NYOUG

#C16LV

ORACLE12C REDACTION
AND
ADVANCED DATA ENCRYPTION
FOR
ROBUST IAM REGULATORY COMPLIANCE

AN INNOVATIVE DATABASE-FOCUSED

INFORMATION SECURITY PARADIGM

SESSION ID: 1343

ANTHONY D. NORIEGA

COLLABORATE16

A>D<N R&D

@anthonydnoriega

anthonydnoriega

COLLABORATE16

AGENDA

- Executive Overview
- Oracle Data Security Strategies
  - Preventive
  - Detective
  - Administrative
- Oracle12c Redaction
- Oracle Transparent Data Encryption (TDE)
- Implementing Oracle Advanced Encryption
  - Via SQL
  - Via Utilities
- Case Studies
- Oracle Data Masking and Subsetting
- Oracle Database Vault
- Oracle Label Security
- Oracle Virtual Private Database (VPD)
- Oracle Audit Vault

#C16LV

A>D<N R&D

The Grid is the cloud. The cloud is the grid...

COLLABORATE16

EXECUTIVE OVERVIEW

Oracle Redaction and Transparent Data Encryption are the most advanced features available in Oracle12c to guarantee optimal database security and preventive data protection, by utilizing a combination of encryption standards and data retrieval methods and policies beyond SQL execution, which enable specialized administrators to fully condition access to private information, using encryption, row-level with either role-driven or label-driven algorithms, and data masking where appropriate and as intended through a database environment configured via supplied Oracle PL/SQL packages, with emphasis on the mechanisms behind this Advance Security option with a few real world proven scenarios.

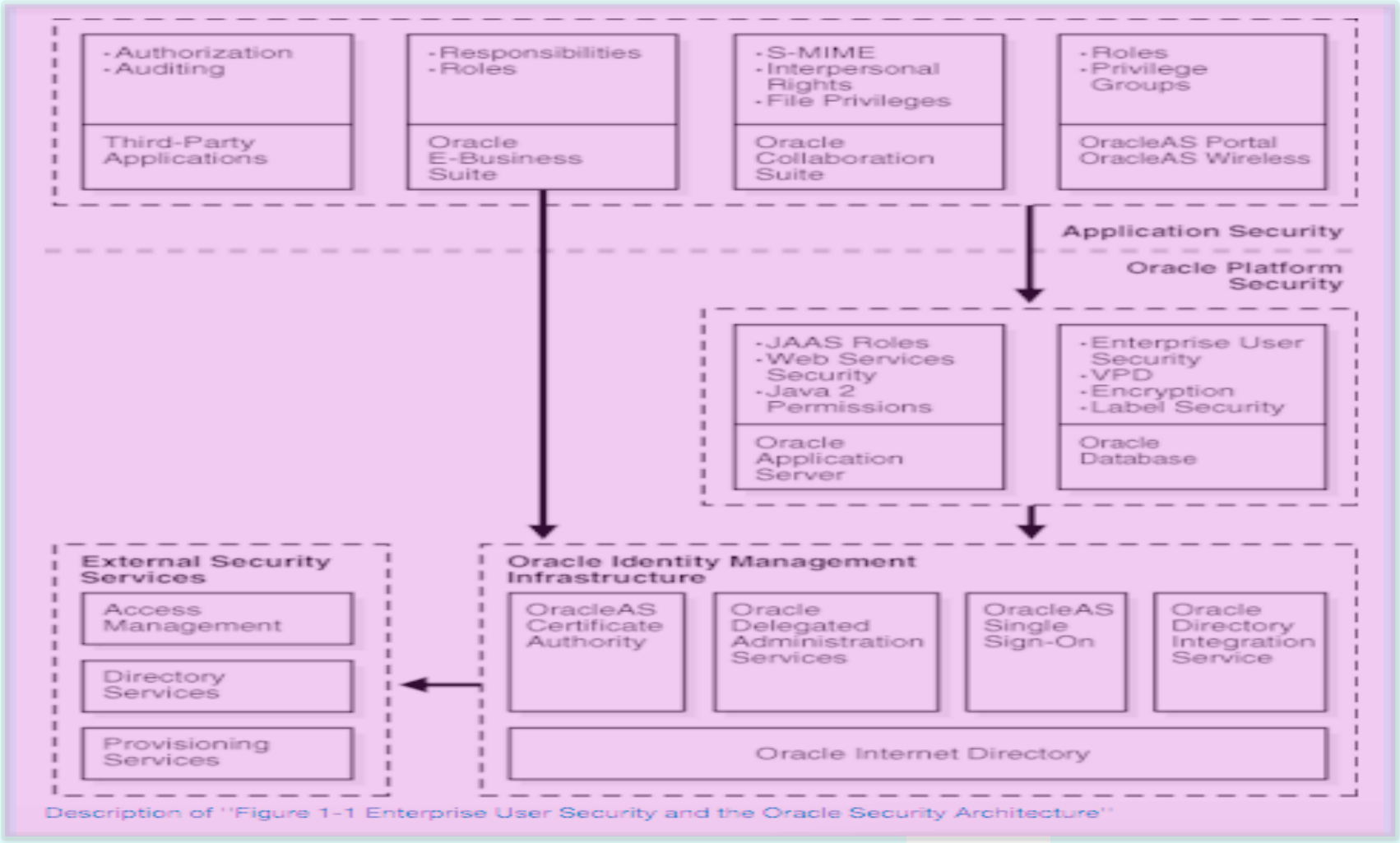
OBJECTIVES

- Provide insightful approaches to use Data Redaction, including encryption, VPD, Label, and Data Masking security strategies for optimal data privacy and security.
- Present the fundamental advanced application scenarios where Oracle Redaction based security is practical and possible.
- Consolidate best practices to overcome, maintain, and optimized this complex security paradigm while minimizing any relevant risk.

