

Ingeniero de Sistemas, con especialidad en Base de Datos, Oracle Certified Professional con más de 12 años de experiencia en Administración, Respaldo, Recuperación, Afinamiento, y Replicación de Base de Datos.

Especialista y Certificado en Alta Disponibilidad (Oracle OCP 9i, 10g & 11g, OCE RAC & Tuning)

Especialista en Soluciones de Contingencia (Oracle Standby, Dataguard, Golden Gate & Shareplex)

Especialista en Implementaciones de Datawarehouse & Datamarts with Oracle Databases

Administrador de Servidor de Aplicaciones Oracle (OAS) y conocimientos sólidos de Linux and UNIX.

Administrador Oracle DBA-APPS - Oracle E-Business Suite 11i

SQL Server & Informix Dynamic Server Database Administrator

SAP BASIS Administrator con Tecnología NetWeaver sobre plataformas Windows, Linux and UNIX.

SAP HANA Administrator on Suse Enterprise Linux

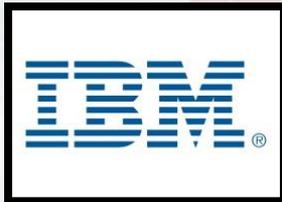
Ing. Yonogy Curi Pomahuali



Oracle University Instructor since April 2004
At Cibertec, GBS, New Horizons & Edutronic



Actualmente trabajo en:



Correo : ycuri@pe.ibm.com



Email: yonogy.curi@edutronicgs.com

Skype ID: [yonogy.orcl](https://www.skype.com/en/contacts/yonogy.orcl)

Blog: <http://orclperunet.blogspot.com/>

Facebook Group: [Oracle Peruvian Network](https://www.facebook.com/OraclePeruvianNetwork)

Facebook Page: [Edutronic Global Services](https://www.facebook.com/EdutronicGlobalServices)

Nuestra Visión



ORACLE WORKFORCE
DEVELOPMENT PROGRAM

Programa exclusivo para individuos

EDUTRONIC tiene como visión convertirse en una entidad líder en capacitación en Tecnologías de Información en todo el Perú.



Nuestra Misión



ORACLE WORKFORCE DEVELOPMENT PROGRAM

Programa exclusivo para individuos

EDUTRONIC tiene como misión especializar en Tecnologías de la Información a estudiantes universitarios y profesionales en general para que puedan alcanzar destreza técnica , reconocimientos laborales y certificaciones Internacionales



Nuestros Instructores



ORACLE WORKFORCE
DEVELOPMENT PROGRAM

Programa exclusivo para individuos

Los Instructores con amplia experiencia técnica y pedagógica que forman parte de nuestro equipo son:

- Ing. Martín Sarmiento
- Ing. Mauricio Rojas
- Ing. Jorge Zorrilla
- Ing. Francisco Riccio
- Ing. Javier Anto
- Ing. Yonogy Curi





ORACLE® WORKFORCE DEVELOPMENT PROGRAM

Programa exclusivo para individuos

Oracle University eDelivery

Logged in as yonogy.curi@edutronicgs.com | [Logout](#)

[OU PARTNER HOME](#) | [OU PARTNER MEMBER HOME](#) | [CONTACT US](#)

INSTITUTIONS

[Apply for membership](#)

[Find a member near you](#)

Find a Member Near You

Select a Country: Select a State: Enter a City: Partner Type:

Delivery Method:

Search Results

Institution Name	Nombre del Departamento	Ubicación de las Instalaciones	Country	State	Delivery Method	Website
BS Grupo S.A.C.	Capacitación	Arequipa	PE	AREQUIPA	Instructor Led Training	BS Grupo S.A.C.
CENTRO NETEC PERU SAC	Capacitación	Lima	PE	SAN ISIDRO	Instructor Led Training	CENTRO NETEC PERU SAC
Cibertec Peru S.A.C.	Cibertec	Av. Salaverry 2255 I27	PE	LIMA	Instructor Led Training	Cibertec Peru S.A.C.
Edutronic Global Services E.I.R.L	Educacion	Lima	PE	LIMA	Instructor Led Training	Edutronic Global Services E.I.R.L



ORACLE WORKFORCE DEVELOPMENT PROGRAM

Programa exclusivo para individuos



eKit

Oracle University eDelivery

Logged in as yonogy.curi@edutronicgs.com | [Logout](#)

[MEMBER LOG IN](#)

[CONTACT US](#)

Ingresar una Orden

Nombre del Producto de Búsqueda :

Language :

