Oracle® Database

Security Assessment Tool User Guide

Release 1.0.2

E72220-03

October 2016

Overview

The Oracle Database Security Assessment Tool (DBSAT) analyzes database configurations and security policies to uncover security risks and improve the security posture of Oracle Databases within your organization.

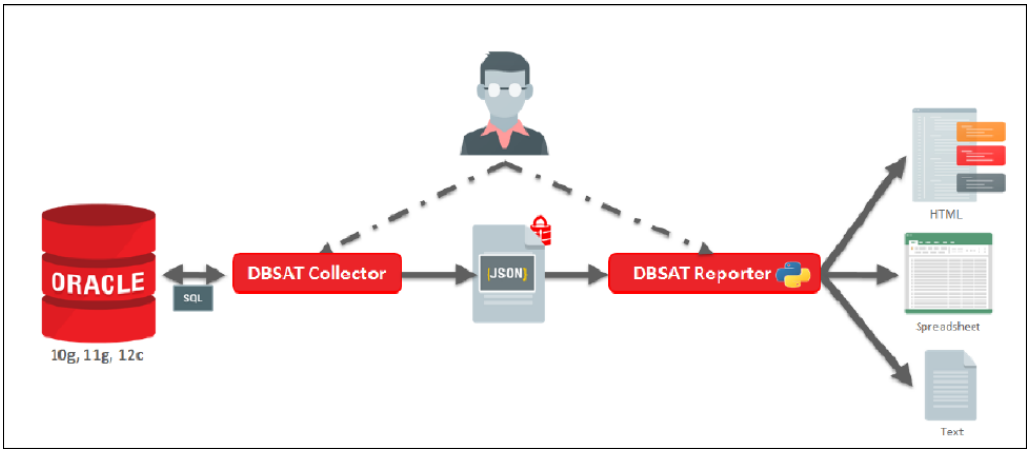
You can use DBSAT to implement and enforce security best practices in your organization. DBSAT reports on the state of user accounts, role and privilege grants, and policies that control the use of various security features in the database.

You can use report findings to:

- Fix immediate short-term risks
- Implement a comprehensive security strategy

Components of DBSAT

DBSAT Components and Flow



DBSAT consists of two components, the DBSAT Collector and the DBSAT Reporter that correspond to the functions of data collection and data analysis respectively:

1. The **DBSAT 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 file that is used by the DBSAT Reporter in the analysis phase.

2. The **DBSAT Reporter** analyzes the collected data and reports its findings and recommendations in multiple formats: PDF, Excel, and Text. The Reporter can run on any machine: PC, laptop, or server. You are not limited to running it on the same server as the Collector.

Benefits of Using DBSAT

You can use DBSAT to:

- Quickly identify security configuration errors in your databases
- Promote security best practices
- Improve the security posture of your Oracle Databases
- Reduce the attack surface and exposure to risk

Installation Requirements

You must meet certain system and target database platform requirements to install and use DBSAT successfully.

The following sections outline system requirements, supported target database platforms, database versions, and target database requirements.

System Requirements

The DBSAT Reporter is a platform-independent Python program and requires Python 2.6 or later to run.

Both the DBSAT Collector and Reporter use Zip and Unzip utilities already installed on the system to encrypt the generated files. The DBSAT tool expects to find these utilities in the locations shown below. If the utilities are somewhere else on your system, you must update these lines in the appropriate script.

Windows (dbsat.bat script):

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

All other platforms (dbsat script):

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

Supported OS Platforms

The database configuration collection queries run on most supported Oracle Database platforms. However, currently the OS data collection will be skipped on Windows platforms. The list of skipped rules such as OS file permissions can be found at the end of the Text and HTML report.

DBSAT runs on:

- Solaris x64 and Solaris SPARC
- Linux x86-64

- Windows x64
- HP-UX IA (64-bit)
- IBM AIX & zSeries Based Linux

Supported Database Versions

You can run the DBSAT tool on Oracle Database 10.2.0.5 and later releases.

Data is collected by running SQL queries and operating system commands. 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.

Requirements to Run the DBSAT Collector

In order to collect complete data, the DBSAT Collector must be run on a server that contains the database, because it executes some operating system commands to collect process and file system information that cannot be obtained from the database. In addition, the DBSAT Collector must be run as an OS user with read permissions on files and directories under `ORACLE_HOME` in order to collect and process file system data using OS commands.

The 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. You can grant the DBSAT user the individual privileges in the following list, or you can grant this user the DBA role plus the `DV_SECANALYST` role if needed.

Required privileges and roles:

- `CREATE SESSION`
- `SELECT` on `SYS.REGISTRY$HISTORY`
- Role `SELECT_CATALOG_ROLE`
- Role `DV_SECANALYST` (if Database Vault is enabled)
- Role `AUDIT_VIEWER` (12*c* only)
- Role `CAPTURE_ADMIN` (12*c* only)
- `SELECT` on `SYS.DBA_USERS_WITH_DEFPWD` (11*g* and 12*c*)
- `SELECT` on `AUDSYS.AUD$UNIFIED` (12*c* only)

Note: In order to successfully collect Database Vault information in a Database Vault environment, you must connect as a non-SYS user with the DV_SECANALYST role.