ORACLE12C COMPLIANCE-FOCUSED SECURITY MODELS

PREVENTIVE	DETECTIVE	ADMINISTRATIVE
ENCRYPTION	ACTIVITY MONITORING	CONFIDENTIAL DATA PROTECTION
REDACTION AND MASKING	DATABASE FIREWALL	PRIVILEGED ANALYSIS
PRIVILEGED USER CONTROL	AUDITING AND REPORTING	SENSITIVE DATA DISCOVERY
CUSTOMIZED STRATEGIES	CUSTOM SOLUTIONS	CONFIGURATION MANAGEMENT

ORACLE12C COMPLIANCE-FOCUSED USER SECURITY ARCHITECTURE



Description of ''Figure 1-1 Enterprise User Security and the Oracle Security Architecture''

#C16LV

A>D<N R&D

COLLABORATE16

ORACLE ADVANCED SECURITY AND IAM TECHNOLOGIES

#C16LV

A>D<N R&D

The Grid is the cloud. The cloud is the grid...

COLLABORATE16

PREVENTIVE SECURITY STRATEGIES

- Oracle12c Transparent Data Encryption (TDE)
- Oracle12c Redaction
- Oracle Data Masking
- User Privilege Control
  - Oracle Database Vault
  - Oracle Label Security
  - Oracle Virtual Private Database (VPD)
  - Oracle Real Application Security (RAS)

ORACLE12C REDACTION CONCEPTS

- Oracle Data Redaction enables administrators and developers to redact (mask) column data, using full redaction, partial redaction, regular expressions, and random redaction. They can create policies that perform no redaction as well, for testing purposes.
- Data Redaction performs the redaction at runtime, *i.e.*, as the user attempts to view the data. This is ideal for dynamic production systems in which data constantly changes.
- Oracle12c Redaction and Sibling Technologies empower data privacy and information security via a variety of strategies over various security virtual tiers.

ORACLE12C REDACTION CONCEPTS

- While the data is being redacted, Oracle Database is able to process all of the data normally and to preserve the data model's referential integrity constraints.
- Data redaction can help you to comply with industry regulations such as:
  - HIPAA (protecting Private Health Information, PHI)
  - Payment Card Industry Data Security Standard (PCI DSS)
  - Sarbanes-Oxley Act (SOX).

ORACLE12C REDACTION CONCEPTS

Masking and subsetting can be performed on a cloned copy of the original data, eliminating any overhead on production systems. Alternatively, masking and subsetting can be performed during database export, eliminating the need for staging servers. Masking and subsetting can be performed on data in non-Oracle databases by staging the data in an Oracle Database using the relevant Oracle Database Gateway, e.g., Oracle Transparent Gateway for IBM DB2, IBM Informix, Sybase or Microsoft SQL Server.

TYPES OF REDACTION

- **Full redaction:** Feasible on all of the contents of the column data, whose value is based on the data type of the column; *e.g.*, columns of the NUMBER data type can be redacted with zeroes (0) and character data types, with blank spaces.
- **Partial redaction:** as a portion of the column data; *e.g.*, redacting most of a Social Security number with asterisks (*), except for the last 4 digits.

TYPES OF REDACTION

- **Regular expressions:** Using regular expressions in both full and partial redaction. This allows to redact data based on a search pattern for the data; *e.g.*, redacting specific phone numbers or email addresses in the database.
- **Random redaction:** in which the redacted data queried appears as randomly generated values each time it is displayed, depending on the data type of the column.
- **No redaction:** Useful to test the internal operation of redaction policies; practical in non-production environments.

ORACLE12C REDACTION EXAMPLES

FULL REDACTION

```
function_type    => DBMS_REDACT.FULL
```

REGULAR EXPRESSION REDACTION

SEARCH PATTERN:

```
regexp_pattern       => '(.+)@(.+\.[A-Za-z]{2,4})'
```

REPLACEMENT STRING:

```
regexp_replace_string  => '[redacted]@\2'
```

STARTING POSITION IN STRING:

```
regexp_position      => DBMS_REDACT.RE_BEGINNING
```

KIND OF SEARCH OR REPLACE OPERATION:

```
regexp_occurrence     => DBMS_REDACT.RE_ALL
```