Search Results

Cart	Número de Parte #  	Descripción:  
	D80198GC11S	Oracle Database 12c: SQL and PL/SQL Fundamentals, 1.1 English Student Kit
	D81250GC10S	Oracle Database 12c: RAC Administration, 1.0 English Student Kit
	D79236GC10S	Oracle Database 12c: Performance Management and Tuning, 1.0 English Student Kit
	D77758GC20S	Oracle Database 12c: New Features for Administrators, 2.0 English Student Kit
	D77766GC10S	Oracle Database 12c: Install and Upgrade Workshop, 1.0 English Student Kit
	D78850GC20S	Oracle Database 12c: Backup and Recovery Workshop, 2.0 English - Student Kit
	D78846GC20S	Oracle Database 12c: Administration Workshop, 2.0 English Student Kit
	D50323GC20S	Oracle Database 11g: Security, 2.0 English Student Kit
	D52163GC10S	Oracle Database 11g: SQL Tuning Workshop 1.0 English Student Kit

Buenas Prácticas de Seguridad de BD

ORACLE™

Oracle Database Security Best Practices

Ing. Yonogy Curi Pomahuali
Edutronic CEO

Oracle Security Solutions



Buenas Prácticas de Seguridad de BD

Configurar y Supervisar Reportes de Auditoría

- Configurar DB EXTENDED ó XML EXTENDED y AUDIT_SYS_OPERATIONS
- Analizar Eventos de Auditoría de Base de Datos y Alertar actividades sospechosas en la Base de Datos
- Implementar AUDIT VAULT y DATABASE FIREWALL para proteger, centralizar y consolidar Logs y Reportes de Auditoría de diferentes Motores de Base de Datos

Monitorear Trafico de BD y bloquear amenazas

- Monitorear y alertar tráfico de la Base de Datos sobre la red
- Proteger de «SQL Injection» para evitar código malicioso a nivel de SQL Dinámico

Proteger Ambientes de Base de Datos

- Enmascarar la data para Base de Datos de Desarrollo y Calidad
- TDE para proteger información sensitiva de la Base de Datos

Limitar el Acceso a la BD y APPS

- Limitar acceso a la data a nivel de SO, Red y a los dispositivos de almacenamiento.
- Separación de Responsabilidades para una buena administración de la Infraestructura en general
- Limitar acceso a la data de la aplicación para los usuarios privilegiados (DATABASE VAULT)

Configurar Auditoría

Configurar y
Supervisar
Reportes de
Auditoría

- Configurar
DB EXTENDED ó
XML EXTENDED y
AUDIT_SYS_OPERATIONS

```
oracle@oracle12c:~  
SQL>  
SQL>  
SQL>  
SQL> show parameter audit_trail  


| NAME        | TYPE   | VALUE        |
|-------------|--------|--------------|
| audit_trail | string | DB, EXTENDED |



```
SQL>
SQL> show parameter audit_sys_operations

NAME	TYPE	VALUE
audit_sys_operations	boolean	TRUE


```
SQL>  
SQL>  
SQL>  
SQL>
```


```


```

Analizar Eventos de Auditoría

Configurar y
Supervisar
Reportes de
Auditoría

- Analizar Eventos de Auditoría de Base de Datos y Alertar actividades sospechosas en la Base de Datos

Implementar AUDIT VAULT para centralizar y consolidar los Reportes de Auditoría de diferentes Base de Datos

```
oracle@oracle12c:/u01/app/oracle/product/12.1.0/db_1
SQL> SELECT COUNT (*) FROM DBA_PRIV_AUDIT_OPTS;

COUNT (*)
-----
0

SQL> SELECT COUNT (*) FROM DBA_STMT_AUDIT_OPTS;

COUNT (*)
-----
0

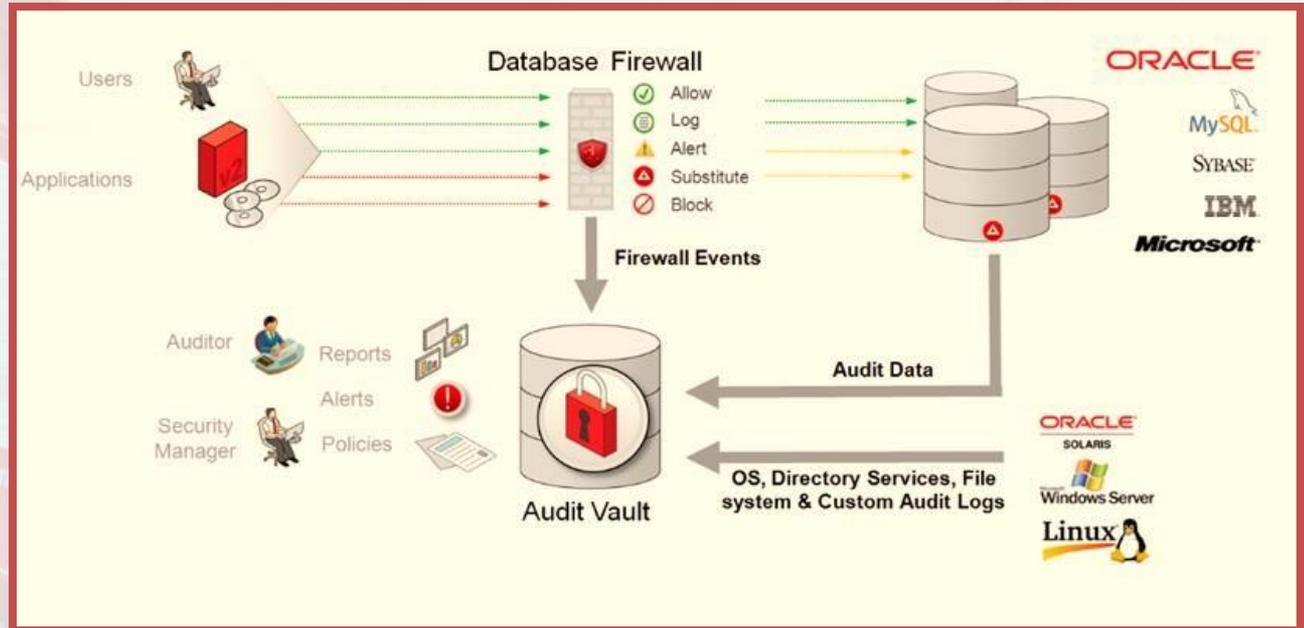
SQL> select count(*) from dba_audit_trail;

COUNT (*)
-----
0

SQL>
```

