



# PEOUG

PERU ORACLE USERS GROUP



## **Database Security: ¿Cómo identificar áreas de riesgo y vulnerabilidades de seguridad? Mitíguelos**

**28 de Agosto 2019**

**Miguel Palacios**

**Oracle ACE Database & Performance**

# LAOUC.ORG



[www.peoug.org](http://www.peoug.org)

¿Continuidad?



¿Moda?

¿Necesidad?

¿Cumplimiento?

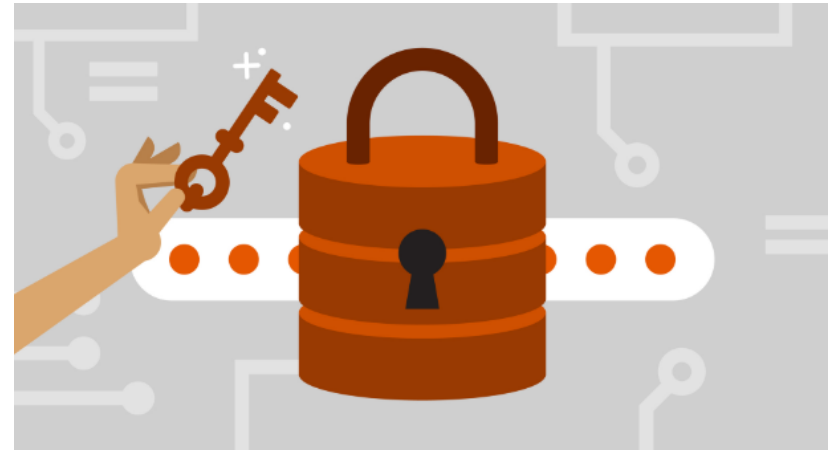
¿CyberSeguridad?

¿Transformación Digital?