RANDOMIZED REDACTION

```
function_type    => DBMS_REDACT.RANDOM
```

PARTIAL REDACTION EXAMPLES

CHARACTER DATATYPES

XXX-XX-7890 function_parameters => DBMS_REDACT.REDACT_US_SSN_F5,

*****-**-1234 function_parameters => 'VVVFVVFVVVV,VVV-VV-VVVV,*,1,5',**

NUMBER DATATYPES

XXXXX7890 function_parameters =>
DBMS_REDACT.REDACT_NUM_US_SSN_F5,

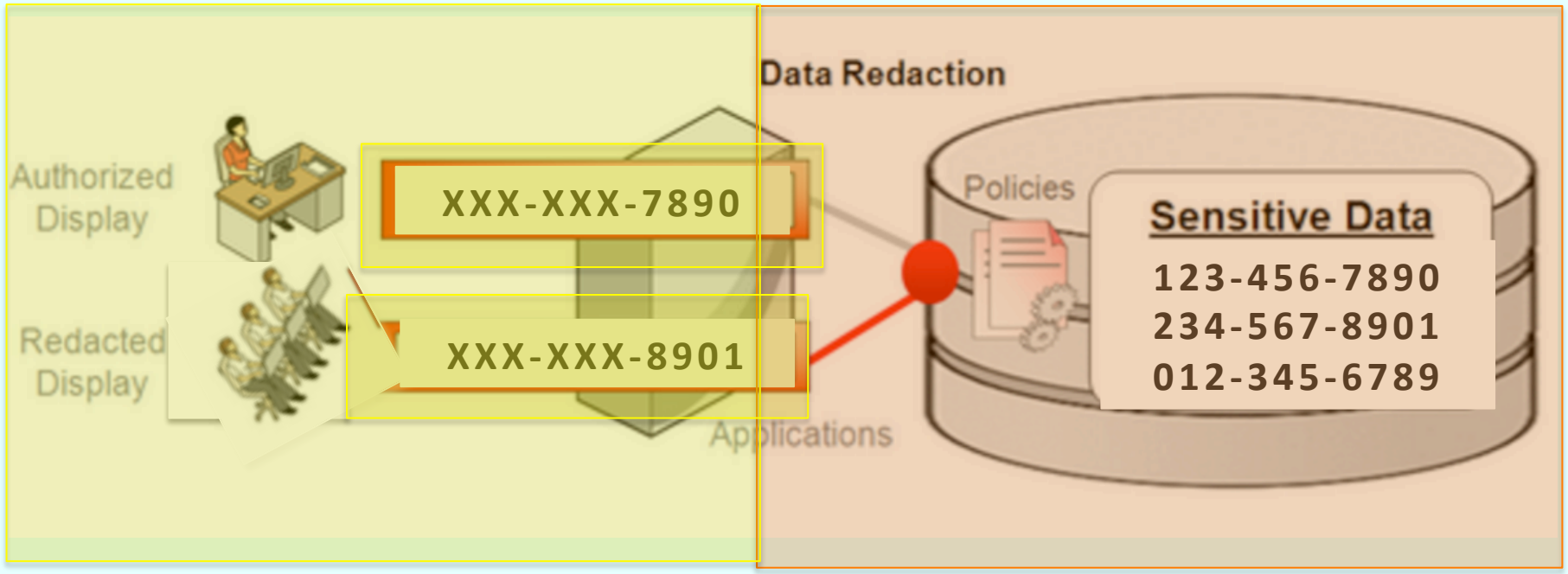
999991234 function_parameters => '9,1,5',

DATETIME DATATYPES

02-OCT-14 15.21.50.000000 AM function_parameters => 'Md02YHMS',

01-JAN-15 14.33.40.000000 AM function_parameters => 'm12DYHMS',

ORACLE12C REDACTED VIEWS



ORACLE12C REDACTION EXAMPLES

```
DECLARE
    newer_red_blob BLOB;
BEGIN
        DBMS_LOB.CREATETEMPORARY(newer_red_blob, TRUE);
        DBMS_LOB.WRITE( newer_red_blob, 10, 1,
                                UTL_RAW.CAST_TO_RAW('[redacted]')
                               );
        DBMS_REDACT.update_full_redaction_values(
                            blob_val =>  newer_red_blob);
        DBMS_LOB.FREETEMPORARY(newer_red_blob);
EXCEPTION
WHEN OTHERS THEN
        DBMS_OUTPUT.put_line(SQLERRM);
END;
```

ORACLE12C REDACTION POLICIES

POLICY	FUNCTIONALITY
DBMS_REDACT.ADD_POLICY	Adds a Data Redaction policy to a table or view
DBMS_REDACT.ALTER_POLICY	Modifies a Data Redaction policy
DBMS_REDACT.UPDATE_FULL_REDACTION_VALUES	Globally updates the full redaction value for a given data type. You must restart the database instance before the updated values can be used.
DBMS_REDACT.ENABLE_POLICY	Enables a Data Redaction policy
DBMS_REDACT.DISABLE_POLICY	Disables a Data Redaction policy
DBMS_REDACT.DROP_POLICY	Drops a Data Redaction policy

ORACLE12C REDACTION EXAMPLES

```
BEGIN
 DBMS_REDACT.ADD_POLICY(
     object_schema           => 'HR',
     object_name             => 'PS_EMPLOYEES',
     column_name             => 'SSN',
     policy_name             => 'redact_emp_ssn5',
     function_type           => DBMS_REDACT.PARTIAL,
     function_parameters     => DBMS_REDACT.REDACT_US_SSN_F5,
     expression              => '1=1',
     policy_description      => 'Partially redacts first 5 digits in SSN',
     column_description      => 'SSN has Social Security numbers');
EXCEPTION
WHEN OTHERS THEN
      DBMS_OUTPUT.put_line(SQLERRM);
END;
```

ORACLE12C REDACTION EXAMPLES

```
BEGIN
        DBMS_REDACT.ADD_POLICY(
            object_schema        => 'HR',
            object_name          => 'PS_BENEFITS',
            column_name          => 'birth_date',
            policy_name          => 'redact_emp_bdate',
            function_type        => DBMS_REDACT.PARTIAL,
            function_parameters => 'mdy2016HMS',
            expression           => '1=1',
            policy_description   => 'Replaces birth year with 2016',
            column_description  => 'birth_date contains
            employees's birthdate');
EXCEPTION
WHEN OTHERS THEN
            DBMS_OUTPUT.put_line(SQLERRM);
END;
```