Security Considerations

Security Guidelines

The output files from the DBSAT Collector and the DBSAT Reporter 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 on a short-term basis and revoke these when no longer necessary.

System Impact While Running DBSAT

DBSAT is a light weight utility that will not impair system performance in a measurable way.

Caution

This tool is intended to assist in you in identifying potential vulnerabilities in your system, but 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.

Installing and Running the Oracle Database Security Assessment Tool

To analyze a database using the Oracle Database Security Assessment Tool (DBSAT) you must first install it, then run the Collector and the Reporter in that order.

You can get DBSAT reports in three steps:

1. Task 1: Install the Database Security Assessment Tool (page 4)
2. Task 2: Run the DBSAT Collector (page 5)
3. Task 3: Run the DBSAT Reporter (page 6)

Task 1: Install the Database Security Assessment Tool

The Oracle Database Security Assessment Tool (DBSAT) installation is a simple process. Simply extract the file `dbsat.zip` on the Target Database server.

To install the Database Security Assessment Tool:

1. Create a directory on the target system where you can extract the DBSAT file.

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

2. Extract the DBSAT file to the directory.

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

Where `-d` refers to the directory path.

3. Navigate to the directory.

```
cd /home/oracle/dbsat
```

You can now run the DBSAT Collector and DBSAT Reporter scripts from here. You can add this directory to your `PATH` and skip the step of going to the directory every time you want to run the tool.

Task 2: Run the DBSAT Collector

The DBSAT Collector queries the database to collect data for further analysis.

You can invoke the DBSAT Collector with the `dbsat collect` script . You must ensure that the target database and listener are running before executing this step. The DBSAT Collector first connects to the database, then collects the data in a file.

1. Run the DBSAT Collector:

```
$ dbsat collect <connect_string> <destination>
```

Where:

`connect_string` refers to the database user's credentials to connect to the database with the appropriate privileges, for example: `system/manager`. If `connect_string` contains spaces, you must enclose it within quotes.

`destination` refers to the full path including the file name, for example: `/home/oracle/dbsat/db04`.

The file with basename `db04` is created by the DBSAT Collector.

The following output appears:

```
Connecting to the target Oracle database...
SQL*Plus: Release 12.1.0.2.0 Production on Mon Feb 22 06:50:46 2016
Copyright (c) 1982, 2014, Oracle.  All rights reserved.
Enter password: <input user password>
Last Successful login time: Mon Feb 22 2016 06:50:15 -08:00

Connected to:
Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production

This tool is intended to assist in you in identifying potential
vulnerabilities in your system, but 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.

Setup complete.
SQL queries complete.
OS commands complete.
```

```
Disconnected from Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 -
64bit Production

DBSAT Collector completed successfully.
Calling /u01/app/oracle/product/12.1/db_1/bin/zip to encrypt db04.json...
Enter password: <input password to encrypt collected data file, here db04>
Verify password: <input password>
    adding: db04.json (deflated 88%)
zip completed successfully.
[oracle@db04 sat]$
```

If you do not want to encrypt the file invoke the `dbsat collect` script with the `-n` option. This is not recommended.

Note that running the DBSAT 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 DBSAT Collector for these pluggable databases separately.

Task 3: Run the DBSAT Reporter

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

You can invoke the DBSAT Reporter with the `dbsat report` script.

To generate a DBSAT report follow these steps:

1. Check that the Python version is 2.6 or later.

   ```
   [oracle@db04 sat]$ python -V
   ```

   The following output appears:

   ```
   Python 2.7.11rc1
   ```

2. Run the DBSAT Reporter.

   ```
   [oracle@db04 sat]$ dbsat report [-a] [-n] [-x <section>]
   <pathname>
   ```

   Where the argument `pathname` stands for the full or relative path name to the data file `db04` 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 DBSAT Reporter.

   The DBSAT Reporter supports the following command-line options:

   - `-a` means: include all the database user accounts in the analysis. (Locked Oracle-supplied accounts are excluded by default as they cannot be used to connect to the database.)
   - `-n` means: do not encrypt the reports generated by the analysis.
   - `-x` means: exclude a section from the report. Valid sections are:
     - `USER` : **User Accounts**

- PRIV : **Privileges and Roles**
- AUTH : **Authorization Control**
- CRYPT : **Data 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 Excel, HTML, and Text formats with the appropriate file extensions.

