accentureoperations

Oracle Exadata Security – BIWA 2017

Agenda of the meeting -

- State of Database Security
- Exadata Security
- 360 view of Security with Exadata
- GDPR
- Oracle 12.2 new features

Chaitanya Geddam
Oracle Security
Practice Lead

Julian Dontcheff
Oracle Technology
Practice Executive

State of Database Security

WHY DATABASE SECURITY?

- Increase in vulnerabilities related to databases, and internal users having access to data
- Perimeter/network security alone is not enough

WHAT SHOULD SECURITY EXECUTIVES BE CONCERNED ABOUT?

- Do the IT policies adhere to industry standards with regards to database security?
- What measures are in place to protect from unauthorized access or misuse by privileged users?
- What measures are in place to protect from data corruption and unrecoverable and intentional damage to data?

$170
Avg. cost per lost or stolen record[1]

2,122
Confirmed data breaches[2]

$3.79M
Avg. total cost of data breach – 23% increase over last year – based on 350 companies from 11 countries[1]

55%
Of insider misuse is abuse of privilege by those already in trusted role[2]

40%
Of insider misuse motivated by financial gain[2]

[1] 2015 Cost of Cyber Crime Study Global – Ponemon Institute
[2] 2015 Data Breach Investigations Report – Verizon

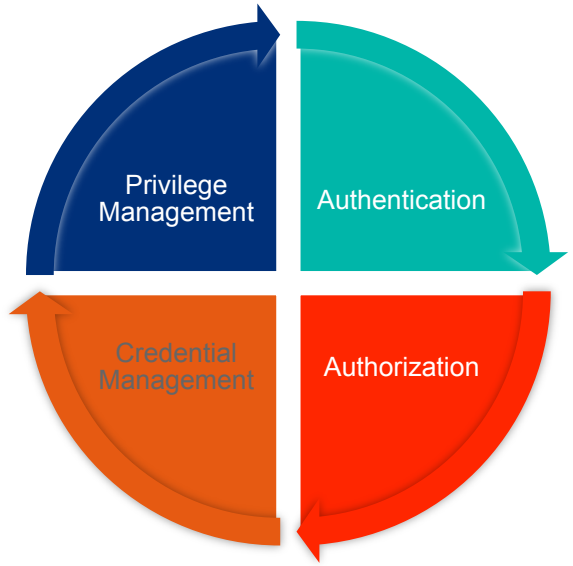
State of Exadata Security

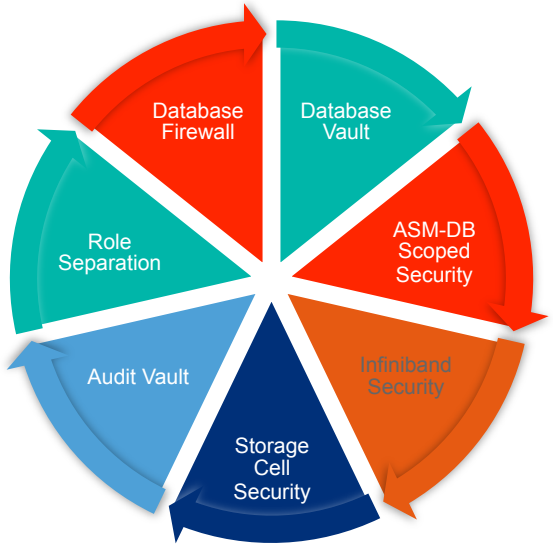
In build Perimeter Security

A complete engineered system that is ideal for consolidation and performance of Oracle Databases.

High Components of DB security:

- Perimeter Security
- Defence in depth
- Open Security by default
- DB Scoped Security and ASM Scoped Security (CellKey.ora – Key, asm, realm)
- Infiniband, Open Security by default but particular gateways can be assigned to segregate the networks.
- Auditd monitoring enabled (/etc/audit/audit.rules)
- Cellwall: iptables firewall
- Boot loader password protected





Compliance Strategy →

Intrusion Detection System (IDS) – Oracle Audit Vault and DB Firewall

DATABASE FOOTPRINT SUPPORTED

OPERATING SYSTEMS

- Linux (RHEL, OEL, SUSE)
- Solaris
- Windows
- HP-UX
- Z/OS

DATABASE SYSTEMS

- Oracle
- Teradata
- SQL Server
- DB2
- IMS
- Hadoop

DATABASE USERS, APPLICATION SERVERS

Source of Transactions

- Users
- Applications
- SOG
- Auditor
- Security Analyst
- SIEM / Integration

FIRST LEVEL OF DEFENSE MECHANISM

Database Firewall

Alerts
Built-in Reports
Custom Reports
Policies
QRadar

Database Firewall

Allow
Log
Alert
Substitute
Block

Firewall Events

Audit Vault
servicenow

CENTRALIZED AUDITING AND REPORTING

Oracle Audit Vault

Audit Data

OS, Directory, File System & Custom Audit Logs

ORACLE
TERADATA
SYBASE
IBM
Microsoft

ORACLE
SOLARIS
Windows Server

Oracle Advanced Security

INTRODUCTION

Oracle Advanced Security components include features of User administration and authentication, providing credentials
checks, centralized user management and TNS management.