ORACLE12C REDACTION EXAMPLES

```
BEGIN
        DBMS_REDACT.ALTER_POLICY(
            object_schema => 'HR',
            object_name    => 'PS_PERSONAL_DATA',
            policy_name    => 'hr_emp_payroll',
            action             => DBMS_REDACT.MODIFY_EXPRESSION,
            expression       =>
        'SYS_CONTEXT("USERENV","SESSION_USER") != "HR"');
EXCEPTION
WHEN OTHERS THEN
   RAISE_APPLICATION_ERROR(-20101, 'Invalid Access. ');
END;
```

ORACLE12C REDACTION EXAMPLES

```
BEGIN
        DBMS_REDACT.ALTER_POLICY(
        object_schema       => 'HR',
        object_name         => 'PS_EMPLOYEES',
        policy_name         => 'redact_emp_ids',
        action              => DBMS_REDACT.ADD_COLUMN,
        column_name         => ‘CARD_ID_NUM',
        function_type       => DBMS_REDACT.FULL,
        function_parameters => '',
        expression           =>
        'SYS_CONTEXT("SYS_SESSION_ROLES","ADM") = "TRUE"');
   WHEN OTHERS THEN
        RAISE_APPLICATION_ERROR(-20101, 'Unauthorized Profile. ');
END;
```

ORACLE12C REDACTION EXAMPLES

```
BEGIN
        DBMS_REDACT.DISABLE_POLICY (
                object_schema  => 'HR',
                object_name    => 'PS_EMPLOYEES',
                policy_name    => 'hr_emp_payroll'
                );
END;

BEGIN
        DBMS_REDACT.ENABLE_POLICY (
                object_schema  => 'HR',
                object_name    => 'PS_EMPLOYEES',
                policy_name    => 'hr_emp_payroll'
                );
END;
```

SIBLING TECHNOLOGIES

- Oracle Transparent Data Encryption (TDE)
- Oracle Virtual Private Database (VPD)
- Oracle Label Security
- Oracle Database Vault
- Oracle Data Masking
- Oracle Audit Vault

ORACLE12C TDE CONCEPTS

- Oracle12c TDE attains an outstanding level of data protection and data privacy. This session presents a quick and efficient way to attain the best from Oracle12c TDE with any major obfuscation, introducing an agile model to optimal encryption with Oracle TDE, including control on network processes under TCP/IP, HTTP, and multi-VPN, operating system authentication, operating system level encryption, and complex network topology environments.
- It is critical to elucidate Oracle Transparent Data Encryption by eliminating complexity myths and establishing best practices to attain optimal data protection robustness and system reliability while minimizing risk and fear.