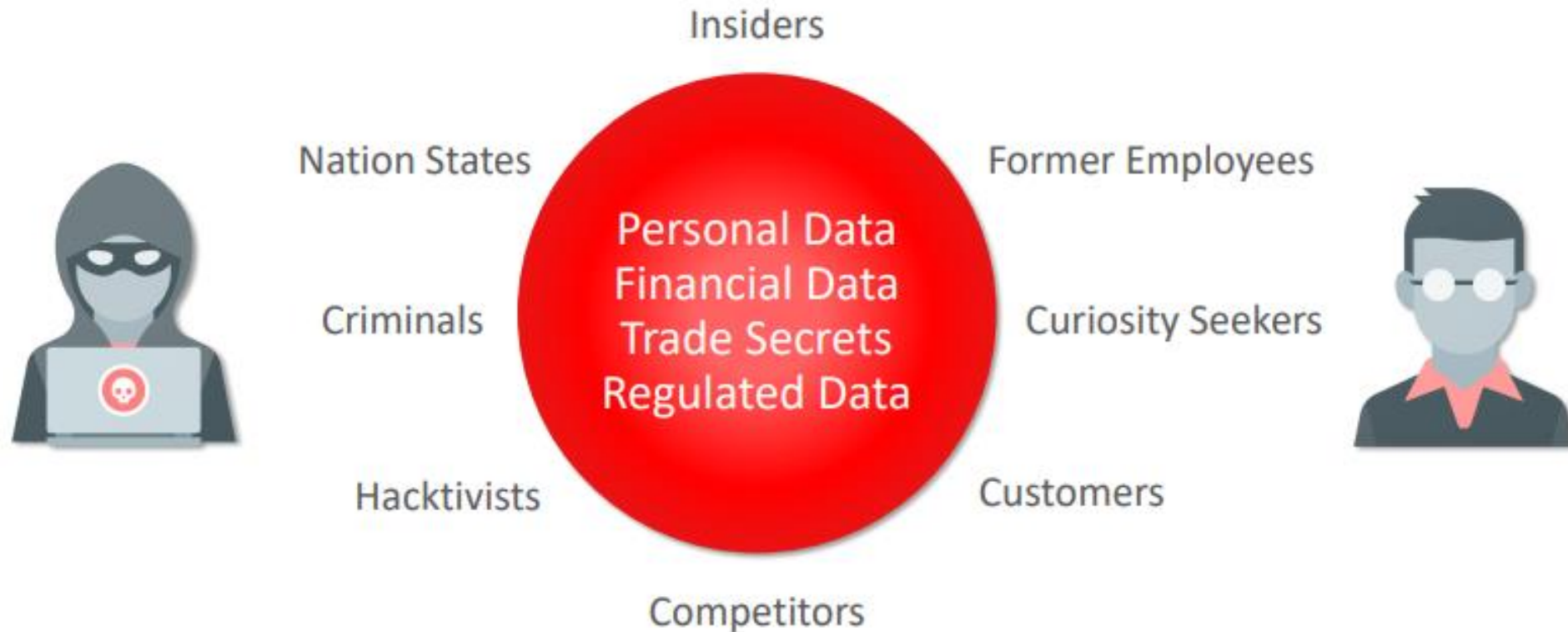
**¿Qué opina?**

# Premisas

1. Las bases de datos siguen siendo atractivas para hackers o usos mal intencionados. Es un activo muy valioso
2. Necesidad de Cumplimiento regulatorio internacional y nacional (EU GDPR, PCI DSS, SOX, HIPAA/HITECH, LDPD, NTP, etc.)
3. Orientación y enfoque preventivo de seguridad



# ¿Quién quiere nuestra data?





# ¿Sabe cómo han evolucionado las técnicas de ataques?



# ¿Quiénes pueden vulnerar?



# ¿Por dónde empezamos y qué buscar?



1. ¿Dónde residen los datos sensibles?
2. ¿Quiénes son los usuarios y sus derechos?
3. ¿Qué controles he aplicado in situ?
4. ¿Mi base de datos está configurada de forma segura?
5. ¿Tenemos un equipo de seguridad de base de datos?
6. ¿Tengo conocimiento en seguridad?
7. ¿Tengo tiempo para análisis regularmente?



# Oracle Database Security Assessment Tool (DBSAT)

## 1. Configuración de seguridad

- Cifrado de datos
- Políticas de auditoría
- Control de acceso de granular
- Configuración de base de datos y escucha
- Permisos de archivos OS
- Parches de seguridad

## 2. Usuarios y derechos

- Cuentas de usuario, privilegios y roles

## 3. Datos sensibles

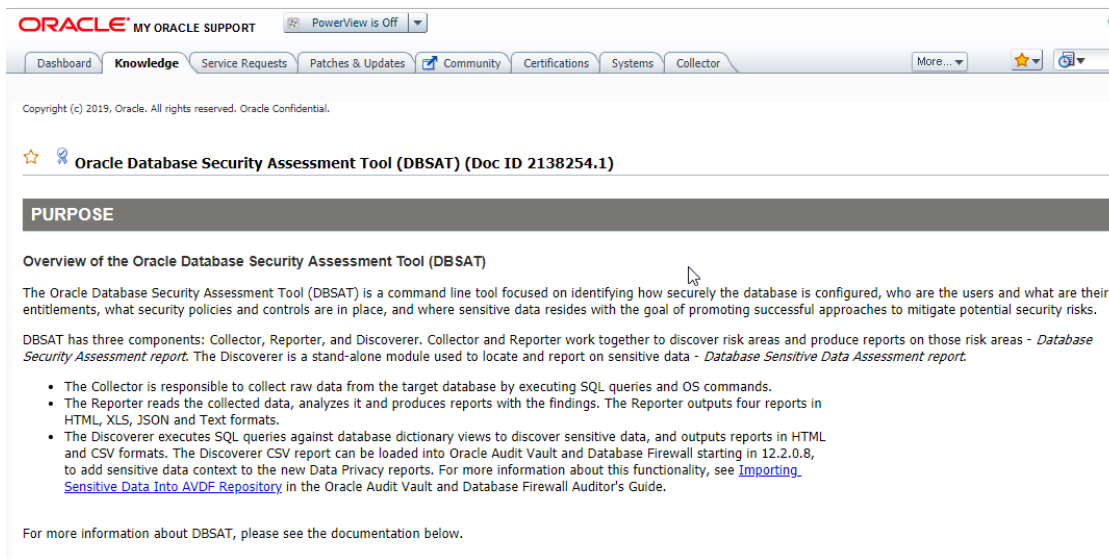
- ¿Qué tipo?, ¿dónde?, ¿cuántos?



For Oracle Databases  
10g and later

# Descarga de Database Assessment Tool - DBSAT

Ingresar al portal de My Oracle Support con sus credenciales e ingresar a la nota técnica de referencia **Oracle Database Security Assessment Tool (DBSAT) (Doc ID 2138254.1)**



ORACLE MY ORACLE SUPPORT PowerView is Off

Dashboard Knowledge Service Requests Patches & Updates Community Certifications Systems Collector More...

