DBSAT, PDBADMIN, PDBUSER`
Remarks	Centralizing user authentication and authorization is a security practice that mitigates the risk of rogue database accounts remaining active after an individual has left the organization. Integrate the Oracle database directly with an enterprise identity service, such as Microsoft Entra ID, Oracle Cloud Infrastructure Identity and Access Management, or Microsoft Active Directory, to streamline user lifecycle management. In accordance with STIG requirements, all locally managed user accounts within the database must receive explicit approval and be properly documented.
References	DISA STIG: V-270499
Documentation	None

Supports efforts to review locally managed accounts

New STIG checks in DBSAT (2/5)

NEW in 4.0



New Users Who Need to Reset Password

USER.NEW — ORP — STIG

New users requiring password to be reset

Status	Evaluate
Summary	Found 2 users who have not logged in since account creation.
Details	New users who need to login and change their password: PDBADMIN, PDBUSER
Remarks	New users should change their password at first login to eliminate weak, default, or temporary credentials, which are common entry points for unauthorized access. To enforce this, ensure all scripts, functions, triggers, and stored procedures that create or reset user accounts include ALTER USER username PASSWORD EXPIRE. This forces users to set a new password at their next login, ensuring credentials are known only to the account owner. Review existing provisioning workflows, password reset procedures, and automation scripts to confirm ALTER USER username PASSWORD EXPIRE is executed after account creation or recovery. For application service accounts that cannot respond to interactive password prompts, coordinate password changes with application owners to update connection pools and credential stores before expiring the password. Configuring PASSWORD_ROLLOVER_TIME in the account profile enables authentication with both old and new passwords during the transition period, preventing service disruptions while maintaining security compliance. It is a good security practice to review user accounts that were created but have never logged in, then execute ALTER USER username PASSWORD EXPIRE for each account to ensure passwords are changed at first login, or lock and remove accounts that are no longer needed.
References	Oracle Recommended Practice DISA STIG: V-270588
Documentation	ALTER USER PASSWORD EXPIRE

Identified users who haven't logged in since account creation

New STIG checks in DBSAT (3/5)

NEW in 4.0

Security Assessment

CONF.ASSESSMENT ORP STIG

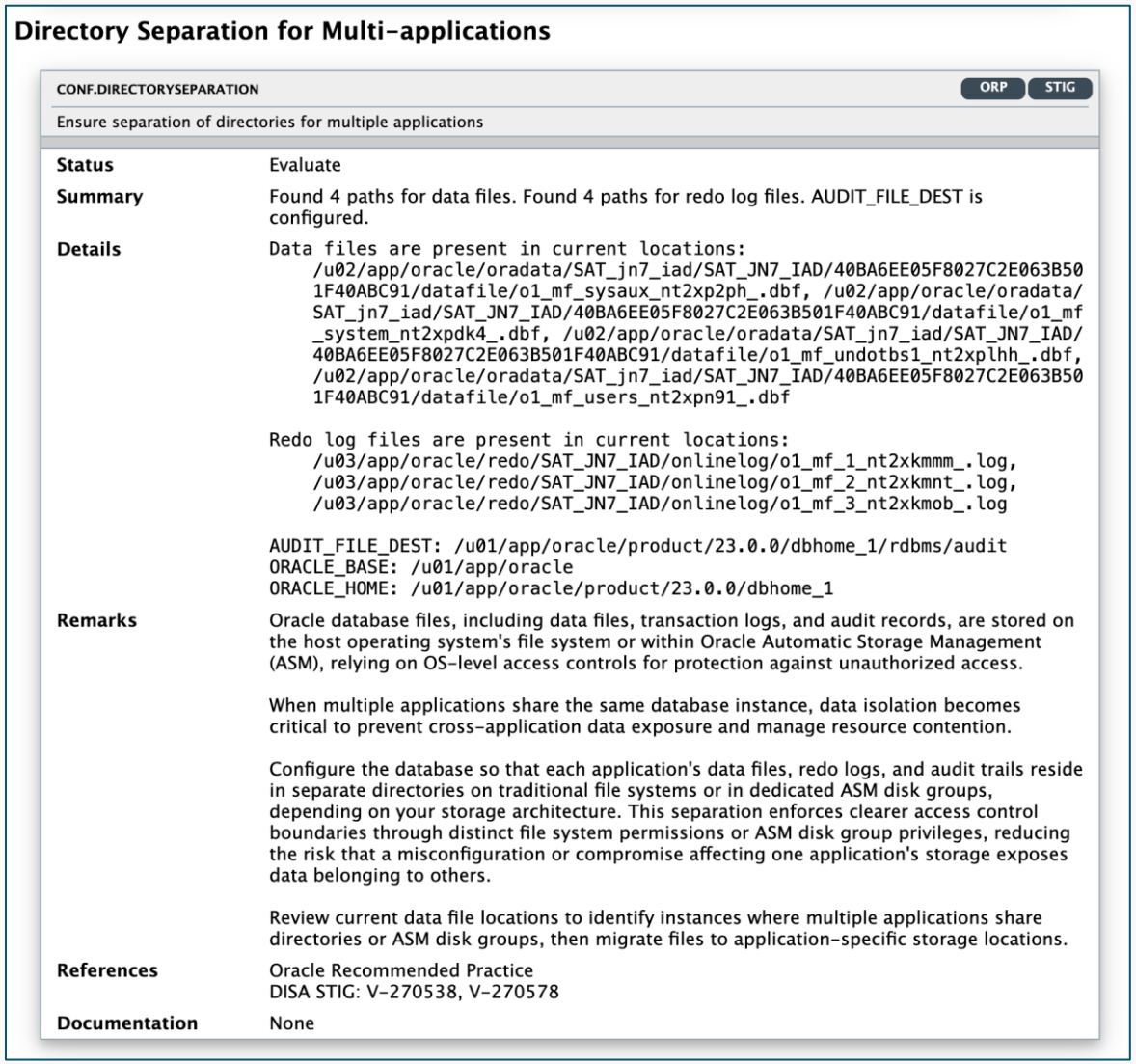
Review security assessment report findings

Status	Evaluate
Summary	Security Assessment was run on the current database. 10 sections in assessment report needs to be reviewed.
Details	Section Database Security Basics needs to be reviewed for 1 checks. Section User Accounts needs to be reviewed for 20 checks. Section Privileges and Roles needs to be reviewed for 29 checks. Section Auditing needs to be reviewed for 17 checks. Section Encryption needs to be reviewed for 3 checks. Section Authorization Control needs to be reviewed for 5 checks. Section Fine-Grained Access Control needs to be reviewed for 5 checks. Section Database Configuration needs to be reviewed for 16 checks. Section Network Configuration needs to be reviewed for 2 checks. Section Operating System needs to be reviewed for 6 checks.
Remarks	For each finding, DBSAT recommends remediation activities that follow best practices to reduce or mitigate risk. Review the security status provided by the DBSAT report, check the categories (sections), and review the findings by risk level and recommendations.
References	Oracle Recommended Practice DISA STIG: V-270520
Documentation	None

Highlight the need to review all findings

New STIG checks in DBSAT (4/5)