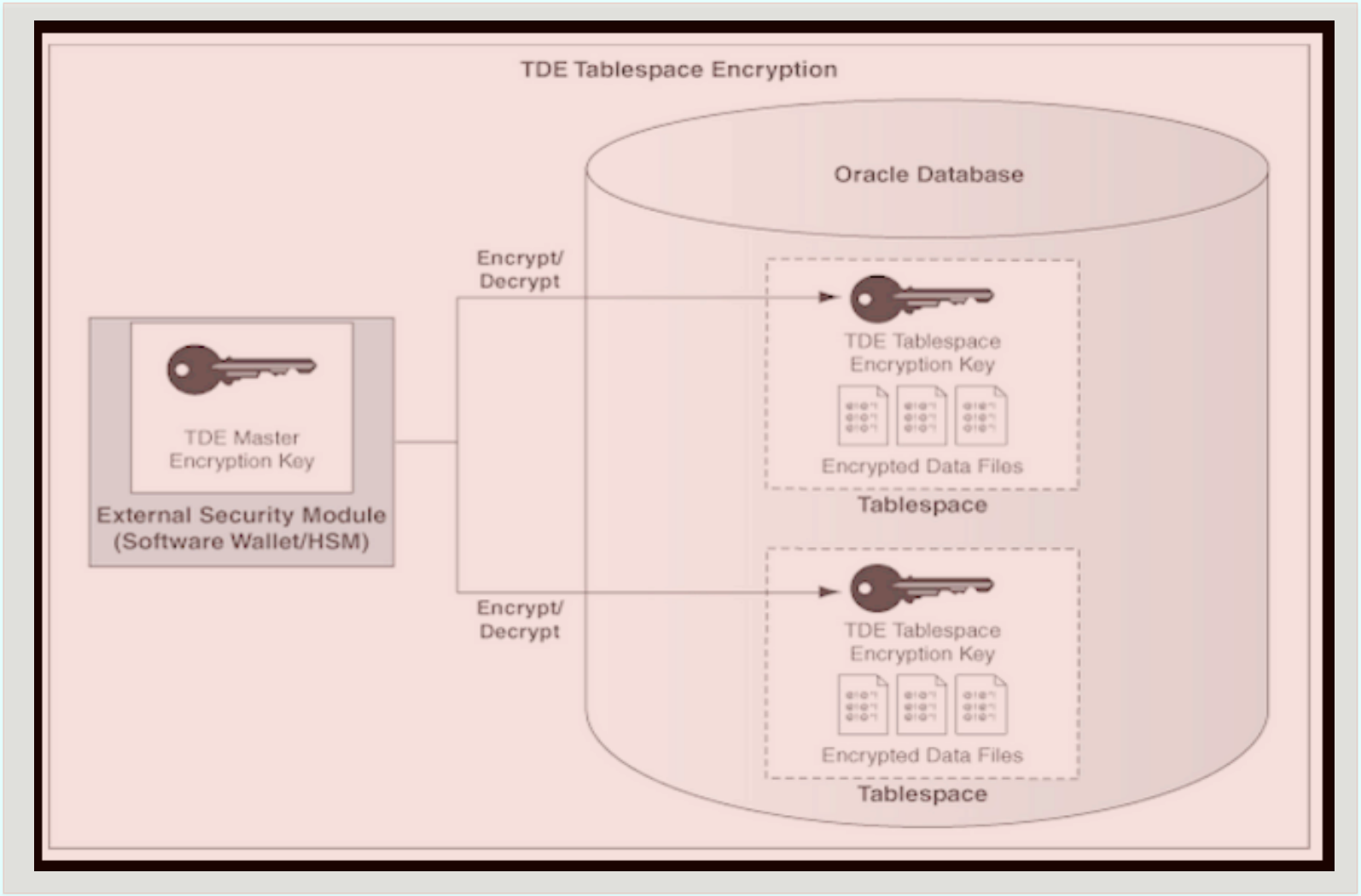
ORACLE12C TDE CONCEPTS

- Encrypting data includes the following components:
- An algorithm to encrypt the data. Oracle Databases use the encryption algorithm to encrypt and decrypt data, e.g., Advanced Encryption Standard (AES) encryption algorithm, already approved by the National Institute of Standards and Technology (NIST).
- A key to encrypt and decrypt data.
- You can encrypt individual table columns or an entire tablespace. V$ENCRYPTED_TABLESPACES and DBA_ENCRYPTED_COLUMNS are useful data dictionary views to verify the encryption options being used.

ORACLE12C TDE CONCEPTS

- Oracle Transparent Data Encryption (TDE) technology utilizes a variety of methods and techniques in order to encrypt a database at both the logical and physical object levels, and provides support for a variety of options such as:
  - Encryption domain instantiation (SALT)
  - Wallet-driven encryption
  - Encryption methods and models
  - Multiple Key Encryption Support
  - A variety of encryption algorithms, such as AES, 3DES, and SHA1, among others.

ORACLE12C TDE CONCEPTS



ORACLE12C TDE CONCEPTS

```
# sqlnet.ora Network Configuration File:
C:\app\oracle\product\12.1.0\dbhome_1\network\admin\sqlnet.ora