Copyright (c) 2019, Oracle. All rights reserved. Oracle Confidential.

Oracle Database Security Assessment Tool (DBSAT) (Doc ID 2138254.1)

### PURPOSE

#### Overview of the Oracle Database Security Assessment Tool (DBSAT)

The Oracle Database Security Assessment Tool (DBSAT) is a command line tool focused on identifying how securely the database is configured, who are the users and what are their entitlements, what security policies and controls are in place, and where sensitive data resides with the goal of promoting successful approaches to mitigate potential security risks.

DBSAT has three components: Collector, Reporter, and Discoverer. Collector and Reporter work together to discover risk areas and produce reports on those risk areas - *Database Security Assessment report*. The Discoverer is a stand-alone module used to locate and report on sensitive data - *Database Sensitive Data Assessment report*.

- The Collector is responsible to collect raw data from the target database by executing SQL queries and OS commands.
- The Reporter reads the collected data, analyzes it and produces reports with the findings. The Reporter outputs four reports in HTML, XLS, JSON and Text formats.
- The Discoverer executes SQL queries against database dictionary views to discover sensitive data, and outputs reports in HTML and CSV formats. The Discoverer CSV report can be loaded into Oracle Audit Vault and Database Firewall starting in 12.2.0.8, to add sensitive data context to the new Data Privacy reports. For more information about this functionality, see [Importing Sensitive Data Into AVDF Repository](#) in the Oracle Audit Vault and Database Firewall Auditor's Guide.

For more information about DBSAT, please see the documentation below.

Validar la última versión actualizada

### INTEGRITY CHECK

#### DBSAT zip file integrity

To make sure that the content is transferred correctly and has not been corrupted, the SHA256 checksum of the downloaded dbsat.zip file matches the value in the table below.

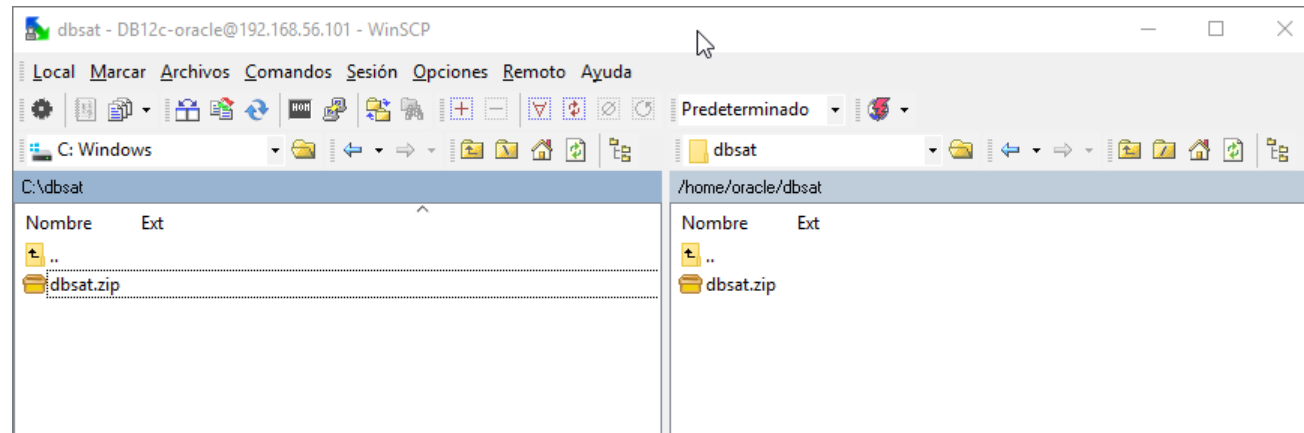
DBSAT Release	SHA256 checksum
2.1.0 (March 2019)	ddd071ada201c8ea6dda4257d6ff9bd49
2.0.2 (May 2018)	54f33fe1a5a8aeb2d2dfd39542e77a4f33
2.0.1 (December 2017)	a485cfbf14ac9ffc70cd0f0a8c101055b2
1.0.2 (October 2016)	cca0d9fa7d446d837472e2321310a6b33
1.0.1 (June 2016)	0ea517275102742e4b98679ff54e6ec31

# Transferir la herramienta dbSAT al servidor

Iniciar sesión en el servidor con cuenta **oracle** a través del **WinSCP**

Crear el directorio **dbSAT**

Transferir el utilitario **dbSAT** en el directorio creado.