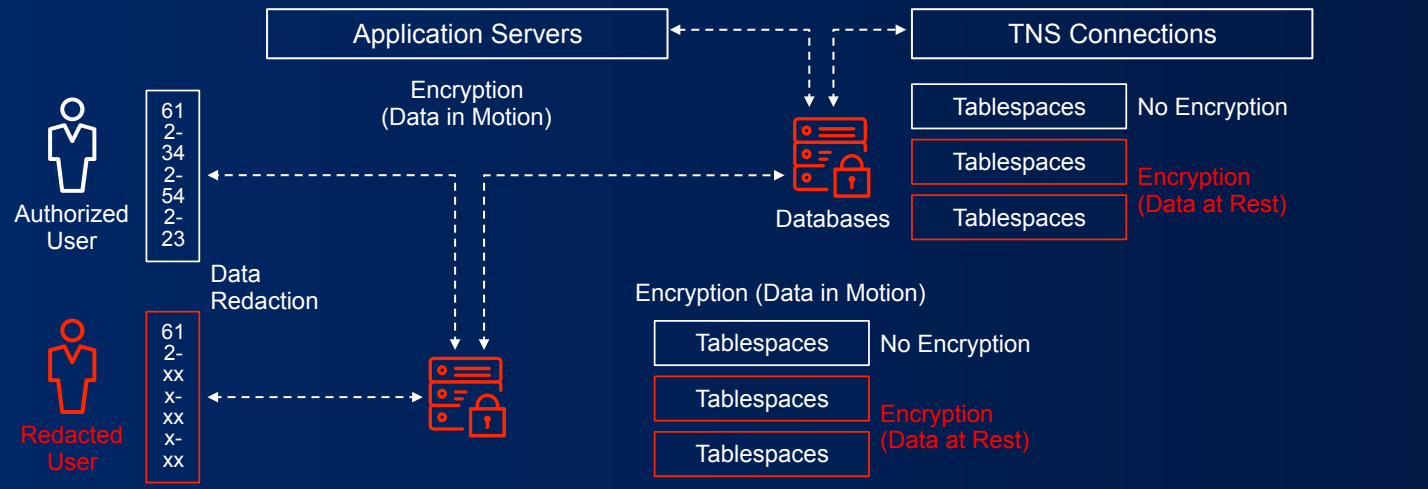
MAJOR COMPONENTS

- Oracle Unified Directory provides a centralized management of USER Stores, along with User administration, user authentication and authorization
- Oracle Key Vault provides capability in storing the Oracle Encryption keys
- Oracle Audit Vault provides capability for centralized database auditing
- Oracle Database Vault enables Privilege access management to comply with SoD governance
- Oracle Virtual Private Database allows granular access to specific set of dataset

SECURITY FEATURES TO BENEFIT ORACLE DATABASES

- Oracle Internet Directory
- Oracle Virtual Directory
- Virtual Private Database
- Oracle Universal Directory
- Oracle Key Vault
- Oracle Database Vault
- Oracle Audit Vault

ENCRYPTION (REST, IN-MOTION), REDACTION, MASKING



Database Security Health Check

INTRODUCTION

The Health check for Oracle database identifies the security risks which include violations to Access Control, Auditing, Authentication, Encryption, Integrity Controls and Application Security.

MAJOR SECURITY ISSUES IDENTIFIED?