NEW in 4.0



Directory Separation for Multi-applications

CONF.DIRECTORYSEPARATION — ORP — STIG

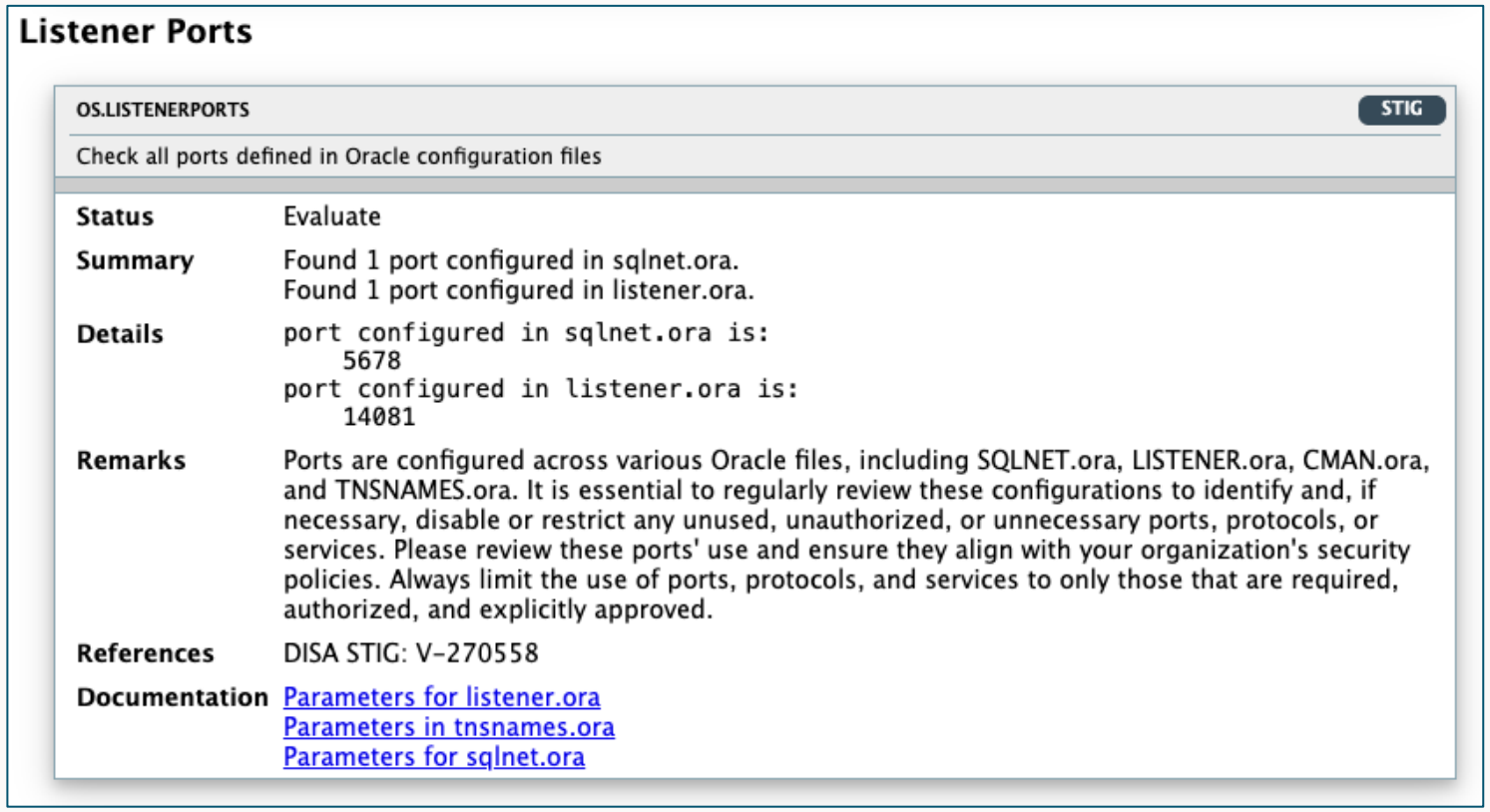
Ensure separation of directories for multiple applications

Status	Evaluate
Summary	Found 4 paths for data files. Found 4 paths for redo log files. AUDIT_FILE_DEST is configured.
Details	Data files are present in current locations: /u02/app/oracle/oradata/SAT_jn7_iad/SAT_JN7_IAD/40BA6EE05F8027C2E063B501F40ABC91/datafile/o1_mf_sysaux_nt2xp2ph_.dbf, /u02/app/oracle/oradata/SAT_jn7_iad/SAT_JN7_IAD/40BA6EE05F8027C2E063B501F40ABC91/datafile/o1_mf_system_nt2xpdk4_.dbf, /u02/app/oracle/oradata/SAT_jn7_iad/SAT_JN7_IAD/40BA6EE05F8027C2E063B501F40ABC91/datafile/o1_mf_undotbs1_nt2xplhh_.dbf, /u02/app/oracle/oradata/SAT_jn7_iad/SAT_JN7_IAD/40BA6EE05F8027C2E063B501F40ABC91/datafile/o1_mf_users_nt2xpn91_.dbf Redo log files are present in current locations: /u03/app/oracle/redo/SAT_JN7_IAD/onlinelog/o1_mf_1_nt2xkmmm_.log, /u03/app/oracle/redo/SAT_JN7_IAD/onlinelog/o1_mf_2_nt2xkmnt_.log, /u03/app/oracle/redo/SAT_JN7_IAD/onlinelog/o1_mf_3_nt2xkmob_.log AUDIT_FILE_DEST: /u01/app/oracle/product/23.0.0/dbhome_1/rdbms/audit ORACLE_BASE: /u01/app/oracle ORACLE_HOME: /u01/app/oracle/product/23.0.0/dbhome_1
Remarks	Oracle database files, including data files, transaction logs, and audit records, are stored on the host operating system's file system or within Oracle Automatic Storage Management (ASM), relying on OS-level access controls for protection against unauthorized access. When multiple applications share the same database instance, data isolation becomes critical to prevent cross-application data exposure and manage resource contention. Configure the database so that each application's data files, redo logs, and audit trails reside in separate directories on traditional file systems or in dedicated ASM disk groups, depending on your storage architecture. This separation enforces clearer access control boundaries through distinct file system permissions or ASM disk group privileges, reducing the risk that a misconfiguration or compromise affecting one application's storage exposes data belonging to others. Review current data file locations to identify instances where multiple applications share directories or ASM disk groups, then migrate files to application-specific storage locations.
References	Oracle Recommended Practice DISA STIG: V-270538, V-270578
Documentation	None

Checks for the location of data files, redo logs, and audit file destination

New STIG checks in DBSAT (5/5)

NEW in 4.0



Listener Ports

OS.LISTENERPORTS — STIG

Check all ports defined in Oracle configuration files

Status	Evaluate
Summary	Found 1 port configured in sqlnet.ora. Found 1 port configured in listener.ora.
Details	port configured in sqlnet.ora is: 5678 port configured in listener.ora is: 14081
Remarks	Ports are configured across various Oracle files, including SQLNET.ora, LISTENER.ora, CMAN.ora, and TNSNAMES.ora. It is essential to regularly review these configurations to identify and, if necessary, disable or restrict any unused, unauthorized, or unnecessary ports, protocols, or services. Please review these ports' use and ensure they align with your organization's security policies. Always limit the use of ports, protocols, and services to only those that are required, authorized, and explicitly approved.
References	DISA STIG: V-270558
Documentation	Parameters for listener.ora Parameters in tnsnames.ora Parameters for sqlnet.ora

Checks for known listener ports.

Better CVE Visibility

Updated in 4.1

Patch Check

INFO.PATCH — CIS ORP STIG

The Oracle Database should be patched regularly

Status	High Risk
Summary	Oracle Database version is supported but latest patch is missing. Latest comprehensive patch has not been applied.
Details	The latest patch for the currently supported database version has not been applied. The current release version is 23.26.0. while the latest available patch is 23.26.01. The absence of the latest patch leaves the database vulnerable to the following CVEs: CVE-2025-12383, CVE-2026-21939, CVE-2025-8194, CVE-2025-67735, CVE-2025-61755, CVE-2025-54874, CVE-2025-13836, CVE-2025-13837, CVE-2025-6069, CVE-2025-6075, CVE-2025-8291, CVE-2025-8869 Installed SQL Patch History: Action time: Thu Oct 09 2025 13:02:19 Action: APPLY Version: 23.26.0.0.0 Description: Database Release Update : 23.26.0.0.0 (38404116) Gold Image
Remarks	Apply the latest Release Update (RU) immediately to maintain Oracle support eligibility and protect against known security vulnerabilities. RUs are released quarterly in January, April, July, and October. These updates contain critical security vulnerability fixes, regression corrections, and functional enhancements for each version of the database. Operating databases on outdated RUs results in an unsupported and high-risk security posture, increasing exposure to known exploits and compliance violations. Oracle AI Database 26ai replaces Oracle Database 23ai starting with RU 23.26.0 (Oct 2025).
References	Oracle Recommended Practice CIS Benchmark: Recommendation 1.1 DISA STIG: V-270513, V-270585
Documentation	Download Security Patches