# Validar el archivo transferido y descomprimir

Iniciar sesión vía putty e ingresar al directorio donde se aloja el archivo dbsat.zip

Descomprimir mediante el comando **unzip dbsat.zip**

```
[oracle@srv1 dbsat]$ ls -l
total 4580
-rw-r--r--. 1 oracle oinstall 4686487 Aug 27 08:32 dbsat.zip
[oracle@srv1 dbsat]$ pwd
/home/oracle/dbsat
[oracle@srv1 dbsat]$ unzip dbsat.zip
Archive:  dbsat.zip
  inflating:  dbsat
  inflating:  dbsat.bat
  inflating:  sat_reporter.py
  inflating:  sat_analysis.py
  inflating:  sat_collector.sql
  inflating:  xlsxwriter/app.py
  inflating:  xlsxwriter/chart_area.py
  inflating:  xlsxwriter/chart_bar.py
  inflating:  xlsxwriter/chart_column.py
  inflating:  xlsxwriter/chart_doughnut.py
  inflating:  xlsxwriter/chart_line.py
  inflating:  xlsxwriter/chart_pie.py
  inflating:  xlsxwriter/chart.py
  inflating:  xlsxwriter/chart_radar.py
  inflating:  xlsxwriter/chart_scatter.py
  inflating:  xlsxwriter/chartsheet.py
  inflating:  xlsxwriter/chart_stock.py
  inflating:  xlsxwriter/comments.py
  inflating:  xlsxwriter/compat_collections.py
  inflating:  xlsxwriter/compatibility.py
  inflating:  xlsxwriter/contenttypes.py
  inflating:  xlsxwriter/core.py
  inflating:  xlsxwriter/custom.py
  inflating:  xlsxwriter/drawing.py
```

# Creación de usuario de Base de Datos DBSAT

Se debe crear un nuevo usuario con nombre DBSAT (Nombre sugerido) y asignarle los siguientes privilegios.

Caso contrario la herramienta puede ser ejecutada con cuentas que tengan el privilegio DBA. (system, sys)

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 (12c only)
- » Role CAPTURE\_ADMIN (12c only)
- » SELECT on SYS.DBA\_USERS\_WITH\_DEFPWD (11g and 12c)
- » SELECT on AUDSYS.AUD\$UNIFIED (12c only)

In this Lab, we will be running DBSAT with the oracle OS user and will create a database user with the privileges that are strictly needed for its execution.

1. As system, in the orcl PDB, execute:

```
grant create session to dbsat identified by oracle;
grant select on sys.registry$history to dbsat;
grant select_catalog_role to dbsat;
grant audit_viewer to dbsat;
grant capture_admin to dbsat;
grant select on sys.dba_users_with_defpwd to dbsat;
grant select on audsys.aud$unified to dbsat;
```

As the output, you should get:



# Ejecución de la herramienta DBSAT

## - Módulo collect

Ingresar a la carpeta de dbsat y ejecutar  
**./dbsat collect system /home/oracle/dbsat/oradb**

Ingresar el password del system:  
password: \*\*\*\*\*

Generamos un password para la  
matriz de reporte  
password: \*\*\*\*\*  
password: \*\*\*\*\*

Se generará un archivo  
similar a **oradb.zip**

```
oracle@srv1:~/dbsat
[oracle@srv1 dbsat]$ ./dbsat collect system /home/oracle/dbsat/oradb

Database Security Assessment Tool version 2.1 (March 2019)

This tool is intended to assist in you in securing your Oracle database
system. 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.

Connecting to the target Oracle database...

SQL*Plus: Release 12.1.0.2.0 Production on Tue Aug 27 08:53:43 2019

Copyright (c) 1982, 2014, Oracle. All rights reserved.

Enter password:
Last Successful login time: Tue Aug 27 2019 08:47:47 -05:00

Connected to:
Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production
With the Partitioning, Automatic Storage Management, OLAP, Advanced Analytics
and Real Application Testing options

Setup complete.
SQL queries complete.
OS commands complete.
Disconnected from Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production
With the Partitioning, Automatic Storage Management, OLAP, Advanced Analytics
and Real Application Testing options
DBSAT Collector completed successfully.

Calling /u01/app/oracle/product/12.1.0/db_1/bin/zip to encrypt oradb.json...

Enter password:
Verify password:
adding: oradb.json (deflated 87%)
zip completed successfully.
```