Identifies

- Default ports for database and cluster ware listeners
- Access Control violations and Authentication violations
- Elevated access violations
- Cross site scripting violations
- Default passwords and violations to best practices for password management
- Analytics and reports of database auditing information

DISCOVERY PHASE

Deploy Scripts

Questionnaire (OR)
Pre-Assessment

VALIDATION PHASE

Access Violations

Authentication Violations

Elevated Access

Encryption (PII Data)

Auditing Analytics

REPORTING PHASE

Generate Reports

Reports (OR)
Compliance Number

GDPR – General Data Protection Regulation using Oracle Security

GDPR recognizes a EU citizens privacy information and the rights to it as a "Fundamental" right of the individual (ex: Bill of Right)

"GDPR is a regulation"

GDPR is a "LAW" versus a directive and it will have the enforcement and associated fines of a regulation

"GDPR Fines"

The GDPR recognizes that EU privacy data could be valued at $1 Trillion Euros and the non-compliance of the proper handling of this data can lead to fines of 4% or annual revenue

Controllers & Processors

The EU Data Directive only held controllers of data responsible for the data whereas the GDPR holds both controllers and processors

GDPR / Accenture Oracle Solution

Enkitec: DataBase Security 360-degree view (esec360) v1701

dbname:orcl version:11.2.0.4.0 host:jarvisdb02 license:T days:9 from:2017-01-22 to:2017-02-01 today:2017-01-31/21:09:37

1/7

Database Configuration

- Identification *(2)* html
- Version *(5)* html
- Database *(1)* html
- Instance *(2)* html
- Database and Instance History *(2)* html
- Instance Recovery *(2)* html
- Database Properties *(36)* html
- Options *(65)* html
- Registry *(19)* html
- Registry History *(3)* html
- Registry Hierarchy *(19)* html
- Apex Release *(1)* html
- Feature Usage Statistics *(161)* html
- License *(2)* html
- Resource Limit *(54)* html
- HWM Statistics *(17)* html
- Database Links *(0)* html
- Security related parameters *(32)* html
- Modified Parameters *(4)* html
- Non-default Parameters *(73)* html
- All Parameters *(707)* html
- Parameter File *(44)* html
- System Parameters Change Log *(19)* html
- SQLTXPLAIN Version *(-1)* html

Tasks

- Jobs *(63)* html
- Jobs Running *(0)* html
- Scheduler Jobs *(21)* html
- Scheduler Job Log for past 7 days *(489)* html
- Scheduler Windows *(9)* html
- Scheduler Window Group Members *(28)* html
- Automated Maintenance Tasks *(3)* html
- Automated Maintenance Tasks History *(36)* html

2/7

User Security Configuration

- Users *(58)* html
- Default Users *(23)* html
- Users With Default Password *(19)* html
- Users Last Changed Password *(58)* html
- Users with HTTP Digest password encryption *(0)* html
- Users with week password encryption *(59)* html
- Proxy Users and Client Privileges *(0)* html
- Proxy Users Cascade Table *(0)* html
- Proxy Users Cascade Graph *(0)* graph
- Password file users *(3)* html
- Inactive Users *(94)* html
- Expired or Locked Users *(28)* html
- Dropped Users still Connected *(0)* html
- Profiles *(32)* html
- Profile Verification Functions *(0)* html
- Profile Verification Functions Code *(0)* html
- Profile security information *(14)* html
- Minimal password security check *(12)* html
- Tablespace Quotas *(17)* html
- Current Session Connection Info *(7464)* html

System Privilege Analyses

- Inappropriate Tablespaces Granted *(3)* html
- Users with Drop User or Alter User *(10)* html
- Users with Alter Session and Alter System *(19)* html
- Elevated system privileges *(262)* html
- Users with EXPORT/IMPORT FULL *(5)* html
- Users with BECOME USER Privilege *(4)* html
- Users with ANY System Privilege *(545)* html
- SYSTEM-level End User Privileges *(1018)* html
- Execute Privileges To Strong SYS Packages *(55)* html
- Execute Privileges that allows User Impersonation *(8)* html
- Execute Privileges that allows Data Exfiltration *(0)* html
- OS Security Vulnerability Privileges *(44)* html
- ADVISOR Privileges *(6)* html
- ADMIN Option Sys Privileges *(269)* html
- Cascade System Privileges *(3599)* html
- Grants by System Privileges *(202)* html
- Grants by User *(86)* html

Object Privilege Analyses

- Non SYS objects on SYSTEM Tablespaces *(0)* html
- Non SYS objects on SYSAUX Tablespaces *(3201)* html
- PL/SQL objects that can Grant DBA *(0)* html
- Directories Privileges *(13)* html
- OBJECT-level End User Privileges to Users *(2694)* html
- OBJECT-level End User Privileges to Roles *(20797)* html
- Columns privileges *(4)* html
- Security holes in database links *(0)* html
- Objects Privileges By Grantee *(70)* html
- Objects Privileges By Grantee, Owner *(119)* html
- Objects Privileges By Grantee, Owner, Privilege *(414)* html
- Access To Sensitive Objects *(39)* html
- Public Execute Privilege To SYS PL/SQL Procedures *(329)* html
- Non-Owner Object Trigger *(15)* html
- Grantable Object/Columns privileges *(1773)* html