Audit Vault & Database Firewall

Configurar y Supervisar Reportes de Auditoría



- Implementar AUDIT VAULT y DATABASE FIREWALL para centralizar y consolidar Logs y Reportes de Auditoría de diferentes Motores de Base de Datos

- Oracle Database Firewall actúa como la primera línea de defensa para bases de datos, ayudando prevenir ataques internos y externos a la base de datos.
- El Audit Vault es el repositorio central que almacena y consolida los eventos de auditoría. Es la plataforma central para la presentación de informes, alertas y gestión de políticas.

Event Time	Class	Type	flame	Client IP	User flame	Command Class	Command Text	Location
11/27/2012 4:08:27 PM	Database	Oracle Database	target1	10.240.114.167	avadmin	DDL	create user joedba identified by HIDDEN	Network
11/28/2012 6:28:46 PM	OS	Microsoft Windows	msw	10.240.169.211	Windows Administrator	LOGON		Event Log
11/28/2012 3:07:53 AM	Database	Oracle Database	Sales DB		SYSTEM	GRANT	grant dba to apposdba	Audit Table
11/28/2012 3:07:50 AM	Database	Oracle Database	Sales DB		SYSTEM	CREATE	create user apposdba identified by *	Audit Table
11/28/2012 2:18:27 AM	Database	Microsoft SQL Server	CRM Database	10.240.169.211	crmapp	SELECT	select * from credit_card where ssn = '*****'	Network

Alertar tráfico de BD sobre la Red

Monitorear
Tráfico de BD
y bloquear
amenazas

- Monitorear y alertar tráfico de la Base de Datos sobre la red

```
C:\Windows\system32\cmd.exe
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
SQL> select * from hr.regions;
REGION_ID REGION_NAME
-----
1 Europe
2 Americas
3 Asia
4 Middle East and Africa
```

*VirtualBox Host-Only Network [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
20	3.40967900	172.68.1.16	172.68.1.1	TCP	54	1521-49547 [ACK] Seq=4540 Ack=5022 win=29568 Len=0
21	3.41001700	172.68.1.16	172.68.1.1	TNS	270	Response, Data (6), Data
22	3.42278400	172.68.1.16	172.68.1.1	TNS	695	Response, Data (6), Data
23	3.42414600	172.68.1.16	172.68.1.1	TNS	175	Response, Data (6), Data
24	3.43211300	172.68.1.16	172.68.1.1	TNS	165	Response, Data (6), Data
25	3.46209700	172.68.1.16	172.68.1.1	TNS	188	Response, Data (6), Data
26	3.46661300	172.68.1.16	172.68.1.1	TNS	377	Response, Data (6), Data
27	3.46776900	172.68.1.16	172.68.1.1	TNS	71	Response, Data (6), Data
28	3.46867700	172.68.1.16	172.68.1.1	TNS	71	Response, Data (6), Data
29	13.2371020	172.68.1.16	172.68.1.1	TNS	391	Response, Data (6), Data
30	13.2380410	172.68.1.16	172.68.1.1	TNS	258	Response, Data (6), Data
31	23.3231680	172.68.1.16	172.68.1.1	TCP	54	1521-49547 [ACK] Seq=6661 Ack=6882 win=47104 Len=0
32	23.5208040	172.68.1.16	172.68.1.1	TNS	165	Response, Data (6), Data
33	25.6158840	172.68.1.16	172.68.1.1	TCP	54	1521-49547 [ACK] Seq=6772 Ack=6895 win=47104 Len=0
34	25.6177280	172.68.1.16	172.68.1.1	TNS	71	Response, Data (6), Data
35	25.6222900	172.68.1.16	172.68.1.1	TCP	54	1521-49547 [FIN, ACK] Seq=6789 Ack=6905 win=47104 Len=0