On-premises Oracle AI Database

Unpatched CVEs are now highlighted

Patch Check

INFO.PATCH — CIS ORP STIG

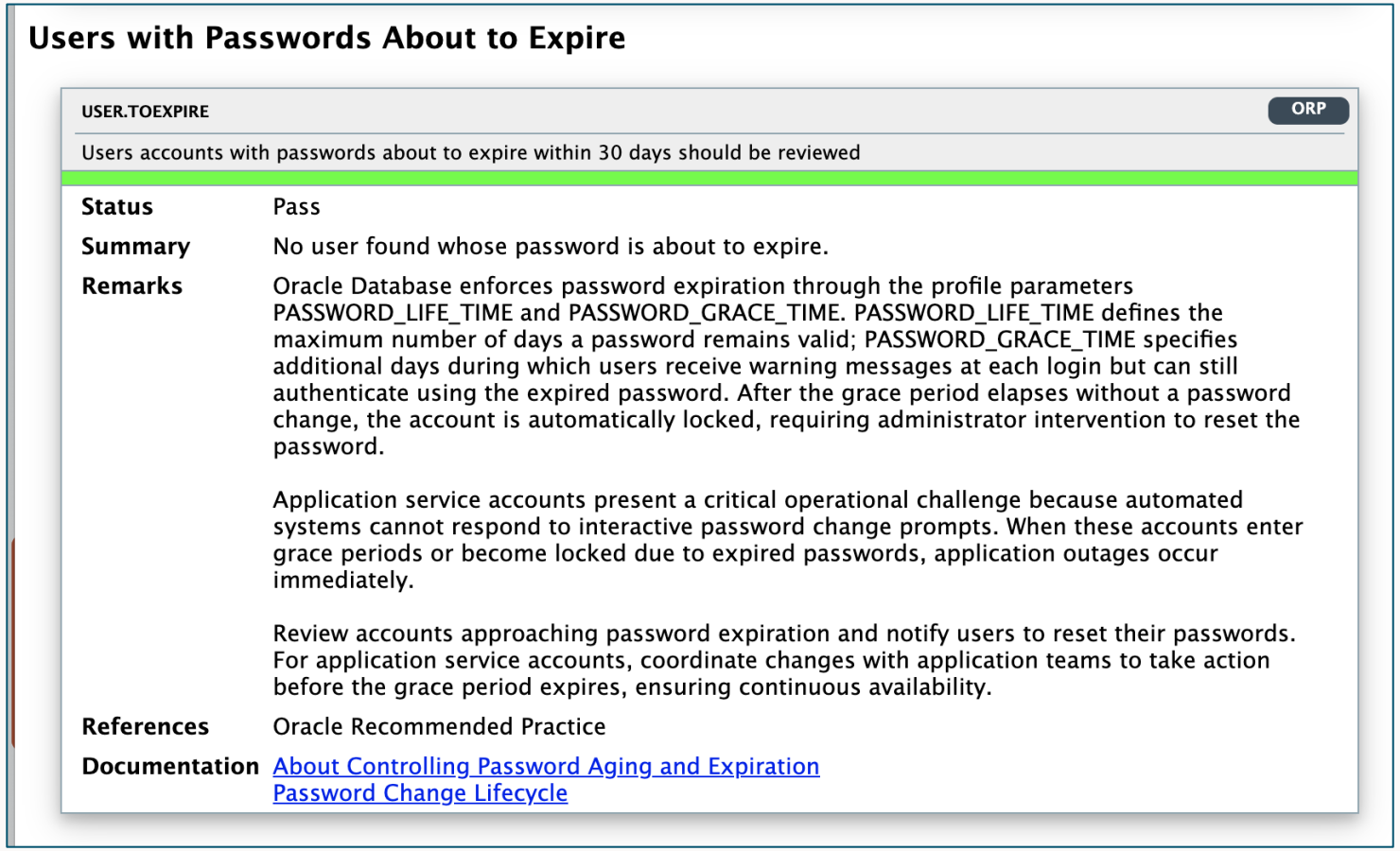
The Oracle Database should be patched regularly

Status	High Risk
Summary	Oracle Database version is supported but latest patch is missing. Latest comprehensive patch has not been applied.
Details	The latest patch for the currently supported database version has not been applied. The current release version is 23.09 while the latest available patch is 23.26. The absence of the latest patch leaves the database vulnerable to the following CVEs: CVE-2025-4517, CVE-2024-12254, CVE-2024-12718, CVE-2024-6923, CVE-2024-8088, CVE-2025-1795, CVE-2025-4138, CVE-2025-4330, CVE-2025-4435, CVE-2025-4949, CVE-2025-53051, CVE-2025-61749, CVE-2025-50106, CVE-2025-59375, CVE-2025-31672, CVE-2025-61881, CVE-2025-53047, CVE-2025-26333, CVE-2025-12383, CVE-2026-21939, CVE-2025-8194, CVE-2025-67735, CVE-2025-61755, CVE-2025-54874, CVE-2025-13836, CVE-2025-13837, CVE-2025-6069, CVE-2025-6075, CVE-2025-8291, CVE-2025-8869 Last installed SQL Patch details: Action time: Mon Oct 06 2025 01:52:38 Action: APPLY Version: 23.10.0.25.10 Description: ADW Bundle Patch : 23.4.0.0.0 (38361783)
Remarks	Oracle Autonomous AI Databases offer varying degrees of flexibility for deferring maintenance and patching activities. To view the next scheduled maintenance window, navigate to the Autonomous AI Database details page in the OCI console and check the 'Next Maintenance' field for the start and end times. Operating databases on outdated RUs results in an unsupported and high-risk security posture, increasing exposure to known exploits and compliance violations. Your database is approaching the maximum allowable deferral period for maintenance, it's crucial to schedule patching immediately to maintain security and performance. In the OCI console, go to the Autonomous AI Database service console, select your database, and under the 'Maintenance' section, schedule the patching at the earliest possible time. Oracle AI Database 26ai replaces Oracle Database 23ai starting with RU 23.26.0 (Oct 2025).
References	Oracle Recommended Practice CIS Benchmark: Recommendation 1.1 DISA STIG: V-270513, V-270585
Documentation	Download Security Patches

Oracle Autonomous AI Database

Users with passwords about to expire

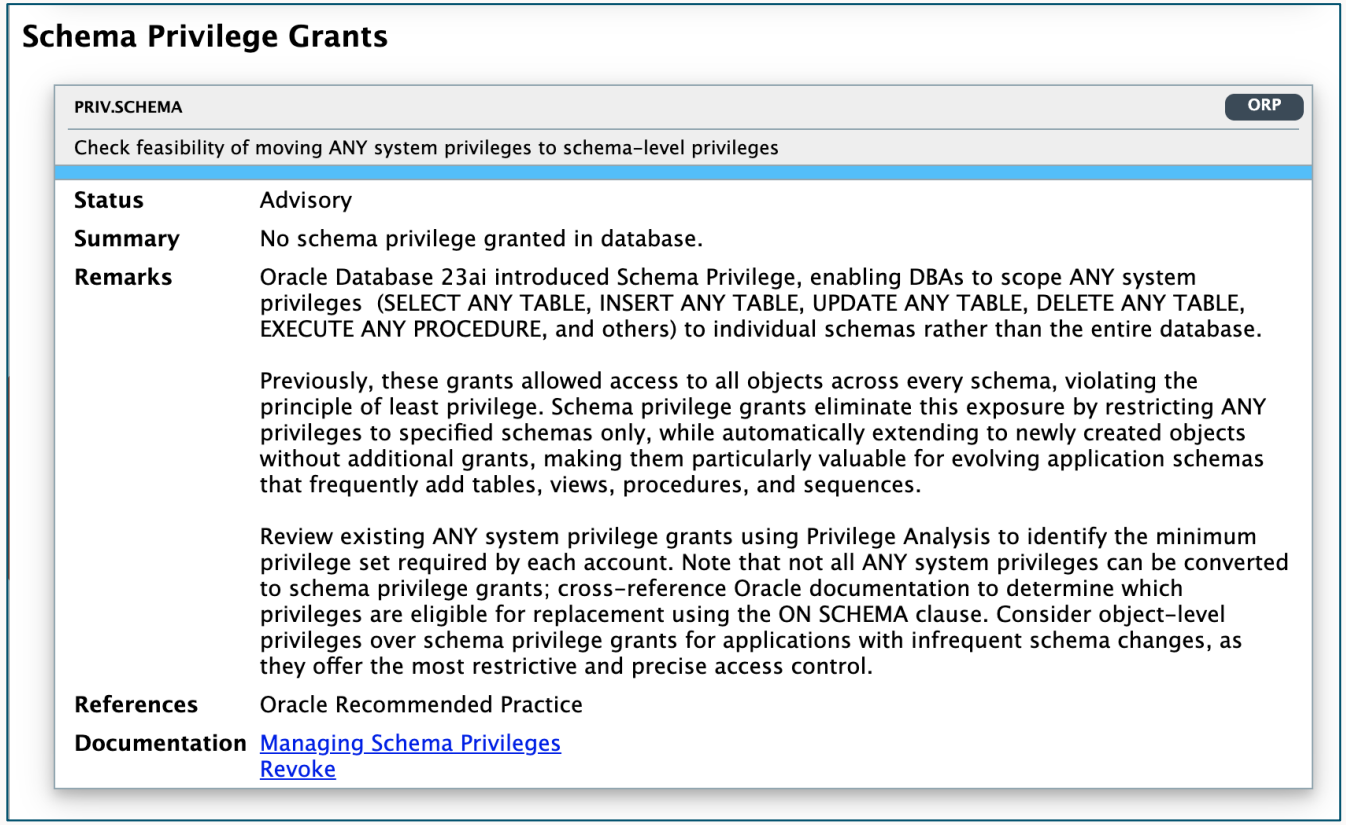
NEW in 4.0



Displays information about user accounts that will expire their passwords within 30 days.