# Generated by Oracle configuration tools.

# This file is actually generated by netca. But if customers choose to
# install "Software Only", this file wont exist and without the native
# authentication, they will not be able to connect to the database on NT.

SQLNET.AUTHENTICATION_SERVICES= (NTS)

NAMES.DIRECTORY_PATH= (TNSNAMES, EZCONNECT)

SSL_CLIENT_VERSION = 0

SSL_VERSION = 1.0

NAMES.DIRECTORY_PATH= (TNSNAMES)

SSL_CLIENT_AUTHENTICATION = FALSE

SQLNET.INBOUND_CONNECT_TIMEOUT = 0

ADR_BASE = C:\app\oracle\product\12.1.0\dbhome_1\log

#SQLNET.WALLET_OVERRIDE = FALSE

WALLET_LOCATION =
  (SOURCE =
    (METHOD = FILE
    (METHOD_DATA =
      (DIRECTORY = C:\app\oracle\product\12.1.0\dbhome_1\NETWORK\ADMIN)
    )
  )
```

ORACLE12C TDE ACTIONS

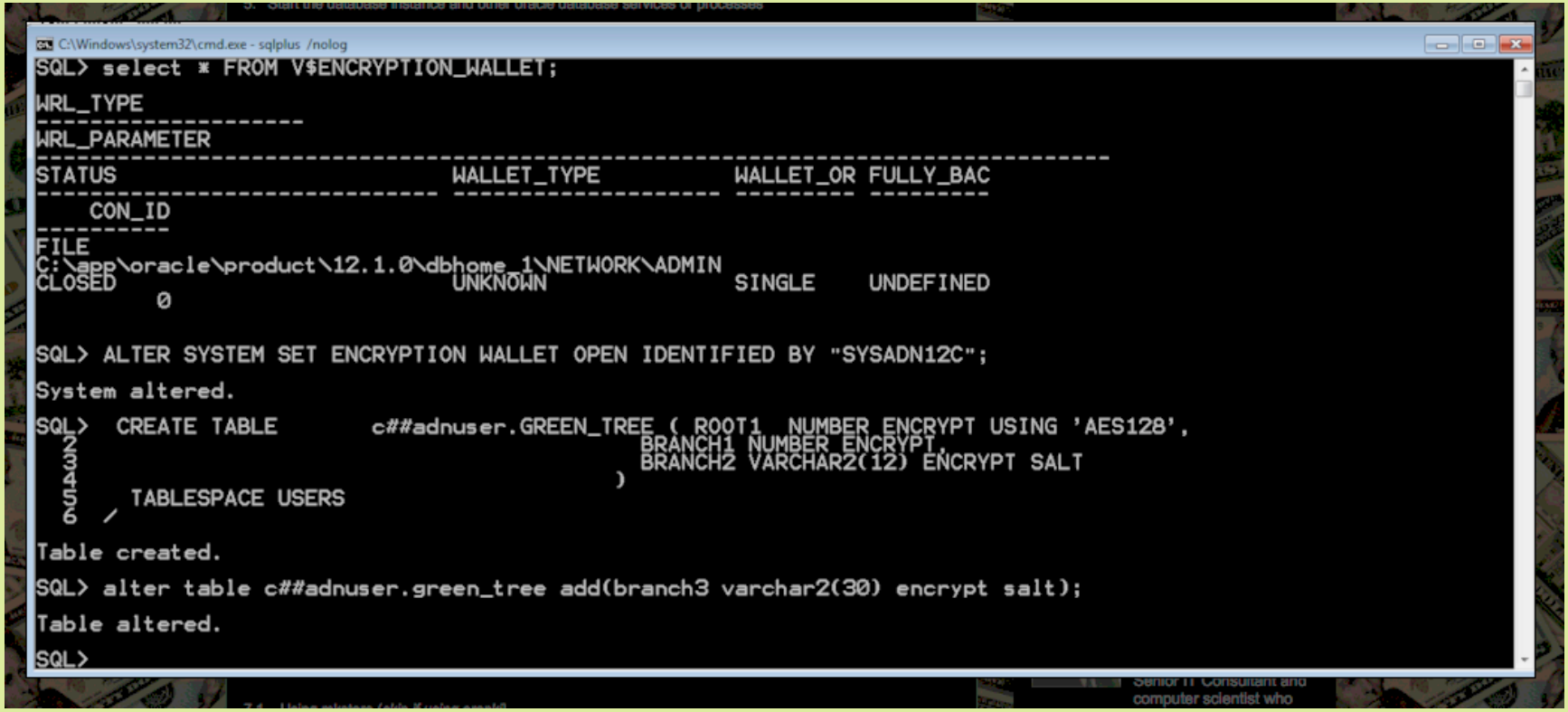
- Encrypting with SQL
  - ALTER SYSTEM SET KEY IDENTIFIED BY "Password";
- Encrypting with Utilities
- mkstore
  - mkstore –wrl "C:\app\oracle\product\12.1.0\dbhome_1\NETWORK\ADMIN" –create
  - mkstore –wrl . –createCredential {CredentialString} {dBUserName} [dbUserPwd}
  - mkstore –wrl –createCredential KEYHOLDER1 orcldba "orcldbapassword"
- orapki
  - orapki wallet create –wallet wallet
  - orapki wallet create –wallet . auto_login_local

