

Changes in This Release for Oracle Database Security Assessment Tool

Oracle Database Security Assessment Tool 3.1.0 (January 2024) focuses on addressing the Center for Internet Security (CIS) Benchmark v1.2 for Oracle Database 19c recommendations. DBSAT 3.1 adds 10 findings based on CIS recommendations, with updated references, as necessary. There is also a new finding for pre-authenticated URL request details in Autonomous Database Serverless, along with other minor improvements.

- New findings:
 - `USER.DEFAULTPROFILE`
Lists the DEFAULT user profile limits.
 - `PRIV.NETPACKAGEPUBLIC`
Checks for EXECUTE grant on DBMS_LDAP, UTL_HTTP, UTL_INADDR, UTL_SMTP, and UTL_TCP packages to PUBLIC. It also checks, when applicable, for users who are authorized to execute these packages via ACLs.
 - `PRIV.FILESYSTEMPACKAGEPUBLIC`
Checks for EXECUTE grant on DBMS_LOB, UTL_FILE, and DBMS_ADVISOR packages to PUBLIC. It also checks for system privilege grants of CREATE ANY DIRECTORY and DROP ANY DIRECTORY to users.
 - `PRIV.ENCRYPTPACKAGEPUBLIC`
Checks for EXECUTE grant on DBMS_CRYPT, DBMS_OBFUSCATION_TOOLKIT, and DBMS_RANDOM to PUBLIC.
 - `PRIV.JAVAPACKAGEPUBLIC`
Checks for EXECUTE grant on DBMS_JAVA and DBMS_JAVA_TEST packages to PUBLIC. Also, it checks for grants of JAVA_ADMIN role to users.
 - `PRIV.JOBSCHPACKAGEPUBLIC`
Checks for 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.

- PRIV.QUERYPACKAGEPUBLIC
Checks for EXECUTE grant on DBMS_XMLQUERY, DBMS_XMLSAVE, DBMS_XMLSTORE, DBMS_REDACT, DBMS_XMLGEN, and DBMS_SQL packages to PUBLIC.
- PRIV.CREDPACKAGEPUBLIC
Checks for EXECUTE grant on DBMS_CREDENTIAL package to PUBLIC. It also checks for privilege grants of CREATE CREDENTIAL and CREATE ANY CREDENTIAL to users.
- AUDIT.SYNONYMS
Checks if create/alter/drop SYNONYM is audited.
- CONF.DEFAULTPDBOSUSER
Checks for the operating system user defined in PDB_OS_CREDENTIAL.
- CONF.PREAUTHTHREQUESTURL
Displays pre-authenticated URL information for Autonomous Database Serverless databases including who can manage them via the DBMS_DATA_ACCESS package.
- Improved findings:
 - USER.NOEXPIRE
Improved logic and summary.
 - USER.APPOWNER
Optimizations to improve performance and reduce the level of detail.
 - ENCRYPT.TDE
Updated remarks to clarify the usage of the TABLESPACE_ENCRYPTION parameter and recommendations when upgrading to Oracle Database 23c and you are using a de-supported algorithm.

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 3.1.0 F2Z336-10

Copyright © 2015, 2024, 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, software documentation, data (as defined in the Federal Acquisition Regulation), 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," "commercial computer software documentation," or "limited rights data" 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®, Java, MySQL and NetSuite 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.