Reserved Byte: 00
Header Checksum: 0x0000
Data

0040	06 1a 02 00 00 00 00 0f 00 00 00 00 00 00 00 00A
0050	00 00 00 00 00 00 07 0f 2c 01 02 02 c1 03 08 41A
0060	6d 65 72 69 63 61 73 07 0b 2c 01 02 02 c1 04 04	mericas.....A
0070	41 73 69 61 07 1d 2c 01 02 02 c1 05 16 4d 69 64	Asia.....Mid
0080	64 6c 65 20 45 61 73 74 20 61 6e 64 20 41 66 72	dle East and Afr
0090	69 63 61 04 01 00 00 00 10 00 04 00 00 00 7b 05	ica.....{.
00a0	00 00 00 00 02 00 00 00 03 00 20 00 00 00 00 00
00b0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00c0	12 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Data (data.data), 194 bytes Packets: 36 - Displayed: 36 (100.0%) - Dropped: 0 (0.0%) Profile: Default

«Injection» para
evitar código
malicioso a nivel
de SQL Dinámico

Protección contra “SQL Injection”

Monitorear
Tráfico de BD
y bloquear
amenazas



sql-injection-01.txt

- Proteger de «SQL Injection» para evitar código malicioso a nivel de SQL Dinámico

```
oracle@oracle12c:/u01/app/oracle/product/12.1.0/db_1
SQL> CREATE OR REPLACE
PROCEDURE show_col (p_colname varchar2, p_tablename  varchar2)
 2   3 AS
 4   type t is varray(200) of varchar2(25);
 5   Results t;
 6   Stmt CONSTANT VARCHAR2(4000) := 'SELECT ' || p_colname || ' FROM ' || p_tablename;
 7
 8   BEGIN
 9     DBMS_Output.Put_Line ('SQL Stmt: ' || Stmt);
10     EXECUTE IMMEDIATE Stmt bulk collect into Results;
11     for j in 1..Results.Count() loop
12       DBMS_Output.Put_Line(Results(j));
13     end loop;
14     --EXCEPTION WHEN OTHERS THEN
15       --Raise_Application_Error(-20000, 'Wrong table name');
16   END show_col;
17   /

Procedure created.

SQL> execute show_col('Email','EMPLOYEES');
SQL Stmt: SELECT Email FROM EMPLOYEES
ABANDA
ABULL
ACABRIO
```

Protección contra “SQL Injection”

Monitorear
Tráfico de BD
y bloquear
amenazas



sql-injection-01.txt

La Base de Datos

- Proteger de «SQL Injection» para evitar código malicioso a nivel de SQL Dinámico

```
oracle@oracle12c:/u01/app/oracle/product/12.1.0/db_1
SQL> execute show_col('Email','EMPLOYEES where 1=2 union select Username c1 from All Users --');
SQL Stmt: SELECT Email FROM EMPLOYEES where 1=2 union select Username c1 from
All_Users --
ANONYMOUS
APEX_040200
APEX_PUBLIC_USER
APPQOSSYS
ASURCO_PE
AUDSYS
BI
CTXSYS
DBSNMP
DIP
DVF
DVSYS
FLOWS_FILES
GSMADMIN_INTERNAL
GSMCATUSER
GSMUSER
HR
IX
JPINOL_CHI
LBACSYS
LGUERREO_CHI
MDDATA
MDSYS
OE
OJVMSYS
OLAPSYS
ORACLE_OCM
```

Protección contra “SQL Injection”

Monitorear
Tráfico de BD
y bloquear
amenazas

```
oracle@oracle12c:~  
NAME                                PASSWORD  
-----  
GSMCATUSER                          0F6108F5BBC60C1F  
GSMUSER                              56D6F489B0F97093  
GSMUSER_ROLE  
GSM_POOLADMIN_ROLE  
HR                                    4C6D73C3E8B0F0DA  
HS_ADMIN_EXECUTE_ROLE  
HS_ADMIN_ROLE  
HS_ADMIN_SELECT_ROLE  
IMP_FULL_DATABASE  
IX                                    2BE6F80744E08FEB
```