ORACLE12C TDE ACTIONS

```
C:\batch>set ORACLE_SID=ADN12C

C:\batch>sqlplus /nolog

SQL*Plus: Release 12.1.0.1.0 Production on Sun Sep 1 03:15:06 2013

Copyright (c) 1982, 2013, Oracle.  All rights reserved.

SQL> connect sys@adn12c as sysdba
Enter password:
Connected.
SQL> ALTER SYSTEM SET KEY IDENTIFIED BY "SYSADN12C";

System altered.

SQL>
```

ENCRYPTING THE DATABASE WITH SQL

ORACLE12C TDE ACTIONS



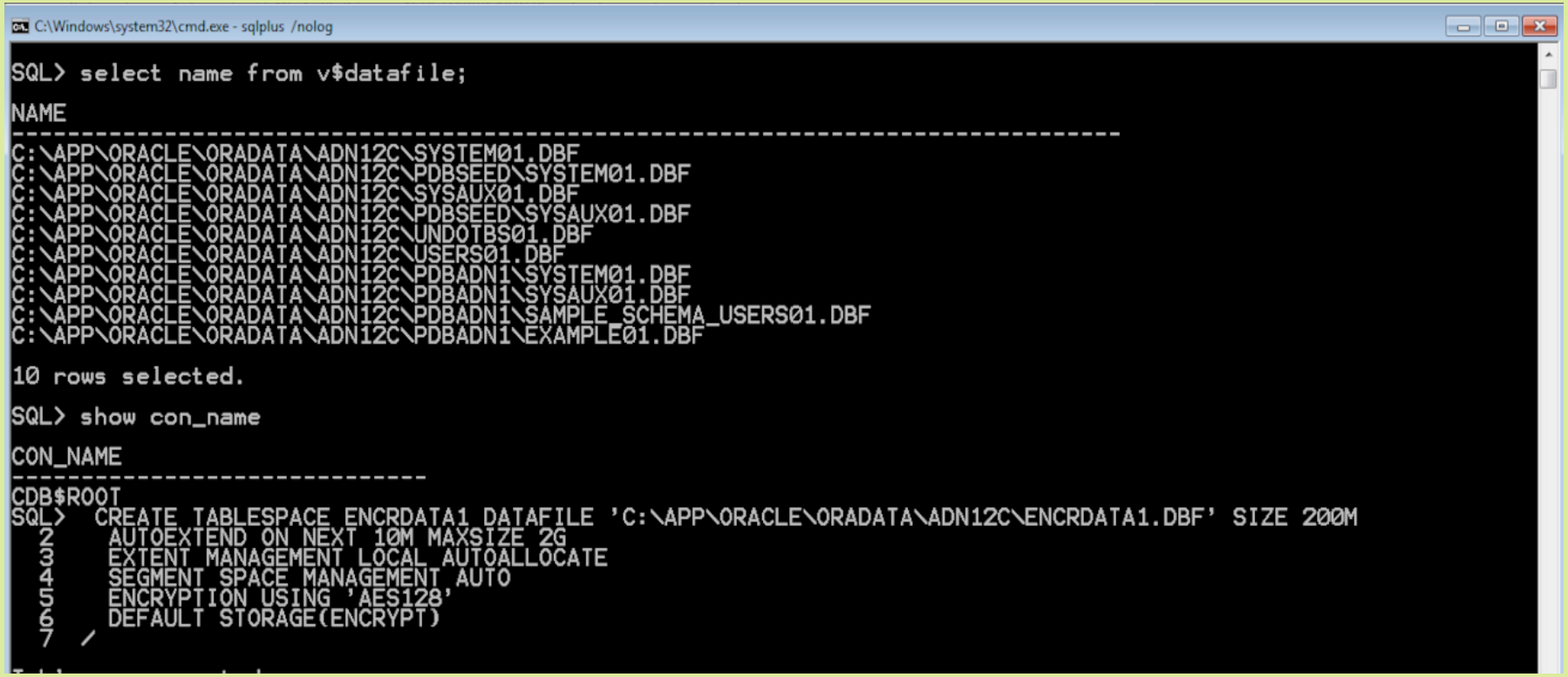
ENCRYPTING THE DATABASE WITH SQL

#C16LV

A>D<N R&D

COLLABORATE16

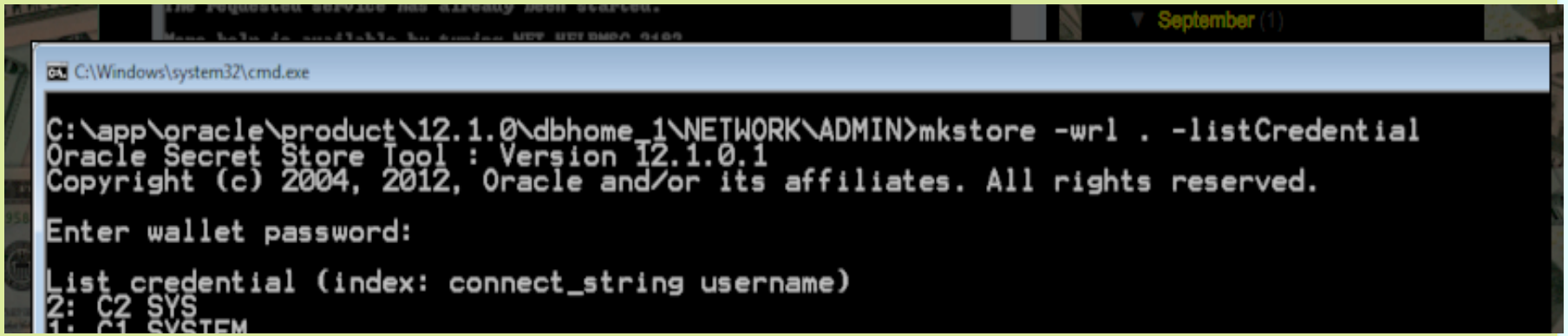
ORACLE12C TDE ACTIONS



TABLESPACE ENCRYPTION

ORACLE12C TDE ACTIONS

```
C:\app\oracle\product\12.1.0\dbhome_1\NETWORK\ADMIN>mkstore -wrl . -createCredential C1 SYSTEM "SYSADN12C"
Oracle Secret Store Tool : Version 12.1.0.1
Copyright (c) 2004, 2012, Oracle and/or its affiliates. All rights reserved.

Enter wallet password:

Create credential oracle.security.client.connect_string1
C:\app\oracle\product\12.1.0\dbhome_1\NETWORK\ADMIN>
```



CREATING AND LISTING CREDENTIALS WITH MKSTORE

ORACLE12C TDE ACTIONS


```
SQL> select * from v$encryption_wallet;

WRL_TYPE
--------------------
WRL_PARAMETER
------------------------------------------------------------------------------
STATUS                         WALLET_TYPE          WALLET_OR FULLY_BAC
------------------------------ -------------------- --------- ---------
    CON_ID
----------
FILE
C:\app\oracle\product\12.1.0\dbhome_1\NETWORK\ADMIN
OPEN                           PASSWORD             SINGLE    NO
         0

exit;
```

QUERYING THE ENCRYPTION WALLET METADATA (V$ENCRYPTION_WALLET)

ORACLE12C TDE ACTIONS

AUTOMATICALLY OPENING THE WALLET WITH A STARTUP TRIGGER

#C16LV

A>D<N R & D

COLLABORATE16

OTDE TECHNOLOGY INTEGRATION

Database Products and Technologies	Example Points of Integration	TDE Support
Exadata	Exadata Smart Scans, Exadata Hybrid Columnar Compression	✓
Database Compression	Oracle Advanced Compression	✓
Backup and Restore	Oracle Recovery Manager (RMAN), Oracle Secure Backup	✓
Export and Import	Oracle Data Pump Export and Import	✓
High-Availability Clusters	Oracle Real Application Clusters (RAC), Oracle Active Data Guard	✓
Storage Management	Oracle Automatic Storage Management (ASM)	✓
Database Replication	Oracle GoldenGate	✓

ORACLE12C TDE TIPS

- In complex network environments, such as those using RAC or Oracle High Availability Services (OHAS), ASM, Oracle12c Clusterware, it is recommended to control or automate encryption via SQL rather than using utilities. Utilities require a careful plan-ahead strategy.
- Some convergence may occur with Oracle Restart, which may be deprecated in future releases of Oracle Clusterware and Grid Infrastructure, so SQL is better.
- Preserving and Securing the Master and all Encryption Keys is important for reliability and database high availability.
- The **mkstore** utility performs several actions of the **orapki** utility in one single command.

ORACLE12C TDE BUSINESS STRATEGIES

- Method or Resource Used
  - SQL-Driven
  - Utility-Driven (mkstore, orapki)
- Logical Object Scope
  - Tablespace Encryption
  - Table Encryption
    - Full table
    - Selected Columns Encryption
- Encryption Extensions
  - Encrypted Backup with RMAN
  - Integration with other Oracle technologies, namely: VPD, Label, Vault, Redaction, Data Masking and Subsetting.

ORACLE12C TDE CASE STUDIES

- Case Studies
  - HIPAA
  - Banks and other Financial Institutions
  - MasterCard

OTHER ORACLE12C PREVENTIVE SECURITY TECHNOLOGIES

#C16LV

A>D<N R&D

The Grid is the cloud. The cloud is the grid...