Schema Privileges

NEW in 4.0



Displays information about user accounts with ANY system privileges and schema-level grants.

This will allow reviewing cases where SELECT ANY TABLE system privilege was granted to simplify management and replace them with schema-level grants instead.

Database Vault (1/3)

Updated in 4.0

Database Vault

AUTHZ.DATABASEVAULT — GDPR | ORP | STIG

Ensure proper configuration of Database Vault command rules and realms

Status	Evaluate
Summary	Database vault is enabled in 1 PDB (CDB1_PDB1). Found 5 Database Vault realms and 5 command rules.
Details	Realms: HR.EMPLOYEES_Realm (Simulation mode) OBJECTS Protected: HR.EMPLOYEES (TABLE) Realm (Enabled) Realm1 (Disabled) OBJECTS Protected: DV_TEST_SCHEMA1.<Any Object> (Any Type) Realm2 (Disabled) Realm3 (Disabled) Command Rules: CREATE PLUGGABLE DATABASE (Enabled) CREATE TABLE on DV_TEST_SCHEMA1.<Any Object> (Enabled) DROP TABLE on DV_TEST_SCHEMA1.<Any Object> (Disabled) INSERT on DV_TEST_SCHEMA1.<Any Object> (Enabled) SELECT on DV_TEST_SCHEMA1.<Any Object> (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.
References	Oracle Recommended Practice EU GDPR: Article 6, 25, 29, 32, 34, 89; Recital 28, 29, 78, 156 DISA STIG: V-270500, V-270572
Documentation	What is Oracle Database Vault Restrict common users from seeing PDB data Database Vault roles DBA Operations in an Oracle Database Vault Environment AUTHORIZE_PROXY_USER Procedure

Displays whether Oracle Database Vault is enabled, details realms, command rules, their status, and protected objects.

Database Vault (2/3)

NEW in 4.0

Database Vault Separation of Duty

AUTHZ.DATABASEVAULTSOD — ORP

Ensure Database Vault Separation of Duties

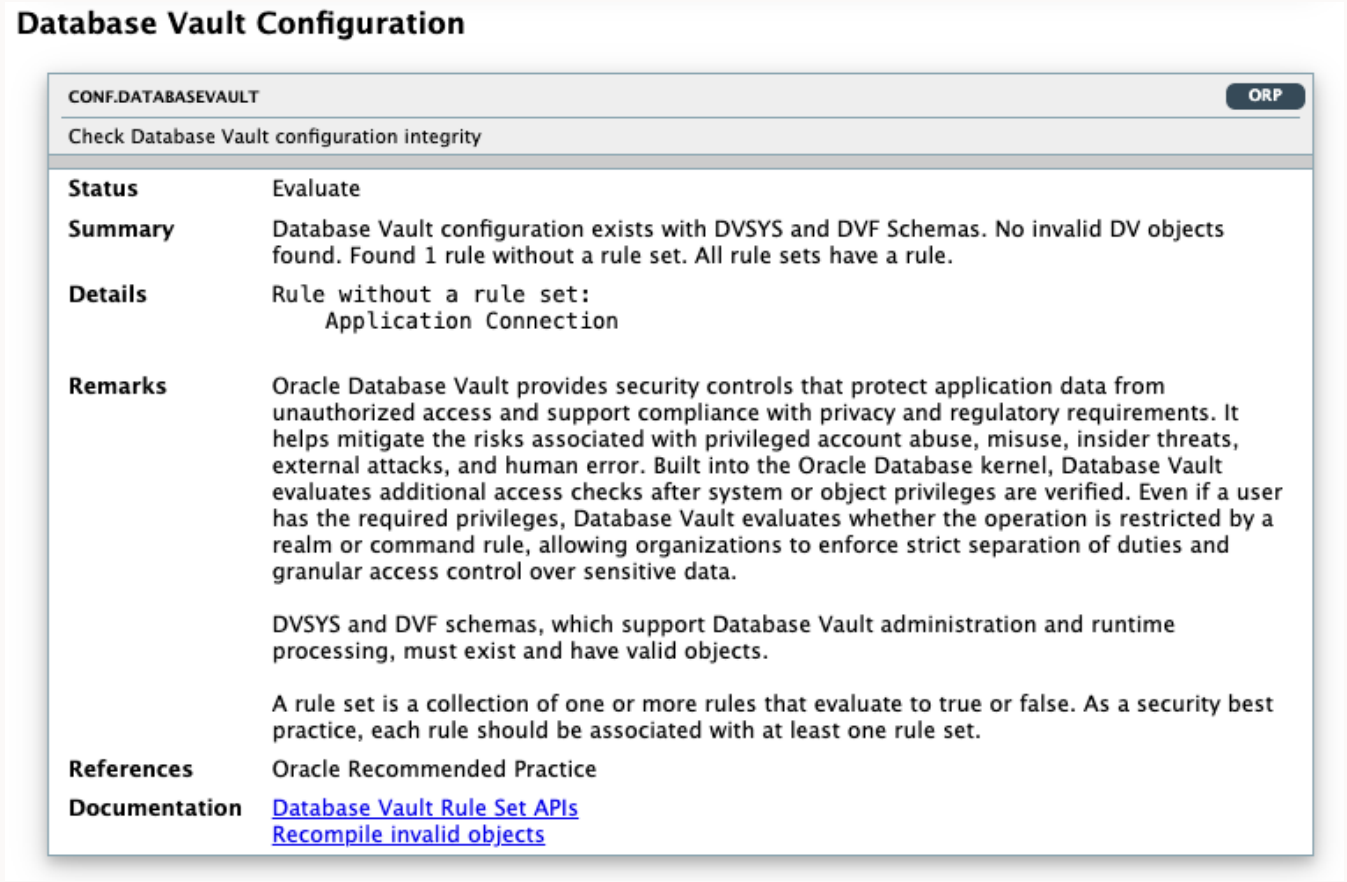
Status	Evaluate
Summary	Found 1 user with Data Pump operation roles but not granted the proper Database Vault authorization. All proxy-client pairs are authorized by Database Vault. Found 5 DV Roles granted to 5 users. Found 1 User Granted with DV_OWNER role with ADMIN option. Found 1 User Granted with DV_ACCTMGR role with ADMIN options. SYS is Not granted any DV role. Database Vault operations control is not enabled.
Details	User with Data Pump operation roles but not granted the proper Database Vault authorization: BACKUP_ADMIN Users with Database Vault Roles: DV_OWNER: DBV_OWNER_PDB1(*)(Recommended is 2 users with admin option) DV_PATCH_ADMIN: MASKING_ADMIN DV_ACCTMGR: DBV_ACCTMGR_PDB1(*)(Recommended is 2 users with admin option) DV_SECANALYST: DBSAT_ADMIN DV_DATAPUMP_NETWORK_LINK: BACKUP_ADMIN, MASKING_ADMIN (*) = granted with admin option (Checked only for DV_ACCTMGR and DV_OWNER)

Displays information about users with Database Vault-specific roles, including DV_OWER, DV_ACCTMGR, DV_PATCH_ADMIN, and others.

It also verifies if users have been properly authorized for specific operations (e.g., Data Pump export/import requires roles and a specific Database Vault authorization) and checks if Database Vault operation control is enabled.

Database Vault (3/3)

NEW in 4.0



Checks for Database Vault integrity. Validates the presence of both the DVSYS and DVF schemas, checks for invalid Database Vault objects, identifies rules that are not associated with any rule sets, and flags any empty rule sets.