- Proteger de «SQL Injection» para evitar código malicioso a nivel de SQL Dinámico

```
C:\Windows\system32\cmd.exe  
  
C:\Users\dauid>orabf 4C6D73C3E8B0F0DA:HR -c 3 -m 5  
orabf v0.7.6, (C)2005 orm@toolcrypt.org  
-----  
Trying default passwords...  
password found: HR:HR  
C:\Users\dauid>  
C:\Users\dauid>  
C:\Users\dauid>
```


Protección contra “SQL Injection”

Monitorear
Tráfico de BD
y bloquear
amenazas



sql-injection-02.txt

- Proteger de «SQL Injection» para evitar código malicioso a nivel de SQL Dinámico

```
oracle@oracle12c:/u01/app/oracle/product/12.1.0/db_1
SQL> SET SERVEROUTPUT ON

CREATE OR REPLACE
PROCEDURE show_col2 (p_colname varchar2, p_tablename  varchar2)
AS
type t is varray(200) of varchar2(25);
Results t;

    stmt CONSTANT VARCHAR2(4000) :=
        'SELECT ' || dbms_assert.simple_sql_name( p_colname ) || ' FROM ' || dbms_assert.simple_sql_name( p_tablename ) ;
BEGIN
    DBMS_output.Put_Line ('SQL Stmt: ' || Stmt);
    EXECUTE IMMEDIATE Stmt bulk collect into Results;
    for j in 1..Results.Count() loop
    DBMS_output.Put_Line(Results(j));
    end loop;
--EXCEPTION WHEN OTHERS THEN
    --Raise_Application_Error(-20000, 'Wrong table name');
SQL> SQL> 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 END show_col2;
19 /

Procedure created.

SQL> execute show_col2('Email','EMPLOYEES where 1=2 union select Username c1 from All_Users --');
BEGIN show_col2('Email','EMPLOYEES where 1=2 union select Username c1 from All_Users --'); END;

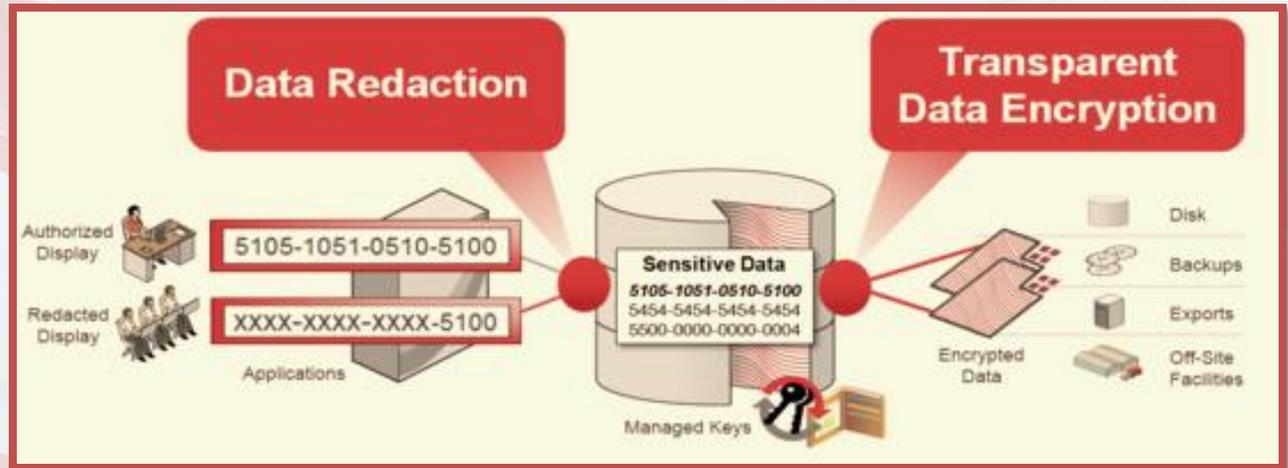
*
ERROR at line 1:
ORA-44003: invalid SQL name
ORA-06512: at "SYS.DBMS_ASSERT", line 206
ORA-06512: at "HR.SHOW_COL2", line 6
ORA-06512: at line 1

SQL>
```

Data Redaction

Proteger
Ambientes de
Base de Datos

- Enmascarar la data para Base de Datos de Desarrollo y Calidad



de la Base de Datos

Sin protección:

```
oracle@oracle12c:/u01/app/oracle/product/12.1.0/db_1
SQL> SELECT *
FROM payment_details
ORDER BY id; 2 3
```

