

Oracle Database Security Assessment Tool

ORACLE® Database

KEY BUSINESS BENEFITS

- Quickly assess the current security status and identify sensitive data within the Oracle database
- Reduce risk exposure using proven Oracle Database Security best practices and CIS benchmark recommendations
- Leverage security findings to accelerate compliance with EU GDPR and other regulations
- Installs and provides valuable reports in minutes
- Provided at no additional cost to Oracle customers

KEY FEATURES

- Identify configuration settings that may increase your risk exposure
- Identify sensitive user accounts, their entitlements, and security policies
- Discover sensitive data
- Recommend and prioritize relevant security controls

With data breaches growing every day along with the evolving set of data protection and privacy regulations, protecting business sensitive and regulated data is mission critical. However, knowing whether the database is securely configured, who can access it, and where sensitive personal data resides is a challenge for most organizations. As part of Oracle's defense in depth capabilities, the Oracle Database Security Assessment Tool (DBSAT) helps identify areas where your database configuration, operation, or implementation introduces risks and recommends changes and controls to mitigate those risks.

Evolving Regulatory Compliance

Security configuration scanning has become an important part of many regulations such as the EU General Data Protection Regulation (EU GDPR), Payment Card Industry Data Security Standard (PCI-DSS), and numerous breach notification laws. Various organizations such as the Center for Internet Security (CIS) and U.S. Department of Defense also have recommendations for security configuration best practices. The importance of security controls cannot be understated as new regulations are being released and existing regulations are evolving aiming to protect the most valuable asset of many organizations – the data.

One of the biggest challenges organizations face before they put new controls in place is understanding their database security posture. They need to quickly identify how securely their databases are configured, where sensitive data is, how much sensitive data they have, which users have access to that data, what are their entitlements, and what security controls are implemented.

Whether your database is running on-premises or in the Cloud, the Oracle Database Security Assessment Tool (DBSAT) identifies potential sensitive data and areas where your database configuration, operation, or implementation introduces risk. DBSAT collects and analyzes different types of data from the database to identify the security risks. DBSAT further recommends changes and controls to mitigate those risks.

Think Like a Hacker

Attackers typically spend considerable time understanding their target. They may use several tools that automate the discovery of databases, open ports, known vulnerabilities, and sensitive user accounts. They may then launch various attacks including password theft, brute force password cracking, privilege escalations, and SQL injection attacks. Once they finish probing, they identify the weakest links and then

determine their next steps. In essence, the attackers first evaluate the current security status to find the easiest way to get to the sensitive data without being caught.

For example, if the data is encrypted, they probably need to get into the database as an authorized user. Are there users using default passwords? Can I escalate privileges? Is auditing on? Who has DBA-like privileges? What are the known vulnerabilities for this database version? Have those been patched? Which packaged applications are running? Are they running with powerful system privileges? What type of sensitive data do they process? All these and many more questions are inside the hacker's mind, and these answers help them come up with a plan to break into the database and steal your data.

As the owners, controllers, or processors of data, organizations need to think similarly, but with the aim to improve the security posture before the hackers target their databases.

Despite knowledge of what is needed to evaluate the current security posture and avoid being caught off guard, many organizations struggle to assess the security of their databases due to lack of database security expertise, shortage of time, lack of proper prioritization, or misunderstanding of the risks. Knowledge of how to secure a database might also be organizationally scattered between the DBAs and the IT Security team that is mostly focused on protecting the network or the endpoints.

Oracle DBSAT accelerates the assessment process by collecting relevant types of configuration information from the database, and evaluating the current security state to provide recommendations on how to mitigate the identified risks. DBSAT quickly provides a view on how securely the database is configured, who are the users and what are their entitlements, what security policies are in place, what security controls are implemented, and where sensitive data resides. The figure below summarizes the security status of a sample database, and categorizes its findings by risk levels.

RELATED PRODUCTS

Oracle Database Defense-In-Depth Security Products:

- Oracle Advanced Security
- Oracle Key Vault
- Oracle Database Vault
- Oracle Data Masking and Subsetting
- Oracle Label Security
- Oracle Audit Vault and Database Firewall

Section	Pass	Evaluate	Advisory	Low Risk	Medium Risk	High Risk	Total Findings
Basic Information	0	0	0	0	0	1	1
User Accounts	2	0	0	5	4	1	12
Privileges and Roles	2	11	0	0	6	0	19
Authorization Control	0	1	1	0	0	0	2
Data Encryption	0	1	1	0	0	0	2
Fine-Grained Access Control	0	4	1	0	0	0	5
Auditing	0	5	1	0	6	0	12
Database Configuration	1	4	0	2	3	3	13
Network Configuration	1	0	0	1	3	0	5
Operating System	1	1	0	2	1	0	5
Total	7	27	4	10	23	5	76

Figure 1. Current Security State Summary of an Oracle Database

DBSAT reports the results of its analysis in the form of a series of Findings. Each Finding provides high level status, risk levels, summary, details, and references as appropriate. It points out if the finding is related to a Center for Internet Security (CIS) benchmark recommendation or related to GDPR Articles/Recitals. The two findings below show which users have the powerful DBA role, and how that role was obtained

(directly granted, granted via another role) and current audit configuration and number of audit records for this particular database.