Resource Manager Plans

NEW in 4.0

Database Resource Plans

CONF.RESOURCEMANAGER — ORP

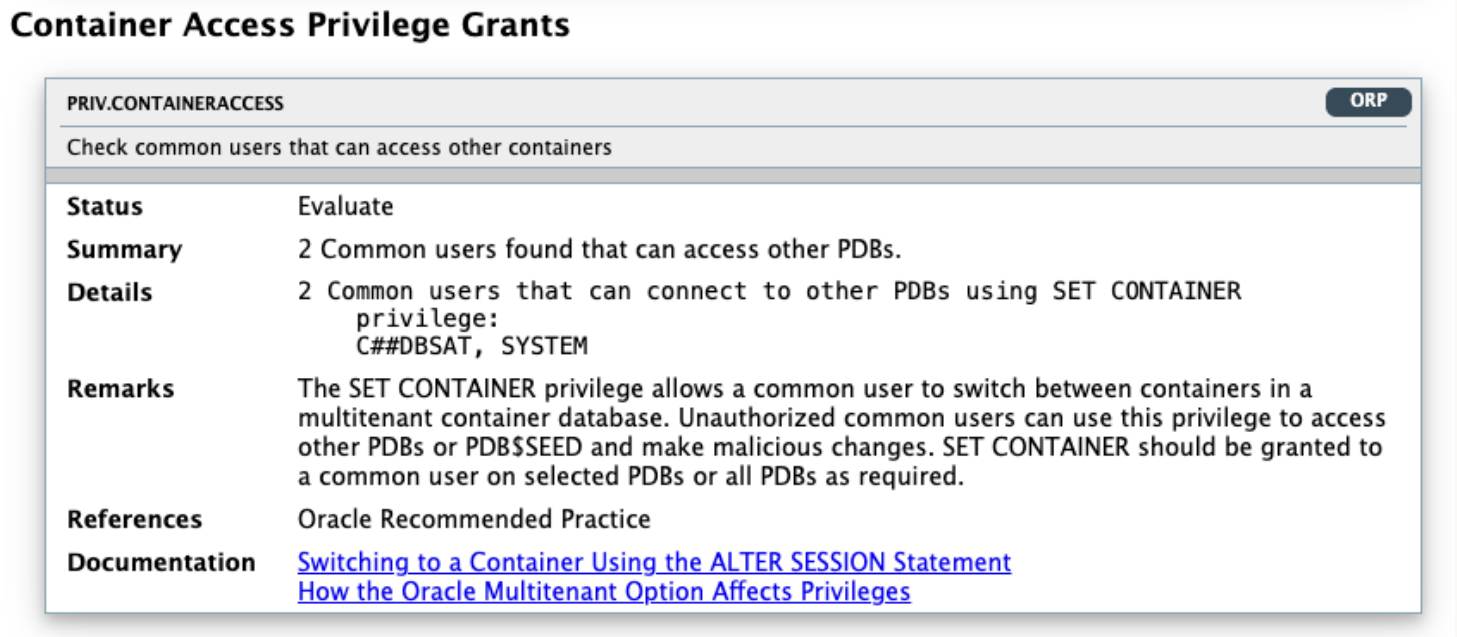
Check enabled resource manager plans

Status	Evaluate
Summary	Found 11 users with EXECUTE on DBMS_RESOURCE_MANAGER package and a system privilege that allows them to create and manage resources in the database using DBMS_RESOURCE_MANAGER package. Found 1 enabled plan in the database.
Details	Users with system privilege (ADMINISTER RESOURCE MANAGER) and EXECUTE on DBMS_RESOURCE_MANAGER package: BACKUP_ADMIN, C##ZEUS, DBA_DEBRA, DBA_HARVEY, DBA_NICOLE, DMS_ADMIN, EVIL_RICH, JSCHAFFER, JTAYLOR, MASKING_ADMIN, SCOTT SHARES: 1 PLAN NAME: INTERNAL_PLAN UTILIZATION_LIMIT: 100% CPU_COUNT: 4 CPU_MIN_COUNT: 4 PARALLEL_SERVER_LIMIT: 100% PARALLEL_SERVERS_ACTIVE: 0 PARALLEL_SERVERS_TOTAL: 32 PARALLEL_EXECUTION_MANAGED: FIFO
Remarks	The DBMS_RESOURCE_MANAGER package is used to create and maintain resource plans, consumer groups, and plan directives. With the DBMS_RESOURCE_MANAGER package, you can control resource allocation, ensuring critical workloads get the necessary resources. Users with EXECUTE on the package and ADMINISTER RESOURCE MANAGER system privilege can manage resource plans. You should review the existing plans to validate they are set to meet your organization's needs and control who has EXECUTE privilege on DBMS_RESOURCE_MANAGER and has ADMINISTER RESOURCE MANAGER. Users with these privileges can create and modify resource plans, potentially disrupting database operations or causing performance degradation. You can limit CPU threads for a PDB by setting the initialization parameters CPU_COUNT (upper limit) and CPU_MIN_COUNT (lower limit).
References	Oracle Recommended Practice
Documentation	Managing Resources with Oracle Database Resource Manager About Resource Manager Administration Privileges DBMS_RESOURCE_MANAGER

Checks for users with EXECUTE on DBMS_RESOURCE_MANAGER package and with ADMINISTER RESOURCE MANAGER system privilege. Also lists the existing resource plans.

Container Access

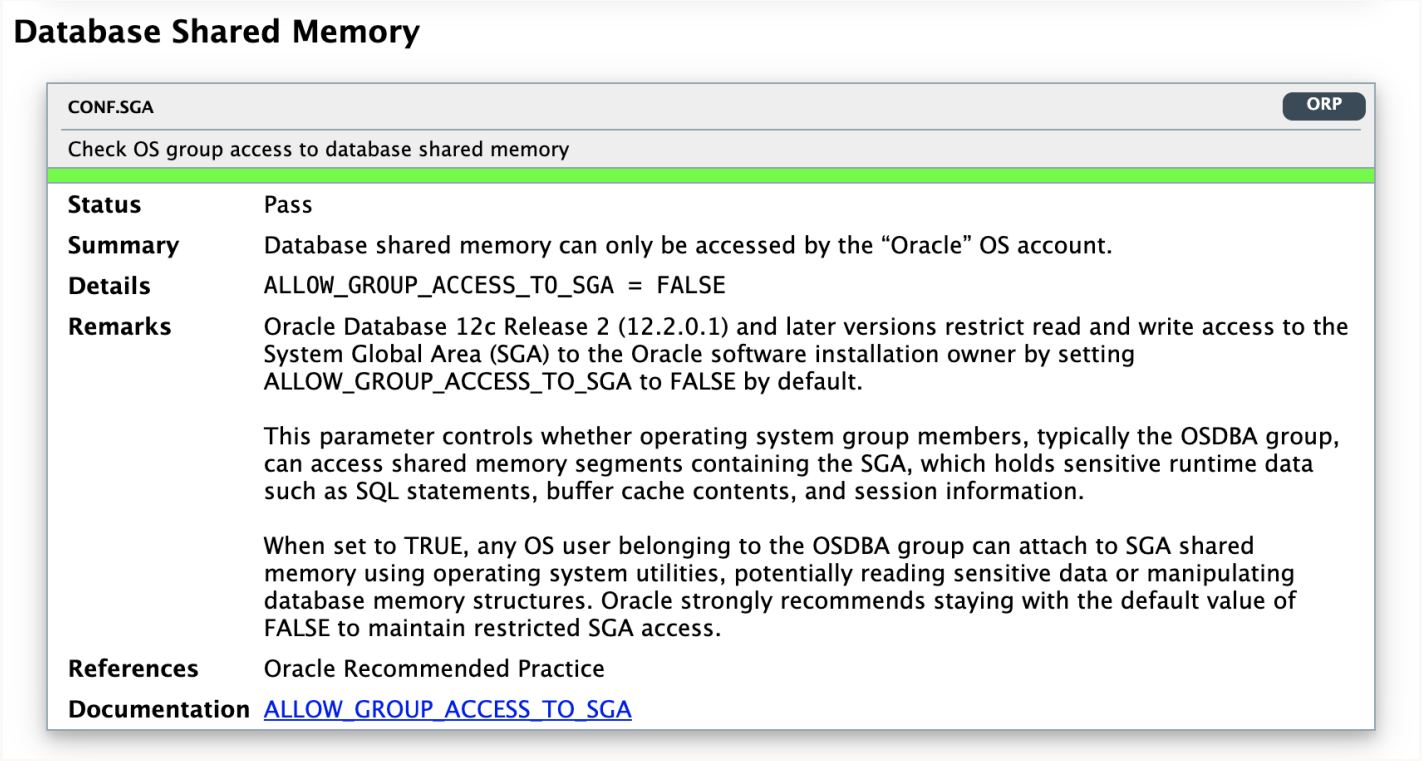
NEW in 4.0



Displays information about common users with set container privilege grants.
This is a CDB check.

