ORACLE

Oracle Database Security Assessment Tool FAQ

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 challenging 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.

GENERAL

What are the primary use cases for the Oracle Database Security Assessment Tool (DBSAT)?

There are three core use cases. Assessing how securely the database is configured, determining who the users and their entitlements are, and identifying where sensitive data resides within the database.

How does DBSAT work?

DBSAT has three components: Collector, Reporter, and Discoverer. The Collector collects all relevant data from the database that the Reporter then analyzes and generates a *Security Assessment* report. The Discoverer is a stand-alone module that identifies different types of sensitive data in the database and generates a *Sensitive Data Assessment Report*.

What type of data is collected and analyzed?

DBSAT collects and reports on the following categories of data:

- User accounts, privileges, and roles
- Authorization Control
- Fine-grained Access Control
- Auditing Policies
- Data Encryption
- Database Configuration
- Listener Configuration
- Related Operating System Configuration

To discover the type and quantity of sensitive data in the database, DBSAT Discoverer does pattern matching on column names and column comments. It categorizes sensitive data as follows:

- Identification Information

- Biographic Information
- IT Information
- Financial Information
- Health Information
- Job Information
- Academic Information

What is the performance impact of running DBSAT?

The performance impact on the database is negligible. DBSAT Collector and Discoverer gather data only from the database configuration files and Oracle data dictionary views. It does not look at the application data.

How much time does it take to learn how to run DBSAT and analyze the data?

DBSAT itself is a straightforward command-line tool to use. It takes a few minutes to learn how to run the tool. You could go from Install to Reports in as little time as 10 minutes.

Can I run DBSAT on my databases that are deployed in the Cloud?

DBSAT can be used whether your database is running on-premises, in Autonomous Databases, customer-managed Database Cloud Services (DBCS), or IaaS deployed databases. Other prerequisites apply. Please refer to the documentation.

Can I run it on Autonomous Databases?

Yes. DBSAT is certified for Autonomous Data Warehouse Cloud (ADW) and Autonomous Transaction Processing (ATP) databases.

Will DBSAT provide me with different recommendations depending on the database type?

Yes. DBSAT starts by identifying the target type and performs specific checks whether your databases are running on-premises or in-cloud. Currently, DBSAT differentiates between on-premises databases, Autonomous Database Shared, Autonomous Database Dedicated, and DBCS. For these target types, and when applicable, DBSAT provides specific recommendations.

DBSAT COLLECTOR AND REPORTER

How do I run the DBSAT Collector?

The Collector is invoked against an Oracle Database:

```
$ dbsat collect <connect_string> <dest-file>
```

`connect_string` is the connection string for the target database.

`dest-file` is the name of the output file created by the Collector, without the extension suffix.

Here is an example of the command:

```
$ dbsat collect dbsatusr@orcl dbdata
```

As the DBSAT Collector analyzes both database and operating system configuration, it is recommended that you run the DBSAT Collector from the same host where the

database server is running. Some checks are skipped (e.g., Operating System) when executed remotely.

To get the reports, you need to run the DBSAT reporter (described below).

How do I run the DBSAT Reporter?

The DBSAT Reporter can be run on any system, including a desktop/laptop with Python 2.6 or later.

```
$ dbsat report <dest-file>
```

The `dest-file` is the JSON/zip file name produced by the Collector (without the file extension). The same pathname is used as the base for all report files created by the DBSAT Reporter, with appropriate suffixes added for the Text, HTML, JSON, and XLS report formats. For example,

```
$ dbsat report dbdata
```

What is a Finding?

The output of the DBSAT Reporter creates a *Database Security Assessment Report* composed of multiple Findings. Each finding includes suggestions to improve the database security posture or provide information for further analysis. When appropriate, findings also include a reference to the applicable portion of the Oracle Database STIG rules, CIS benchmark recommendations, or to EU GDPR articles/recitals.

Is it possible to extract only Findings, compare different reports, or create an aggregated report from multiple databases?