ID	CUSTOMER_ID	CARD_NO	CARD_STRING	EXPIRY_DATE	SEC_CODE	VALID_DATE
1	4000	1234123412341234	1234-1234-1234-1234	12-AUG-2016	123	
2	4001	2345234523452345	2345-2345-2345-2345	12-AUG-2016	234	
3	4002	3456345634563456	3456-3456-3456-3456	12-AUG-2016	345	
4	4003	4567456745674567	4567-4567-4567-4567	12-AUG-2016	456	
5	4004	5678567856785678	5678-5678-5678-5678	12-AUG-2016	567	

```
SQL>
```



Data-redaction.txt

Data Redaction

Proteger
Ambientes de
Base de Datos

- Enmascarar la data para Base de Datos de Desarrollo y Calidad

```
oracle@oracle12c:/u01/app/oracle/product/12.1.0/db_1
SQL> CONNECT PCI/PCI
Connected.
SQL> BEGIN
  DBMS_REDACT.add_policy(
    object_schema => 'PCI',
    object_name   => 'payment_details',
    column_name   => 'card no',
    policy_name   => 'redact_card_info',
    function_type => DBMS_REDACT.full,
    expression    => '1=1'
  );
END;
/ 2 3 4 5 6 7 8 9 10 11

PL/SQL procedure successfully completed.

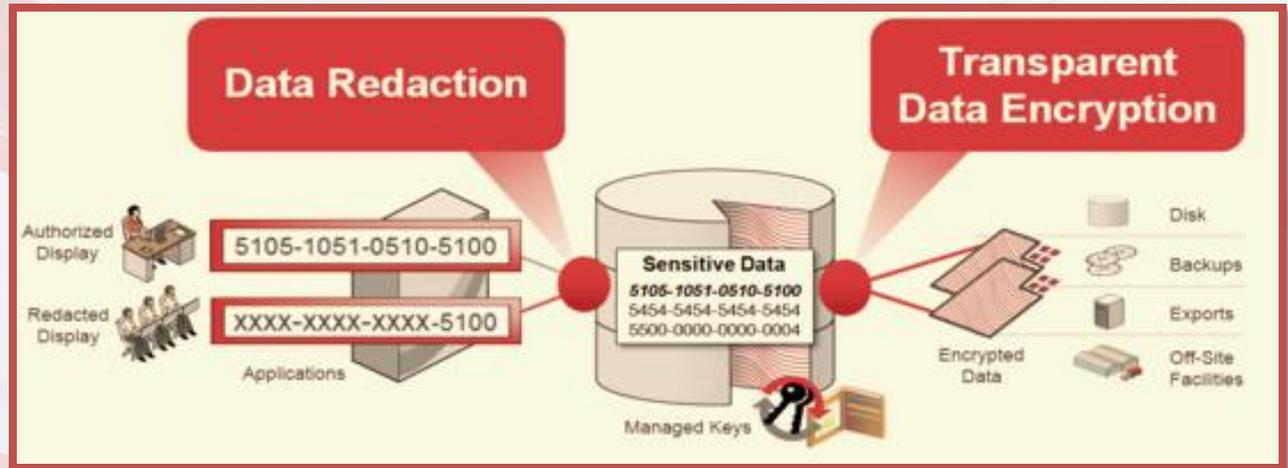
SQL>
```

```
oracle@oracle12c:/u01/app/oracle/product/12.1.0/db_1
SQL>
SQL> SELECT *
FROM   payment_details
ORDER BY id;
 2    3
-----
      ID CUSTOMER_ID CARD_NO CARD_STRING          EXPIRY_DATE      SEC_CODE VALID_DATE
-----
      1          4000          0 1234-1234-1234-1234 12-AUG-2016          123
      2          4001          0 2345-2345-2345-2345 12-AUG-2016          234
      3          4002          0 3456-3456-3456-3456 12-AUG-2016          345
      4          4003          0 4567-4567-4567-4567 12-AUG-2016          456
      5          4004          0 5678-5678-5678-5678 12-AUG-2016          567

SQL>
```

Transparent Data Encryption (TDE)