Database Shared Memory Access

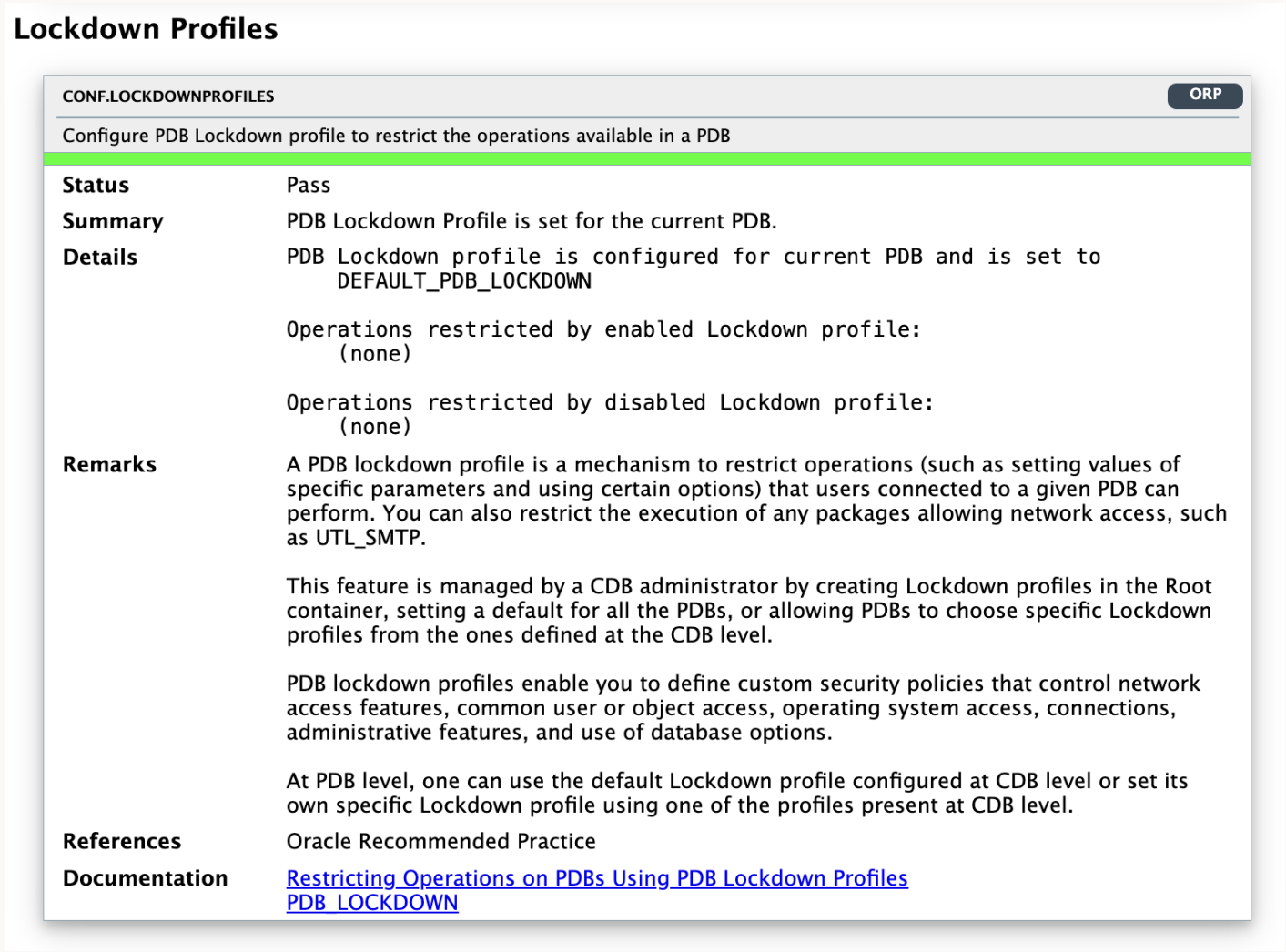
NEW in 4.0



Checks if only the Oracle software installation owner have read and write access to the SGA.

PDB Lockdown Profiles

NEW in 4.0



Lockdown Profiles

CONF.LOCKDOWNPROFILES — ORP

Configure PDB Lockdown profile to restrict the operations available in a PDB

Status	Pass
Summary	PDB Lockdown Profile is set for the current PDB.
Details	PDB Lockdown profile is configured for current PDB and is set to DEFAULT_PDB_LOCKDOWN Operations restricted by enabled Lockdown profile: (none) Operations restricted by disabled Lockdown profile: (none)
Remarks	A PDB lockdown profile is a mechanism to restrict operations (such as setting values of specific parameters and using certain options) that users connected to a given PDB can perform. You can also restrict the execution of any packages allowing network access, such as UTL_SMTP. This feature is managed by a CDB administrator by creating Lockdown profiles in the Root container, setting a default for all the PDBs, or allowing PDBs to choose specific Lockdown profiles from the ones defined at the CDB level. PDB lockdown profiles enable you to define custom security policies that control network access features, common user or object access, operating system access, connections, administrative features, and use of database options. At PDB level, one can use the default Lockdown profile configured at CDB level or set its own specific Lockdown profile using one of the profiles present at CDB level.
References	Oracle Recommended Practice
Documentation	Restricting Operations on PDBs Using PDB Lockdown Profiles PDB_LOCKDOWN

Checks whether a PDB lockdown profile is configured for the current PDB. If a profile is set, it lists the restricted functionalities along with their current status. Also verifies if the PDB_LOCKDOWN parameter is set and displays its value.

Better Usability & Advanced Options

Collect just X rows.

```
./dbsat collect -r 16000 dbsat_admin@freepdb1 pdb1
```

Show warning and generate collector.log file.

```
./dbsat collect -d dbsat_admin@freepdb1 pdb1
```

Generate the report just in HTML format.

```
./dbsat report -f html pdb1
```

Extract report from .dbsat encrypted output files

```
./dbsat extract pdb1
```

How can DBSAT Help?

Assess your database security before hackers come knocking

How to Get Started?

Quick & Simple!