Roles Privilege Analyses

- Roles *(58)* html
- Sensitive Roles Granted *(38)* html
- Users with CATALOG Roles *(18)* html

3/7

Auditing

- Default Object Auditing Options *(1)* html
- Object Auditing Options *(0)* html
- Statement Auditing Options *(20)* html
- System Privileges Auditing Options *(20)* html
- Audit related Initialization Parameters *(8)* html
- Audit Configuration *(10)* html
- Audit Trail Locations *(4)* html
- Object Level Privileges (Audit Trail) *(1)* html
- Users granted to audit the database *(10)* html
- AUDIT Retention *(1)* html

Audit Analyses

- Audit Events per ErrorMsg *(1)* html pie
- Audit Events per Username *(5)* html
- Audit Events per User/Proxy/External/Global *(5)* html
- Audit Events per Username and Operation *(11)* html
- Audit Events per Username and SysPriv Used *(5)* html
- Audit Events per Instance *(2)* html
- Audit Events per Objects and Operation *(15163)* html
- Audit Events per Day *(5)* html
- Most recent Audit Events *(15293)* html
- Audit Configuration Changes *(0)* html
- Failed Login Attempts *(0)* html
- DDL Actions *(115123)* html
- DML Actions *(0)* html
- User Account Actions *(1)* html
- Schemas being used by multiple applications/users *(0)* html

Fine Grained Audit

- Fine Grained Audit Policies *(0)* html
- FGA Events per Username, Policy and Statement *(0)* html
- FGA Events per Day *(0)* html
- Most recent FGA Events *(0)* html

4/7

Encryption

- Encryption Wallets *(2)* html
- Encryption Keys *(-1)* html
- Encryption Columns *(0)* html
- Encryption Tablespaces *(12)* html
- Encryption Tablespaces 2 *(0)* html
- PL/SQL using DBMS_CRYPTO *(12)* html
- Sensitive Columns Discovery *(2371)* html
- References to Username and Password *(501)* html

Access Control List

- Network ACL *(1)* html
- Network ACL Privileges *(1)* html

Virtual Private Database

- VPD Policies *(105)* html
- VPD Policy Groups *(0)* html
- VPD Policy Contexts *(0)* html
- VPD Relevant Columns *(0)* html
- Users with EXEMPT ACCESS POLICY *(0)* html

SQL Injection

- PL/SQL protected with DBMS_ASSERT *(33)* html
- PL/SQL prone to Sql Injection *(103)* html
- SQL Translations *(-1)* html

Label Security

- Users *(-1)* html
- Users Level *(-1)* html
- Users Lables *(-1)* html
- Users Groups *(-1)* html
- Users Compartments *(-1)* html
- Users Privs *(-1)* html
- Audit Options *(-1)* html
- Compartments *(-1)* html
- Data Labels *(-1)* html
- Groups *(-1)* html
- Group Hierarchy *(-1)* html
- Labels *(-1)* html
- Levels *(-1)* html
- Policies *(-1)* html
- Programs *(-1)* html
- Programs Privs *(-1)* html
- Schema Policies *(-1)* html
- Table Policies *(-1)* html

5/7

Database Vault

- DB Vault *(1)* html
- DB Vault Realms *(-1)* html
- DB Vault Realms authorizations *(-1)* html
- DB Vault Realms Object Grants *(-1)* html
- DB Vault Rules *(-1)* html
- DB Vault Rule Set *(-1)* html
- DB Vault Command Rule *(-1)* html
- DB Vault Roles *(0)* html
- DB Vault Granted Roles *(0)* html
- DB Vault Granted SysPrivs/Roles *(0)* html
- DB Vault Views not in Realm *(-1)* html
- DB Vault Tables granted to Public *(-1)* html
- DB Vault Most Recent Audit Trail *(-1)* html

DBV Configuration Issues Reports

- Command Rule Configuration Issues *(-1)* html
- Rule Set Configuration Issues *(-1)* html
- Realm Authorization Configuration Issues *(-1)* html
- Factor Configuration Issues *(-1)* html
- Identity Configuration Issues *(-1)* html

DBV Enforcement Audit Reports

- Realm Audit Report *(-1)* html
- Command Rule Audit Report *(-1)* html
- Factor Audit Report *(-1)* html
- Label Security Integration Audit *(-1)* html
- Core Database Vault Audit Trail *(-1)* html
- Secure Application Role Audit *(-1)* html