Proteger
Ambientes de
Base de Datos

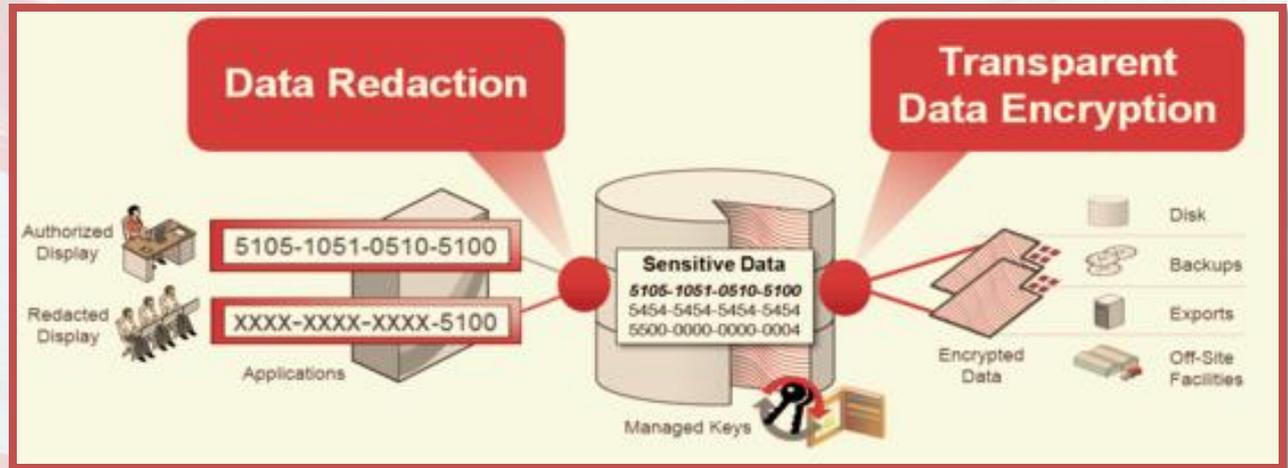


- TDE para proteger información sensible de la Base de Datos

```
oracle@oracle12c:~  
[oracle@oracle12c ~]$  
[oracle@oracle12c ~]$ mkstore -wrl /u01/app/oracle/admin/PRD/wallet -create  
Oracle Secret Store Tool : Version 12.1.0.2  
Copyright (c) 2004, 2014, Oracle and/or its affiliates. All rights reserved.  
  
Enter password:  
Enter password again:  
[oracle@oracle12c ~]$ sqlplus / as sysdba  
  
SQL*Plus: Release 12.1.0.2.0 Production on Wed Aug 12 10:18:11 2015  
  
Copyright (c) 1982, 2014, Oracle. All rights reserved.  
  
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  
  
SQL> ALTER SYSTEM SET WALLET OPEN IDENTIFIED BY "jesed2015";  
  
System altered.
```

Transparent Data Encryption (TDE)

Proteger
Ambientes de
Base de Datos



- TDE para proteger información sensitiva de la Base de Datos

```
oracle@oracle12c:/u01/app/oracle/admin/PRD/wallet
SQL> ALTER SYSTEM SET ENCRYPTION KEY AUTHENTICATED BY "josed2015";
System altered.
SQL> connect pci/PCI
Connected.
SQL> CREATE TABLE tde_test (
  id      NUMBER(10),
  data    VARCHAR2(50) ENCRYPT
) TABLESPACE USERS;
2      3      4
Table created.
SQL>
```

Limitar acceso a la data a nivel de SO

Limitar
el Acceso a la
BD y APPS

- Limitar acceso a la data a nivel de SO, Red y a los dispositivos de almacenamiento.

```
oracle@oracle12c:/u01/app/oracle/product/12.1.0/db_1
[oracle@oracle12c db_1]$ umask
0022
[oracle@oracle12c db_1]$ umask 0027
[oracle@oracle12c db_1]$
[oracle@oracle12c db_1]$ touch edutronic.txt
[oracle@oracle12c db_1]$ ls -lrt edutronic.txt
-rw-r-----. 1 oracle oinstall 0 Aug 11 15:20 edutronic.txt
[oracle@oracle12c db_1]$
[oracle@oracle12c db_1]$ umask
0027
[oracle@oracle12c db_1]$
```

```
oracle@oracle12c:/u01/app/oracle/product/12.1.0/db_1
brw-rw----. 1 root   disk    8,  80 Aug 11 13:07 /dev/sdf
brw-rw----. 1 root   disk    8,  96 Aug 11 13:07 /dev/sdg
brw-rw----. 1 root   disk    8,  65 Aug 11 13:07 /dev/sde1
brw-rw----. 1 root   disk    8,  17 Aug 11 13:07 /dev/sdb1
brw-rw----. 1 root   disk    8,  49 Aug 11 13:07 /dev/sdd1
brw-rw----. 1 root   disk    8,   2 Aug 11 13:07 /dev/sda2
brw-rw----. 1 root   disk    8,   1 Aug 11 13:07 /dev/sda1
brw-rw----. 1 root   disk    8,  33 Aug 11 13:07 /dev/sdc1
brw-rw----. 1 oracle asmadmin 8,  97 Aug 11 15:22 /dev/sdg1
brw-rw----. 1 oracle asmadmin 8,  81 Aug 11 15:22 /dev/sdf1
[oracle@oracle12c db_1]$
```