3. Run the DBSAT Reporter.

```
[oracle@db04 sat]$ ./dbsat report db04
```

The following output appears:

```
Archive:  db04.zip
[db04_collection.zip] db04.json password:
     inflating: ./db04.json

DBSAT Reporter ran successfully.
Calling /usr/bin/zip to encrypt the generated reports...
Enter password: <input password for report files>
Verify password: <input password for report files>
   adding: db04.txt (deflated 84%)
   adding: db04.html (deflated 85%)
   adding: db04.xlsx (deflated 3%)

zip completed successfully.
```

The DBSAT Reporter creates an encrypted file `db04_report.zip` at the end of a successful run.

4. Unzip the Report file

```
[oracle@db04 sat]$ unzip db04_report.zip
```

The following output appears:

```
Archive:  db04_report.zip
[db04_report.zip] db04.txt password: <input report password>
  inflating: db04.txt
```

```
inflating: db04.html
inflating: db04.xlsx
```

The three report files are created at the end of a successful run.

DBSAT Reports

DBSAT produces output in multiple formats for various audiences and purposes.

The HTML report provides detailed results of the assessment 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 usage.

The following figure displays the first three tables of a DBSAT summary.

High-Level DBSAT Summary

Assessment Date & Time

Date of Data Collection	Date of Report	Reporter Version
Wed May 18 2016 16:20:00	Fri May 20 2016 10:43:21	1.0 (May 2016) - 1c0a

Database Identity

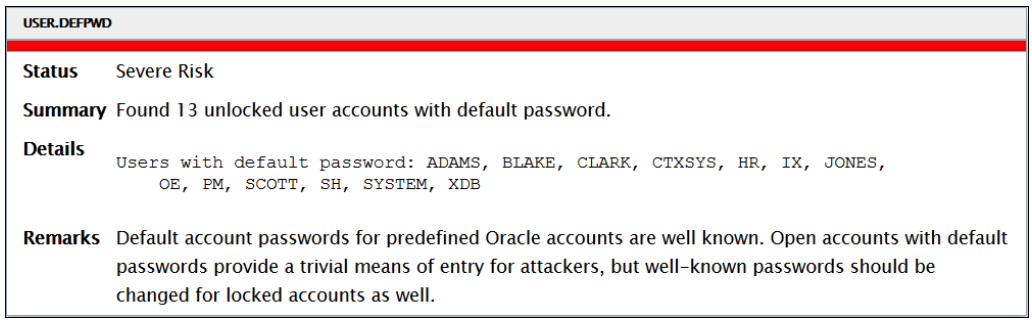
Name	Platform	Database Role	Log Mode	Created
DB	Linux x86 64-bit	PRIMARY	NOARCHIVELOG	Wed Feb 03 2016 09:40:00

Summary

Section	Pass	Evaluate	Opportunity	Some Risk	Significant Risk	Severe Risk	Total Findings
Basic Information	0	0	0	0	0	1	1
User Accounts	4	0	0	3	3	1	11
Privileges and Roles	5	11	0	1	0	0	17
Authorization Control	0	0	2	0	0	0	2
Data Encryption	0	1	1	0	0	0	2
Fine-Grained Access Control	0	0	5	0	0	0	5
Auditing	2	4	2	0	3	0	11
Database Configuration	5	4	0	3	0	0	12
Network Configuration	1	0	0	1	3	0	5
Operating System	3	1	0	0	1	0	5
Total	**20**	**21**	**10**	**8**	**10**	**2**	**71**

The resulting analysis is reported in units called Findings. An example follows:

DBSAT Finding — Users with Default Password



Each Finding consists of the following components:

- **Title and Unique ID for the Rule**

  The ID has two parts: the prefix identifies the report section, and the suffix identifies the specific rule.

- **Status**

  You can use the status values as guidelines to implementing DBSAT recommendations. They can be used to prioritize and schedule changes based on the level of risk, and what it might mean to your organization. Severe risk might require immediate remedial action, whereas other risks might be fixed during a scheduled downtime, or bundled together with other maintenance activities.

  - Pass: no error found
  - Evaluate: needs manual analysis
  - Some Risk: low
  - Significant Risk: medium
  - Severe Risk: high
  - Opportunity: improve security posture by enabling additional security features and technology

- **Summary**

  This is a one-line summary of the finding. When the finding is informational, the summary typically reports only the number of data elements that were examined.

- **Details**

  This provides detailed information to explain the finding summary, typically results from the assessed database, followed by any recommendations for changes.

- **Remarks**

  This explains the standard used to assess the results found. It may also explain the recommended actions for remediation if a risk is reported.

Sample Script to Create a User with Minimum Privileges

You can create a user with required minimum privileges to run the 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$history to dbsat_user;
grant select on sys.dba_users_with_defpwd to dbsat_user; // 11g and 12c
grant select on audsys.aud$unified to dbsat_user; // 12c only
grant audit_viewer to dbsat_user; // 12c
grant capture_admin to dbsat_user;// 12c 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;
```

Known Issues

1. 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.

Attribution for Third-Party Licenses

Third-party licenses used in the Database Security Assessment Tool Release 1.0.

About 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: 0.7.7

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.