DBSAT Reporter provides the report in JSON format to make further processing of Findings possible.

You can also download and leverage DBSAT utils for further processing. DBSAT utils are two sample python programs that can extract a finding and help you compare two JSON reports. DBSAT utils can be downloaded from My Oracle Support.

Alternately, you may also want to consider Oracle Data Safe. Data Safe is a database security cloud service that provides a comprehensive suite of security capabilities, including user and security assessments. Tightly integrated assessment capabilities provide the ability to simultaneously run assessments on multiple databases, schedule assessments, establish a security baseline, and get a comparison report that highlights the drift between that baseline and the current database security assessment. To learn more about Oracle Data Safe, please visit https://www.oracle.com/security/database-security/data-safe/.

Can I run DBSAT Collector on a multitenant pluggable database?

Yes, however, DBSAT needs to be executed for the root container and each PDB separately.

Can I add my custom assessment rules?

DBSAT design center was a quick, easy-to-use tool that addresses the most common issues. DBSAT ships with Oracle Database Security best practices rules and, where applicable, highlights Oracle Database STIG Rules, CIS Benchmark recommendations,

and related EU GDPR articles/recitals. We plan to review all requests for enhancements and consider them for a future release.

DBSAT DISCOVERER

How does DBSAT Discoverer work?

DBSAT Discoverer uses a configuration file, one or more pattern files describing sensitive data types, and regular expressions to search column names and column comments.

e.g., To search for “First Name”, we could use

```
[FIRST NAME]
COL_NAME_PATTERN = (^|[_-])(FNAME|(FIRST|GIVEN).*(NAME|NM)|FORE.?(NAME|NM))($|[_-])
COL_COMMENT_PATTERN = (FIRST|GIVEN) NAME|FORENAME
SENSITIVE_CATEGORY = Identification Info - Public IDs
```

DBSAT comes with the initial configuration and pattern file, but customers can add custom sensitive types and categories/subcategories.

What types of Regular expressions are used?

DBSAT Discoverer supports Extended Regular Expressions (ERE). This syntax is standardized by IEEE and is commonly used in Java.

For example, `(^JOB.*(TITLE|PROFILE|POSITION)$)|^POSITION` matches a string that starts with JOB (^JOB), followed by zero or more occurrences (*) of any character (.), and ends in ($) TITLE or PROFILE or POSITION. Or (|), it matches a string that starts (^) with POSITION.

How accurate are the pattern matching rules? How does one deal with false positives?

The rules provided with DBSAT were created to reduce false positives. However, as DBSAT examines only the column names and column comments, it might generate false positives. One way to reduce false positives is to edit the pattern file and tune the regular expression for your application; another is to exclude schemas, tables, and columns from the search using an exclusion list file. As the CSV report includes a fully qualified name for the column (Schema.Table.Column), you easily exclude false positives by just copy/pasting from the CSV report to the exclusion list file.

Can DBSAT find sensitive data if my data model is in other languages besides English?

Along with a pattern file that searches English-based column names and comments. DBSAT also includes additional pattern files for Dutch, French, German, Italian, Portuguese, and Spanish.

Can I add my custom sensitive type or category in the DBSAT Discoverer?

Yes, you can. Make a copy of the pattern file and add your sensitive type, category, and the regular expressions to search column names and comments. You also need to add the new category along with the risk level to the configuration file.

How do I run the DBSAT Discoverer?

DBSAT Discoverer can be run on any machine including a laptop with Java Runtime Environment (JRE) 1.8 (jdk8-u172) or later. There is no need to run Discoverer on the same server as the database server.

```
$ dbsat discover –c <config file> <dest-file>
```

e.g., `$ dbsat discover –c Discoverer/conf/dbsat.config dbdata`

Do I need to run the DBSAT Collector before running DBSAT Discoverer?

No. DBSAT Discoverer is a standalone component. There is no dependency on the DBSAT Collector or the Reporter.

SECURITY CONSIDERATIONS

What privileges are required for the user account connecting to the database to collect data?