Separación de Responsabilidades

Limitar
el Acceso a la
BD y APPS

Los administradores de bases de datos (DBA) y administradores de sistemas con frecuencia entran en conflicto debido a la superposición de las tareas que realizan a diario.
Se sugiere las siguientes tareas para cada uno de ellos:

SYSTEM ADMINISTRATOR:

- Network
- Server hardware
- Server file/OS backup
- Offline backup
- Server upgrade and patching
- Monitoring and analysing server logs
- Disk space monitoring
- Third party backup tool/ Tape backup
- Manager scheduled tasks
- Allocate LUNs from SAN

DATABASE ADMINISTRATOR:

- Database performance monitoring
- Database server tuning (IO, memory, CPU)
- Database Backup and Recovery
- Database Upgrade and Patching
- Database Disaster Recovery
- Instance Configuration
- Database Creation
- Configure Database Cluster
- Setup and Configure Standby Replication
- Database audits and Change Management
- Configure Database Security
- Database Documentation

- Separación de Responsabilidades para una buena administración de la Infraestructura en general

Limitar accesos con Database Vault

Limitar
el Acceso a la
BD y APPS



Oracle-database-vault.txt

```
Enable Oracle Database Vault
-----
cd $ORACLE_HOME/rdbms/lib
-----
$ make -f ins_rdbms.mk dv_on lbac_on ioracle

SQL> startup;

SQL> select * from v$option where parameter like '%Database Vault%';

PARAMETER
-----
VALUE
-----
Oracle Database Vault      TRUE

SQL> select * from v$option where parameter like '%Label%';

PARAMETER                                     VALUE
-----
Oracle Label Security                                     TRUE

Disable Oracle Database Vault
-----

$ cd $ORACLE_HOME/rdbms/lib
$ make -f ins_rdbms.mk dv_off ioracle
```

- Limitar acceso a la data de la aplicación para los usuarios privilegiados (DATABASE VAULT)

Limitar accesos con Database Vault

Controlar
el Acceso a la
BD y APPS

```
oracle@oracle12c:~  
SQL>  
SQL> show user  
USER is "SYS"  
SQL>  
SQL> select * from hr.region;  
select * from hr.region  
*  
ERROR at line 1:  
ORA-00942: table or view does not exist  
SQL>
```

Oracle Database ▾ Performance ▾ Availability ▾ Schema ▾ Administration ▾

Database Vault Logged in As MACSYS

Home Administration

Page Refreshed Nov 1, 2011 3:48:19 PM PDT Refresh

General

Status Enabled
Realms 6 0
Command Rules 8 0
Attempted Violations 3 (Last 24 Hours)
Database Vault Policy Changes 0 (Last 24 Hours)

Attempted Violations

Time Series View Data Last 24 hours ▾

Top 5 Attempted Violations

Type Realms ▾

No Attempted Violations (Last 24 Hours)

Top 5 Attempted Violators

Type Users ▾

User	Count	Percentage
SYS	2	67%
MACAUTH	1	33%

Policy Propagation

Database Vault Policy Propagation
(Use this feature to securely propagate Database Vault Policies to multiple databases)

Reports

Attempted Violations
Database Vault Policy Changes
Database Vault Reports

Alerts

Severity	Category	Name	Message	Alert Triggered
(No alerts)				

- Limitar acceso a la data de la aplicación para los usuarios privilegiados (DATABASE VAULT)

Buenas Prácticas de Seguridad de BD

Configurar y Supervisar Reportes de Auditoría

- Configurar DB EXTENDED ó XML EXTENDED y AUDIT_SYS_OPERATIONS
- Analizar Eventos de Auditoría de Base de Datos y Alertar actividades sospechosas en la Base de Datos
- Implementar AUDIT VAULT y DATABASE FIREWALL para proteger, centralizar y consolidar Logs y Reportes de Auditoría de diferentes Motores de Base de Datos

Monitorear Trafico de BD y bloquear amenazas

- Monitorear y alertar tráfico de la Base de Datos sobre la red
- Proteger de «SQL Injection» para evitar código malicioso a nivel de SQL Dinámico

Proteger Ambientes de Base de Datos

- Enmascarar la data para Base de Datos de Desarrollo y Calidad
- TDE para proteger información sensitiva de la Base de Datos

Limitar el Acceso a la BD y APPS

- Limitar acceso a la data a nivel de SO, Red y a los dispositivos de almacenamiento.
- Separación de Responsabilidades para una buena administración de la Infraestructura en general
- Limitar acceso a la data de la aplicación para los usuarios privilegiados (DATABASE VAULT)

Preguntas y Respuestas



Muchas Gracias

ORACLE™

Oracle Database Security Best Practices

Ing. Yonogy Curi Pomahuali
Edutronic CEO

Oracle Security Solutions