# Generación de reportes

Ejecutar el siguiente comando  
**./dbsat report oradb**

Solicitará el password asignado anteriormente

Por último se observa que se generan los siguientes archivos:

**oradb\_report.txt**  
**oradb\_report.html**  
**oradb\_report.xlsx**  
**oradb\_report.json**

Y se agrupan en el archivo comprimido

**oradb\_report.zip**

```
[oracle@srv1 dbsat]$ ./dbsat report oradb
Database Security Assessment Tool version 2.1 (March 2019)

This tool is intended to assist in you in securing your Oracle database
system. 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.

Archive: oradb.zip
[oradb.zip] oradb.json password:
  inflating: oradb.json
Traceback (most recent call last):
  File "/home/oracle/dbsat/./sat_reporter.py", line 7131, in <module>
    fn()
  File "/home/oracle/dbsat/./sat_reporter.py", line 4669, in external_procedure
    extproc_envs[name] = env_val
TypeError: unhashable type: 'list'

DBSAT Reporter ran successfully.

Calling /usr/bin/zip to encrypt the generated reports...
Enter password:
Verify password:
  zip warning: oradb_report.zip not found or empty
  adding: oradb_report.txt (deflated 76%)
  adding: oradb_report.html (deflated 83%)
  adding: oradb_report.xlsx (deflated 3%)
  adding: oradb_report.json (deflated 81%)
zip completed successfully.
```

# Reporte generado en formato HTML

## Oracle Database Security Assessment

Highly Confidential

### Assessment Date & Time

Date of Data Collection	Date of Report	Reporter Version
Tue Aug 27 2019 08:53:00	Tue Aug 27 2019 09:02:21	2.1 (March 2019) - 7a38

### Database Identity

Name	Platform	Database Role	Log Mode	Created
ORADB	Linux x86 64-bit	PRIMARY	NOARCHIVELOG	Tue Jan 15 2019 10:43:00

### Summary

Section	Pass	Evaluate	Advisory	Low Risk	Medium Risk	High Risk	Total Findings
<a href="#">Basic Information</a>	0	0	0	0	0	0	0
<a href="#">User Accounts</a>	5	0	0	4	2	1	12
<a href="#">Privileges and Roles</a>	5	15	0	0	0	1	21
<a href="#">Authorization Control</a>	0	0	2	0	0	0	2
<a href="#">Fine-Grained Access Control</a>	0	1	4	0	0	0	5

# Reporte generado en formato EXCEL

The screenshot shows an Excel spreadsheet titled "Oracle Database Security Assessment - Highly Confidential". The report content is as follows:

Oracle Database Security Assessment - Highly Confidential					
Assessment Date & Time	Date of Data Collection	Date of Report		Reporter Version	
	Tue Aug 27 2019 08:53:00	Tue Aug 27 2019 09:02:21		2.1 (March 2019) - 7a38	
Database Identity	Name	Platform	Database Role	Log Mode	Created
	ORADB	Linux x86 64-bit	PRIMARY	NOARCHIVELOG	Tue Jan 15 2019
<b>Basic Information</b>					
Item	Refs ID	Status	Result	Remarks	
Database Version	Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production				
Security Features	Feature		Currently Used		
	-----				
	AUDITING				
	Traditional Audit		Yes		
	Fine Grained Audit		No		
	Unified Audit		Yes		
	AUTHORIZATION CONTROL				
	Database Vault		No		
	Privilege Analysis		No		

# Reporte generado en formato TXT

```
### Oracle Database Security Assessment - Highly Confidential ###

* Assessment Date & Time *
Date of Data Collection  Date of Report          Reporter Version
-----
Tue May 14 2019 11:51:00 Tue May 14 2019 11:52:54 2.1 (March 2019) - 7a38

* Database Identity *
Name  Platform          Database Role Log Mode   Created
-----
OSILDB Linux x86 64-bit PRIMARY     ARCHIVELOG Mon Aug 22 2011 12:57:00

### Summary ###

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      3      6      0     11
Privileges and Roles  5     15      0      0      0      1     21
Authorization Control  0      0      1      0      0      0      1
Fine-Grained Access Control  0      0      2      0      0      0      2
Auditing              4      4      1      0      2      0     11
Encryption            0      1      1      0      0      0      2
Database Configuration  6      2      0      3      4      0     15
Network Configuration  0      1      0      0      2      0      3
Operating System      1      1      0      2      1      0      5
Total                 18     24      5      8     15      2     72
```