While a database user account with the Oracle provided DBA role has the necessary privileges, the principle of least privileges should be followed. Please refer to the documentation for the minimum privileges needed to run DBSAT. In addition, the OS user executing DBSAT Collector must have permission to read the ORACLE_HOME directory and files.

How does DBSAT protect the collected configuration data and generated reports?

By default, DBSAT output files are compressed and password protected using installed zip/unzip. We strongly recommend that all output files always be encrypted as it has sensitive information about your database.

What are the security risks of running DBSAT on production databases?

The risk is minimal as DBSAT only reads configuration and metadata. All database actions performed by DBSAT are read-only.

DBSAT can be run with least privileges to collect the data it needs for analysis. The DBSAT Collector SQL script that collects data can be reviewed to see what operations are executed. The DBSAT Collector output data (in JSON format) can also be examined to see exactly what data is collected. Access to DBSAT generated reports should be restricted.

DOWNLOAD AND INSTALLATION

Where can I download the Oracle DBSAT?

DBSAT can be downloaded from My Oracle Support under Doc ID 2138254.1.

How do I install DBSAT?

DBSAT is provided as a zip file. Just unzip it.

```
$ unzip dbsat.zip –d <directory>
```

Which Database versions are supported?

DBSAT supports Oracle Database 11.2.0.4 and later releases up to 21c.

Which platforms are supported?

DBSAT runs on:

- Solaris x64 and Solaris SPARC
- Linux x86-64
- Windows x64
- HP-UX IA (64-bit)
- IBM AIX & zSeries Based Linux

DBSAT runs on most supported Oracle Database platforms. However, currently, DBSAT Collector does not collect OS data from database servers running on the Windows platforms or if executed remotely. In Unix/Linux systems it requires bash shell.

Can Oracle Sales Consulting (SC), Oracle Consulting Services (OCS), or Advanced Customer Services (ACS) download DBSAT and run it for me?

We recommend that you download and run DBSAT yourself. Oracle consultants are available to help you execute a Database Security Assessment program, analyze the data, and prioritize remediation steps taking into context your organization's environment. In addition, Oracle consultants can give you a better insight into your database security posture through an onsite interview that complements the DBSAT reports. A proper security assessment considers your organizational specifics, broader IT system, processes in place, and regulations that need to be addressed.

PRODUCT LICENSING AND SUPPORT

How is DBSAT distributed?

The tool is available at no additional cost for download by Oracle customers with a My Oracle Support (MOS) account.

How can I report bugs or request enhancements for DBSAT?

Please submit a service request (SR) for DBSAT via the MOS portal.

Where do I go to get the bug fixes for DBSAT?

We plan to make quarterly updates to DBSAT that would include enhancements as well as bug fixes. Therefore, we strongly recommend that you always check for the latest release.

How is DBSAT related to Data Safe?

Data Safe is a database security cloud service that provides a comprehensive suite of security capabilities. These capabilities include Security Assessment, User Assessment, Activity Monitoring, Sensitive Data Discovery, and Data Masking and work for databases running in-cloud or on-premises.

DBSAT is excellent for assessing the current security state of few databases. Data Safe builds on it and addresses enterprise-level requirements. With Data Safe, you'll be able to:

- Execute periodic scheduled assessments
- Set a database security baseline
- See a comparison report with the drift against the baseline
- See the history of all assessment runs
- Get insight into user risks via the User Assessment feature
- Address your company or regulatory requirements that require anonymizing data in non-production environments, monitor database activity, assess your database security posture, and discover sensitive data in a single unified console

To learn more about Oracle Data Safe, please visit https://www.oracle.com/security/database-security/data-safe/.

MORE INFORMATION

Where can I find more information on DBSAT?

Go to the DBSAT oracle.com page.

Where do I go for more details on the Database Security Assessment program?

Multiple Oracle teams across the globe have created their Database Security Assessment programs. Please talk to your Oracle Account Manager for assistance.

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

blogs.oracle.com facebook.com/oracle twitter.com/oracle