DBA Role

PRIV.DBA CIS

Status Evaluate

Summary 5 grants of DBA role.

Details

Grants of DBA role:

SCOTT: DBA

OUTSRC_ADM: DBA

SSWADMIN: DBA

DEBRA <- APP_ROLE: DBA

SYSTEM: DBA

Remarks 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.

References CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 4.4.4

Figure 2. Users with Powerful DBA Role

In the example above, DBSAT reports that the user DEBRA got the DBA role indirectly via another role grant (APP_ROLE) while the other users were directly granted the DBA role.

Audit Records

AUDIT.RECORDS CIS GDPR

Status High Risk

Summary Examined 3 audit trails. Found no audit records. No errors found in audit initialization parameters.

Details

Traditional Audit Trail: No records found

FGA Audit Trail: No records found

Unified Audit Trail: No records found

AUDIT_FILE_DEST=/u01/app/oracle/rdbms/audit

AUDIT_SYSLOG_LEVEL is not set.

AUDIT_TRAIL=DB

Remarks Auditing is an essential component for securing any system. The audit trail allows for monitoring the activities of highly privileged users. For any attack that exploits gaps in other security policies, auditing cannot prevent the attack but it forms the critical last line of defense by detecting the malicious activity. Sending audit data to a remote system is recommended in order to prevent any possible tampering with the audit records. The AUDIT_SYSLOG_LEVEL parameter can be set to send an abbreviated version of some audit records to a remote syslog collector. A better solution is to use Oracle Audit Vault and Database Firewall to centrally collect full audit records from multiple databases.

References CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 2.2.2
EU General Data Protection Regulation: Article 30, 33, 34

Figure 3. Auditing Configuration

Findings are provided in multiple formats including HTML, Microsoft Excel, JSON, and text file so that organizations can incorporate this data as part of their configuration and risk management tools.

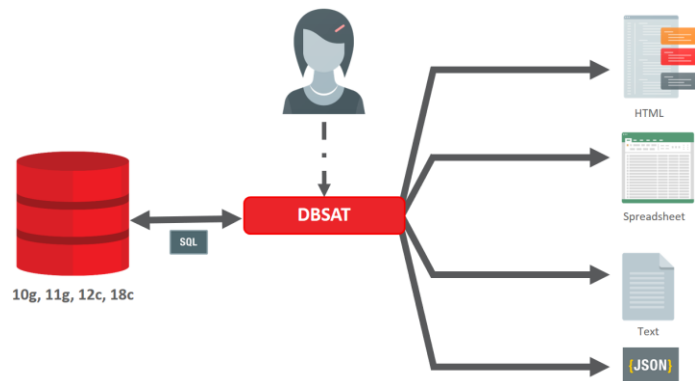


Figure 4. DBSAT Reports

Discover Sensitive Data

Regulations such as the EU GDPR require organizations to protect Personally Identifiable Information (PII) data; however, they first need to know what personal data they have and where.

DBSAT scans the database metadata for sensitive data using customizable regular expression patterns, and reports on the amount and type of sensitive data found. This provides organizations with a deeper insight on how much sensitive data they have and where it resides, enabling them to then protect their databases through appropriate access control, auditing, masking, and encryption. The figure below shows a summary report from a scan of the database metadata.

Sensitive Category	# Sensitive Tables	# Sensitive Columns	# Sensitive Rows
JOB DATA	13	41	476
PII	9	27	699
PII - ADDRESS	12	44	655
PII - IDS	1	2	1
PII - IT DATA	13	13	494
PII-LINKED - BIRTH DETAILS	1	1	7
TOTAL	36*	128	1539**

Figure 5. Sensitive Data Landscape Summary

Summary

Knowing where sensitive data is, and how the database is configured is the foundation for implementing a defense-in-depth strategy. No system is 100% secure but overlooking the basics will only make break-in easier for attackers.

Oracle Database Security Assessment Tool (DBSAT) quickly identifies sensitive data and areas where your database configuration, operation, or implementation introduces risk.


DBSAT is provided at no additional cost to Oracle customers with an active support contract. For more information, or to download DBSAT, visit <http://www.oracle.com/technetwork/database/security/dbsat>




CONTACT US

For more information about Oracle Database Security Assessment Tool, visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

CONNECT WITH US

 blogs.oracle.com/oracle

 facebook.com/oracle

 twitter.com/oracle

 oracle.com

Integrated Cloud Applications & Platform Services

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0118



Oracle is committed to developing practices and products that help protect the environment