3-Step flow

1 Run
./dbsat collect

2 Run
./dbsat report

3 Run
./dbsat discover

Collector & Reporter

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

Generates summary output with prioritized findings

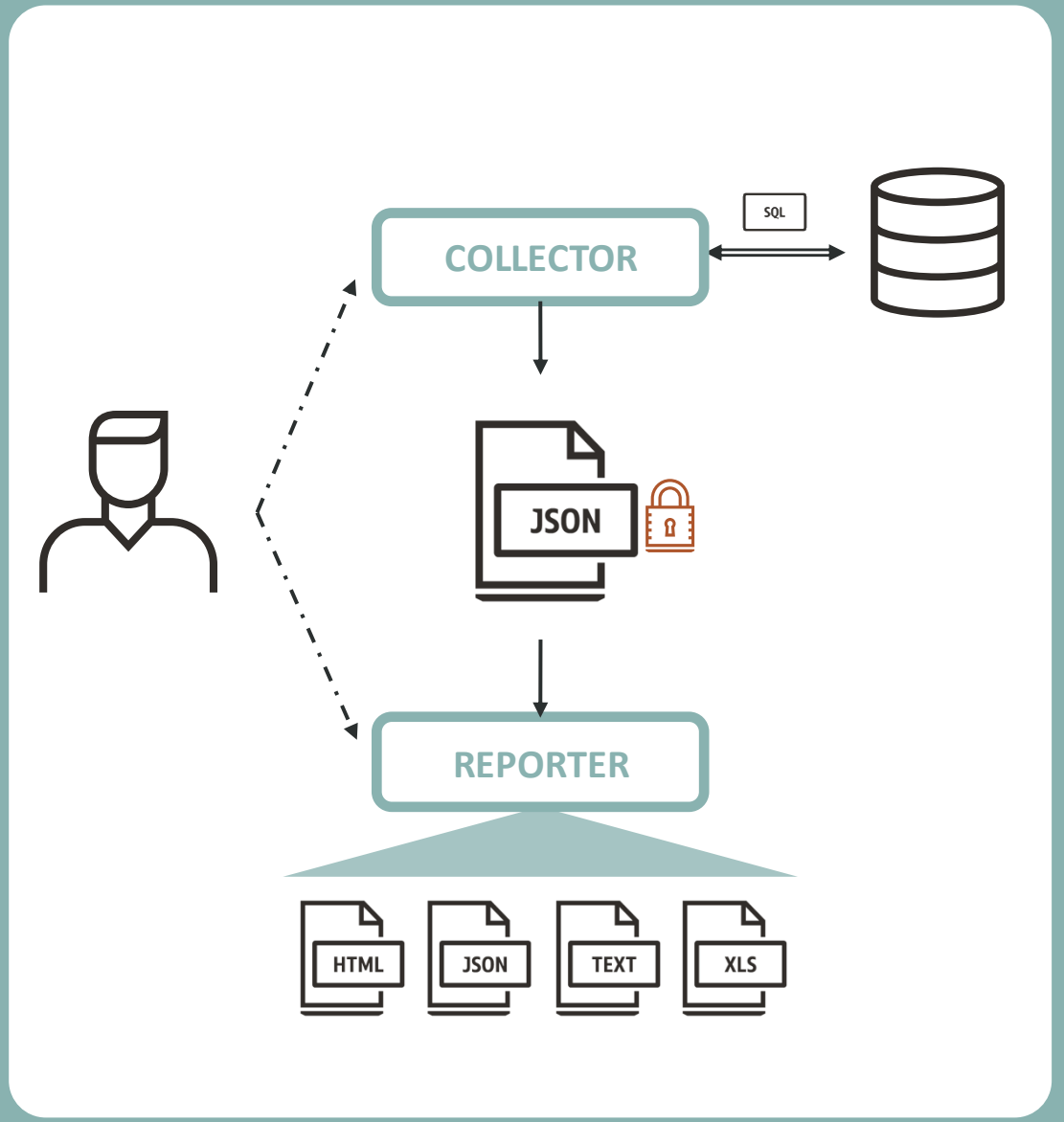
Summary table with identified risks organized by domains: Basic information, user accounts, privileges and roles, authorization control, fine-grained access control, auditing, encryption, config, etc.

Over 140 detailed findings with remarks

Each finding contains a one line explanation of what is expected, a risk level, details, remarks, and documentation links..

References to Oracle Best Practices, CIS Benchmark, STIG Rules and GDPR articles/recitals

Along with Oracle Database security development organization recommended practices, there is a mapping to CIS, STIG rules, and EU GDPR articles and recitals.



Discoverer

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

Discovers sensitive data

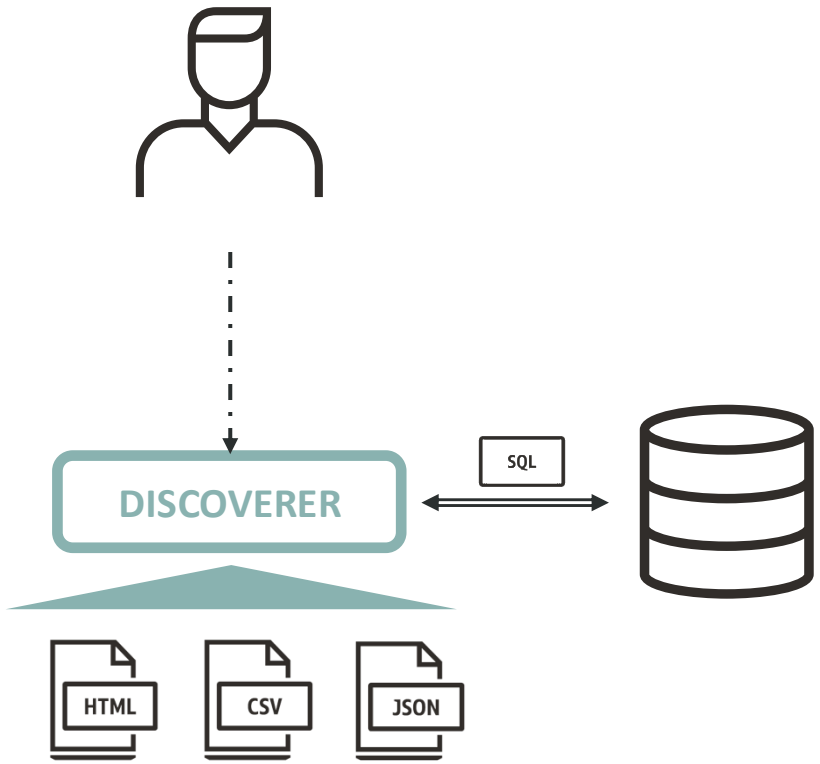
Get summary and details on Sensitive Data Categories and Types (125+), tables, columns, rows, and risk levels.

Provides recommendations on security controls

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

Customizable

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



What else?

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

Data Safe helps secure Oracle database targets everywhere

Security Assessment

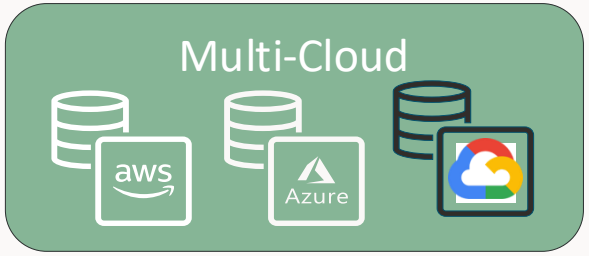
User Assessment

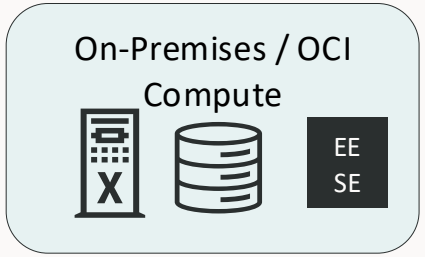
Activity Auditing

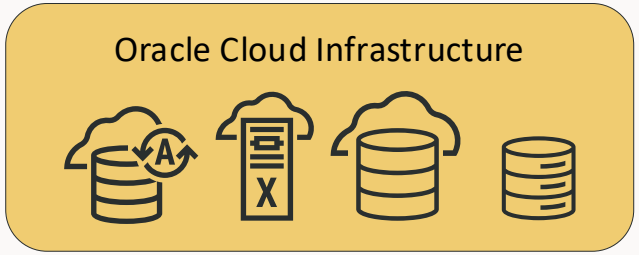
Data Masking

Sensitive Data Discovery

SQL Firewall



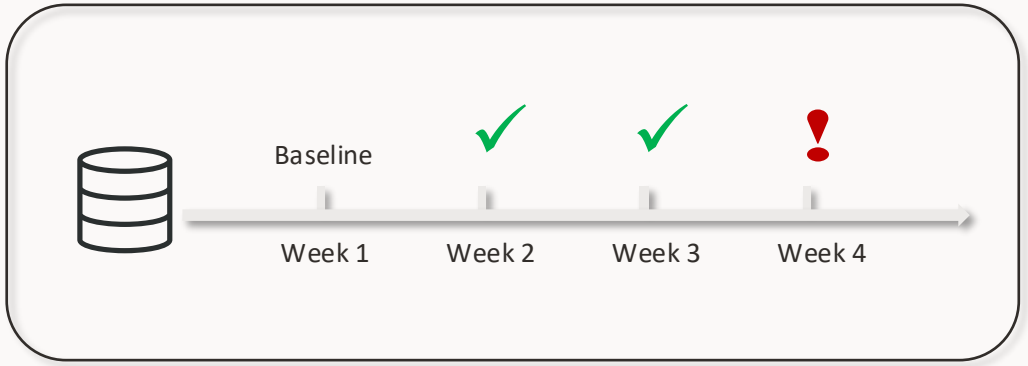




Get instant insights into database security configuration

Data Safe Security Assessment

- Assess security configurations
- Fleet-wide view of risks and
- Detect configuration drifts



Latest assessment for target database: angdbpmazure1

Refresh now | Set as baseline | View history | Update schedule | More actions

Assessment summary | Assessment information | Tags

Top 5 common security controls

PASS **Users with no Password Complexity Requirements** All user accounts are using password verification function.	PASS **Network Encryption** Network traffic is encrypted.	PASS **Patch Check** Maintenance updates applied during last 90 days.	PASS **Transparent Data Encryption** Found 6 encrypted tablespaces. No unencrypted tablespaces found. No encrypted columns found.	PASS **Audit User Logon and Logoff** Database connection events are audited for all users.

