

Changes in This Release for Oracle Database Security Assessment Tool

Oracle Database Security Assessment Tool 2.2.2 (June 2021) is a minor release. It has improved accuracy, remarks, and more checks. In this release, DBSAT can differentiate between an on-premises Oracle Database and cloud databases such as Autonomous Databases (Shared and Dedicated) and DBCS. DBSAT performs different checks and provides specific remarks depending on the assessed database target type.

- Amended findings for Autonomous Databases
 - Specific findings for Oracle Databases whether they are on-Premises or in-Cloud - Autonomous Databases or Database Cloud Service.
 - The target type is now taken into consideration for analysis. The checks, details, and remarks presented are specific. More details in the Database Security Assessment Tool User's Guide.
- New checks:
 - `USER.GPR`
This finding provides recommendations for the Gradual Password Rollover feature. It checks if there are user profiles with `PASSWORD_ROLLOVER_TIME` correctly set and if users are using this profile. It details users in the rollover period or that should have the password rollover period expired.
 - `CRYPT.DBFIPS`
Checks if parameter `DBFIPS_140 = TRUE`. This parameter enables Transparent Data Encryption (TDE) and `DBMS_CRYPT` 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.
- Improved checks:

- INFO.PATCH
Now considers Autonomous Databases specifics. For example, customers can skip two patches (up to 150 days) in Autonomous Database Dedicated, while in Autonomous Database Shared they cannot.
- CRYPT.TDE
Now lists how many days have passed since the master encryption key was last rotated.
- CONF.BKUP
Improved accuracy. Checks were also improved to better assess the frequency of backups in Autonomous Databases.
- CONF.DIR
Directory objects that pose a risk are now identified at the top of the details section.
- AUTH.DV
Improved to focus on user created policies, realms, command rules, and protected objects. DBSAT now ignores default Database Vault policies for simplified analysis. Users with granted Database Vault default roles are listed to assess if the correct segregation of duties is in place. Database Vault Operations Control status is also displayed.



Note:

The PDB_DBA role is now included for all checks where the DBA role was previously being considered.

- Adjusted Severity for:
 - INFO.PATCH
 - USER.VERIFIER
 - AUTH.DV
 - ACCESS.REDACT
 - AUDIT.ADMIN, AUDIT.CONN
 - CONF.BKUP
 - NET.CRYPT
 - OS.LISTEN
- Updated remarks and recommendations
 - More detailed and more action oriented.

Downloading and Installing Oracle Database Security Assessment Tool

- To download the Oracle Database Security Assessment Tool, go to [Oracle Technology Network](#), and click the [Download Oracle Database Security Assessment Tool](#) link.
- See *Oracle Database Security Assessment Tool User Guide* for information about completing the installation of Database Security Assessment Tool.

Known Issues

MS Excel Font Size Display

Some versions of Microsoft Excel may display text on the screen using a font that is too large to fit in the spreadsheet cells, even though it is sized correctly in printed output. If this happens, you can resize columns to be slightly wider in order to make the text visible.

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 customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Oracle® Database Security Assessment Tool Release Notes, Release 2.2.2
F22336-07

Copyright © 2015, 2021, Oracle and/or its affiliates

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

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

Intel and Intel Inside 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, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

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.