DBV Configuration Changes

- All Database Vault Configuration Changes *(-1)* html
- Realm Configuration Changes *(-1)* html
- Command Rule Configuration Changes *(-1)* html
- Rule Set Configuration Changes *(-1)* html
- Rule Configuration Changes *(-1)* html
- Secure Application Role Configuration Changes *(-1)* html
- Factor Configuration Changes *(-1)* html
- Factor Type Configuration Changes *(-1)* html

Fully Encrypted Database

```
ALTER TABLESPACE SYSTEM ENCRYPTION ONLINE ENCRYPT
FILE_NAME_CONVERT=('system01.dbf','system01_enc.dbf');
```

- To encrypt an entire database, you must encrypt all the tablespaces within this database, including the Oracle-supplied SYSTEM, SYSAUX, UNDO, and TEMP tablespaces
- For a temporary tablespace, drop it and then recreate it as encrypted - do not specify an algorithm
- Oracle recommends that you encrypt the Oracle-supplied tablespaces by using the default tablespace encryption algorithm, AES128

Support for ARIA, SEED, and GOST algorithms

```
ALTER TABLE employee REKEY USING 'GOST256';
```

- By default, Transparent Data Encryption (TDE) Column encryption uses the Advanced Encryption Standard with a 192-bit length cipher key (AES192), and tablespace and database encryption use the 128–bit length cipher key (AES128)
- 12.2 provides advanced security Transparent Data Encryption (TDE) support for these encryption algorithms:
  - SEED (Korea Information Security Agency (KISA) for South Korea
  - ARIA (Academia, Research Institute, and Agency) for South Korea
  - GOST (GOsudarstvennyy STandart) for Russia

Setting Future Tablespaces to be Encrypted

```
ALTER SYSTEM SET ENCRYPT_NEW_TABLESPACES = CLOUD_ONLY;
```

- CLOUD_ONLY transparently encrypts the tablespace in the Cloud using the AES128 algorithm if you do not specify the ENCRYPTION clause of the CREATE TABLESPACE SQL statement: it applies only to an Oracle Cloud environment
- ALWAYS automatically encrypts the tablespace using the AES128 algorithm if you omit the ENCRYPTION clause of CREATE TABLESPACE, for both the Cloud and premises scenarios

Schema Level Data Security Policy

```
EXEC SYS.XS_DATA_SECURITY.ENABLE_OBJECT_POLICY(policy
=>'EMPLOYEES_DS',schema=>'hr',object=>'employees');
```

- Beginning with Oracle Database 12c Release 2 (12.2), Real Application Security introduces schema level privileges, which allows a policy administrator to create, update, and apply a policy in only the granted schema and administer policy enforcement within one application
- This level of policy administration is essential in a Cloud computing scenario where each application may be running under one or more schemas

SYSRAC - Separation of Duty in a RAC

```
GRANT SYSRAC to JULIAN;
```

- SYSRAC is a new role for Oracle Real Application Clusters (Oracle RAC) management
- This administrative privilege is the default mode for connecting to the database by the clusterware agent on behalf of the Oracle RAC utilities such as srvctl
- For example, customers can create a named administrative account and grant only the administrative privileges needed such as SYSRAC and SYSDG to manage both Oracle RAC and Oracle Data Guard configurations

Strong Password Verifiers by Default

`SQLNET.ALLOWED_LOGON_VERSION_SERVER=12a`

- The newer verifiers use salted hashes, modern SHA-1 and SHA-2 hashing algorithms, and mixed-case passwords
- SQLNET.ALLOWED_LOGON_VERSION_SERVER=8 generates all three password versions 10G, 11G, and 12C
- SQLNET.ALLOWED_LOGON_VERSION_SERVER=12 generates both 11G and 12C password versions, and removes the 10G password version
- SQLNET.ALLOWED_LOGON_VERSION_SERVER=12a generates only the 12C password version

Automatic Locking of Inactive User Accounts

```
CREATE PROFILE time_limit LIMIT INACTIVE_ACCOUNT_TIME 60;
```

- Within a user profile, the INACTIVE_ACCOUNT_TIME parameter controls the maximum time that an account can remain unused
- The account is automatically locked if a log in does not occur in the specified number of days
- Locking inactive user accounts prevents attackers from using them to gain access to the database
- The minimum setting is 15 and the maximum is 24855
- The default for INACTIVE_ACCOUNT_TIME is UNLIMITED

Chaitanya Geddam

Oracle Database Security Practice Lead

chaitanya.geddam@accenture.com

Julian Dontcheff

Oracle Technology Practice Executive

julian.dontcheff@accenture.com