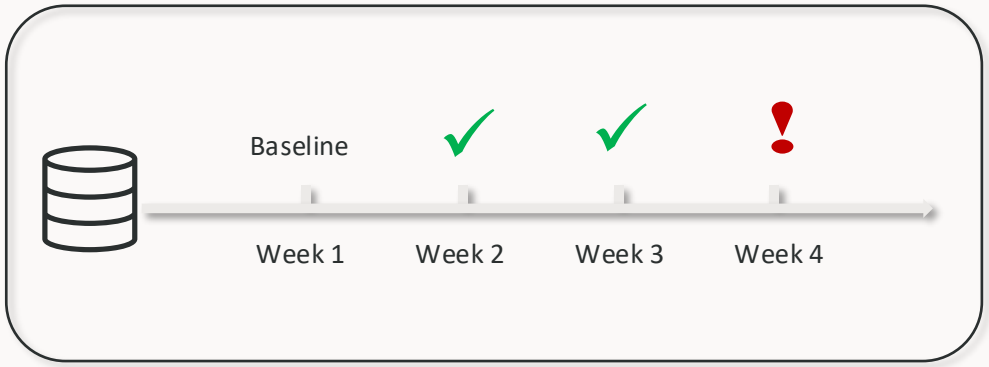
Summary

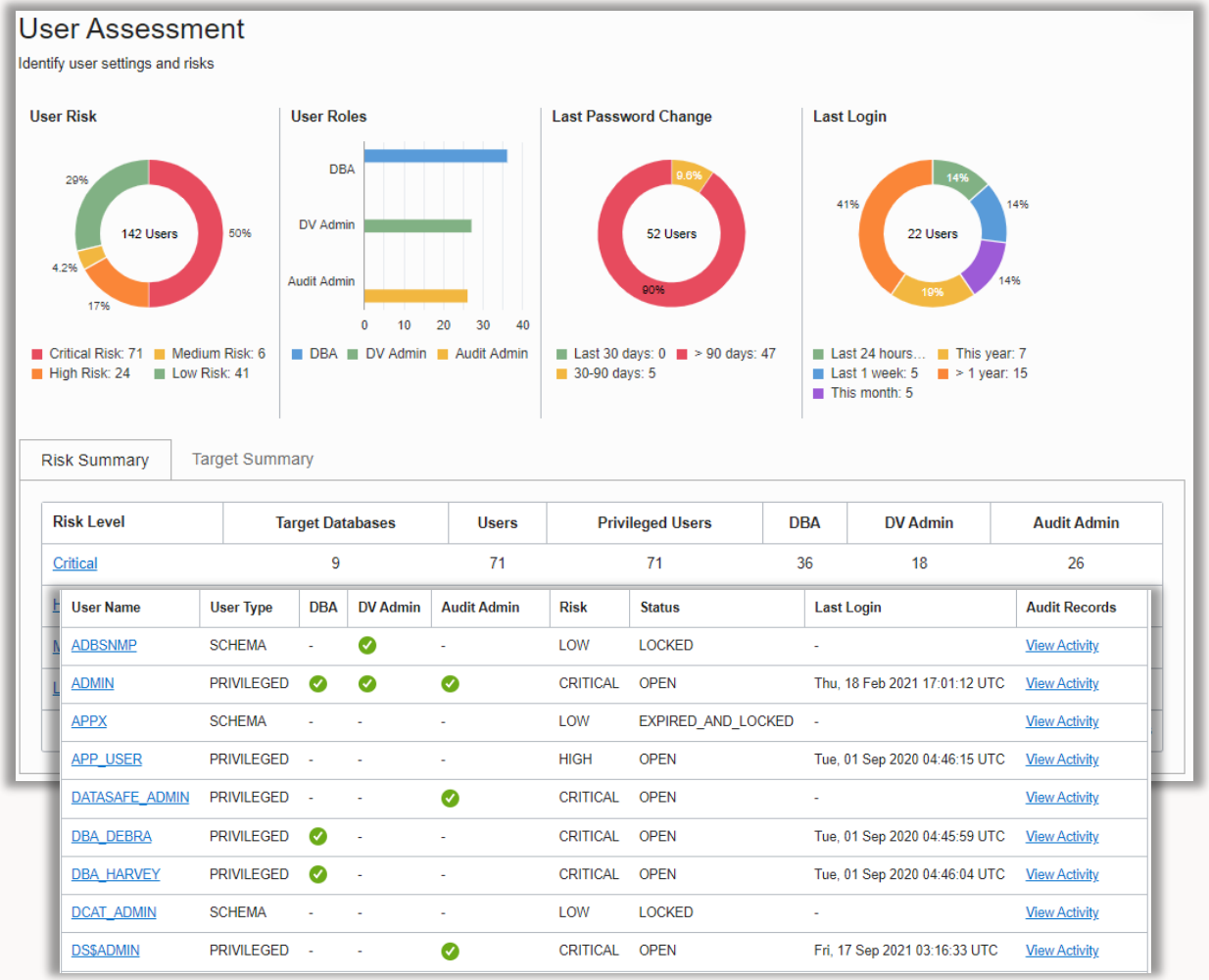
Category	High risk	Medium risk	Low risk	Advisory	Evaluate	Pass	Deferred	Total findings
User accounts	-	-	4	-	9	8	-	**21**
Privileges and roles	-	-	-	-	23	5	-	**28**
Authorization control	-	-	-	2	3	-	-	**5**
Fine-grained access control	-	-	-	4	1	-	-	**5**
Auditing	-	-	-	6	7	4	-	**17**
Encryption	-	-	-	-	1	2	-	**3**
Database configuration	-	-	1	1	4	9	-	**15**
Total risks	**-**	**-**	**5**	**13**	**48**	**28**	**-**	**94**

Reduce risk from users by managing roles/privileges and policies

Data Safe User Risk Assessment

- Identify highly privileged users
- Reduce user account risks
- Spot user and entitlement changes
- Review who can access specific data and how access was granted





Audit Vault and Database Firewall for Oracle Database

Database Security Posture Management (DSPM)

- ✓ Database Discovery
- ✓ Privileged User Discovery
- ✓ Sensitive Data Discovery
- ✓ Security Assessment

- ✓ Audit Policy Management
- ✓ Report Before/After Values*
- ✓ Audit reports for Key Vault, Database Vault, SQL Firewall

Best Auditing, Activity Monitoring, and Posture Management for Oracle databases

*Also available for SQL Server and MySQL

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

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

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

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

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

Summary

Get Started with DBSAT 4.0

Easy to install and run

Download:

- oracle.com/security/database-security/assessment-tool/

Generate Reports:

- Security assessment:
  - Run `dbsat collect` on your target database
  - Run `dbsat report` to create the assessment report

- Sensitive data discovery:
  - Run `dbsat discover` (no collect step required)

Documentation:

- Release notes
- User's Guide

DBSAT is free for customers with an active support contract.

Action plan

Monday Morning

Run DBSAT to assess your current database security state.

What is measured gets done!

Next 30 days

Fix obvious mistakes and high-risk findings.

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

A data breach impacts your business.

Next 90 days

Update Data Security strategy to include database security best practices.

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

Want to learn more?

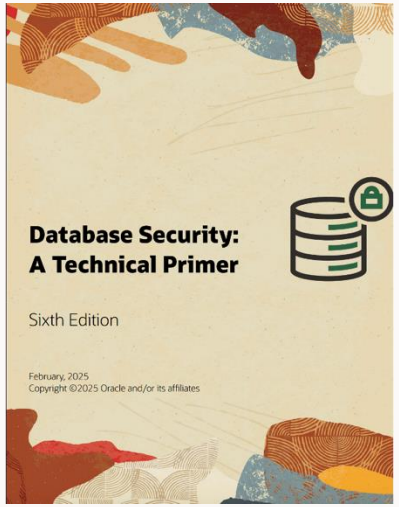
Free hands-on labs that help you learn how to use the different security features and options

livelabs.oracle.com

Database Security office hours – second Wednesday of each month

asktom.oracle.com

Securing the Oracle Database – a technical primer (6th edition)



oracle.com/securingthedatabase


ORACLE