# Ejecución de la herramienta DBSAT - Módulo Discover

Ingresar al directorio

**/home/oracle/dbsat/Discover/conf**

Copiar el archivo **sample\_dbsat.config** y colocarle el nombre **dbsat.config**.  
Editar el archivo **dbsat.config** y agregar los parámetros necesarios

```
#####  
  
#Database Section: Allows the user to provide DB server details  
[Database]  
  
#DB_IP is the IP address or FQDN for the DB Server  
#default is localhost  
  
DB_HOSTNAME = localhost  
  
#DB_PORT is the port at which the DBSAT tool needs to connect to  
#default is 1521  
  
DB_PORT = 1521  
  
#DB_SERVICE_NAME is the service Name for the DB  
#default is empty  
  
DB_SERVICE_NAME = oradb  
  
#####
```

```
[oracle@srv1 dbsat]$ cd Discover/conf/  
[oracle@srv1 conf]$ ls -l  
total 212  
-r--r--r--. 1 oracle oinstall 5136 Feb 28 11:27 sample_dbsat.config  
-r--r--r--. 1 oracle oinstall 29090 Feb 28 11:27 sensitive_de.ini  
-r--r--r--. 1 oracle oinstall 31911 Feb 28 11:27 sensitive_en.ini  
-r--r--r--. 1 oracle oinstall 26829 Feb 28 11:27 sensitive_es.ini  
-r--r--r--. 1 oracle oinstall 27308 Feb 28 11:27 sensitive_fr.ini  
-r--r--r--. 1 oracle oinstall 25172 Feb 28 11:27 sensitive_it.ini  
-r--r--r--. 1 oracle oinstall 26302 Feb 28 11:27 sensitive_nl.ini  
-r--r--r--. 1 oracle oinstall 27424 Feb 28 11:27 sensitive_pt.ini  
[oracle@srv1 conf]$ cp sample_dbsat.config dbsat.config  
[oracle@srv1 conf]$
```

# Ejecución de la herramienta DBSAT – Módulo Discover

Validar variable de entorno JAVA\_HOME: **Se requiere utilizar java 1.8 o superior**

Luego ejecutar el comando discover

**./dbsat discover -c ./Discover/conf/dbsat.config oradb\_discovery**

Solicitará el ingreso de credenciales de un usuario con privilegios DBA

Y se deberá asignar un password para el archivo de reportes.

```
[oracle@srv1 dbsat]$ echo $JAVA_HOME
[oracle@srv1 dbsat]$ export JAVA_HOME=/u01/java/jre1.8.0_211/
[oracle@srv1 dbsat]$ ./dbsat discover -c ./Discover/conf/dbsat.config oradb_discovery

Database Security Assessment Tool version 2.1 (March 2019)

This tool is intended to assist in you in securing your Oracle database
system. 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.

Enter username: system
Enter password:
DBSAT Discover ran successfully.
Calling /usr/bin/zip to encrypt the generated reports...

Enter password:
Verify password:
zip warning: oradb_discovery_report.zip not found or empty
adding: oradb_discovery_discover.html (deflated 85%)
adding: oradb_discovery_discover.csv (deflated 82%)
Zip completed successfully.
[oracle@srv1 dbsat]$
```

# Reporte generado en formato HTML

## Oracle Database Sensitive Data Assessment

Highly Confidential

### Assessment Date & Time

Date of DBSAT Report Generation	DBSAT Discoverer Version
Tue Aug 27 2019 09:29:16	2.1 (March 2019)

### Database Identity

Name	Platform	Database Role	Log Mode	Date Created
ORADB	Linux x86 64-bit	PRIMARY	NOARCHIVELOG	Tue Jan 15 2019 10:43:57

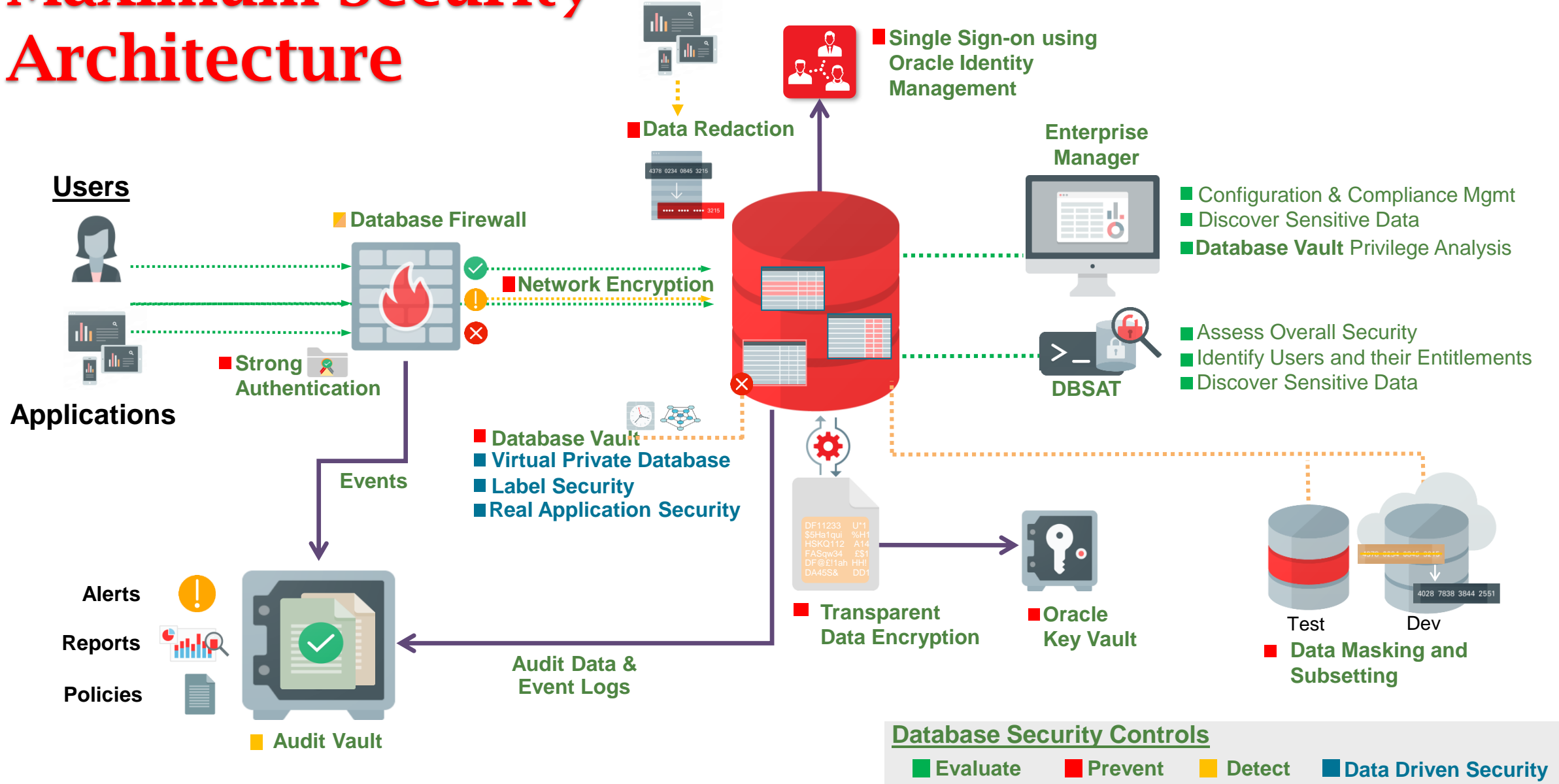
### Database Version

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

### Discovery Parameters

Parameter	Values
Schema Scope	ALL
Exclusion List File	NONE

# Maximum Security Architecture



# Oracle Database Security Controls

EVALUATE	PREVENT	DETECT	DATA DRIVEN SECURITY
Privilege Analysis <b>Database Vault</b>	DBA & Operation Controls <b>Database Vault</b>	Database Firewall	Label Security
EM DB Life-Cycle Management Pack	Data Masking and Subsetting	Audit Vault and Database Firewall	Real Application Security
Security Assessment Tool (Free for Oracle customers)	Key Vault	Alerting & Reporting	(included in) <b>DB Enterprise Edition</b>
(included in) <b>All security options</b>	Data Redaction <b>Advanced Security</b> Data Encryption	(included in) <b>DB Standard Edition</b>	Crypto Toolkit for Applications





*Gracias por tú participación*