COLLABORATE16

ORACLE12C DATA MASKING

- **Oracle Data Masking and Subsetting helps database customers improve security, accelerate compliance, and reduce IT costs by sanitizing copies of production data for testing, development, and other activities and by easily discarding unnecessary data.**

Oracle Data Masking and Subsetting enables entire copies or subsets of application data to be extracted from the database, obfuscated, and shared with partners inside and outside of the business. The integrity of the database is preserved assuring the continuity of the applications.

ORACLE DATA MASKING

- Oracle Data Masking and Subsetting provides sophisticated masking transformations.
- When masking formats are considered as building blocks of a data masking definition, masking transformations align these masking formats according to the varied business requirements.

ORACLE DATA MASKING TRANSFORMATIONS

- Conditional Masking: provides the ability to arrange masking formats according to different conditions.
- Compound Masking (also known as grouping option): masks related columns as a group to ensure that the data being masked across the related columns retain the same relationship.
- Deterministic/Consistent Masking: generates consistent outputs for a given input across various databases (useful for data and system integrity across multiple applications in a SSO environment).
- Shuffle: allows the fields within a column to be shuffled in a random manner. Useful to break the one-to-one mapping between sensitive data elements.

ORACLE DATA MASKING TRANSFORMATIONS

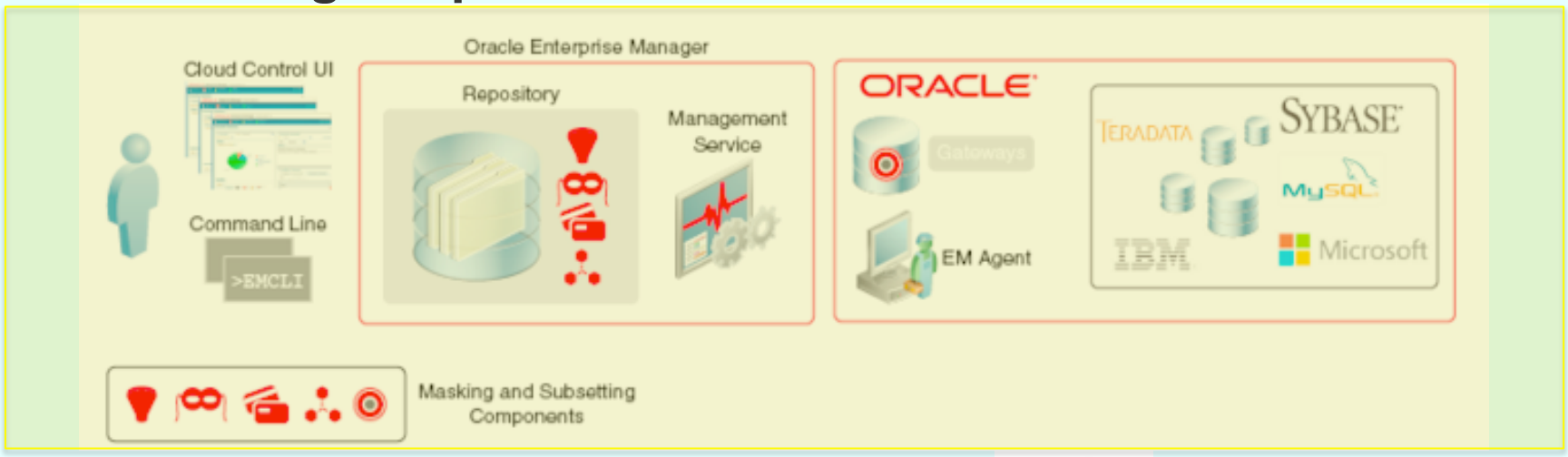
- Key-based reversible masking (also known as Encrypt Format): encrypts and decrypts the original data using a secure key string, while preserving the format of the input data using the 3DES algorithm, and it is helpful for business masking needs).
- Format Preserving Randomization (also known as Auto Mask Format): randomizes the data, preserving the input length, position of the characters and numbers, case of the character (upper or lower), and special characters in the input.

ORACLE DATA MASKING AND SUBSETTING TECHNIQUES

- Oracle Data Masking and Subsetting simplifies subsetting through its easy-to-define goal-based and condition-based subsetting techniques.
- Goal-based subsetting: Data is subsetted based on goals. A goal can be a relative table size.
- Condition-based subsetting: Data is subsetted based on conditions, by specifying the “SQL WHERE clause”, which supports bind variables.
- Conditions can refer to excluding a certain year range or a specific territory or region in a demographic or geographic database.

ODM APPLICATION TEMPLATES

- Oracle Data Masking Application Templates deliver pre-identified sensitive columns, their relationships, and industry-standard best practice masking techniques out-of-the box for packaged applications such as:
  - Oracle E-Business Suite
  - Oracle Fusion Applications.
- Use the Self Update feature to get the latest masking and subsetting templates available from Oracle.



ORACLE12C DATABASE VAULT

- Oracle Database Vault can be used to restrict administrative access to an Oracle database utilizing a fine-grained approach.

ORACLE12C DATABASE VAULT SECURITY FEATURES

- Strong Authentication
- Network Encryption
- Real Application Security
- Unified Auditing
- Secure External Password Store
- Virtual Private Database
- Traditional Database Auditing
- Proxy Authentication
- Enterprise User Security
- Secure Application Roles
- Fine Grained Auditing

ORACLE12C LABEL SECURITY

Oracle Label Security Policy components:

- Labels. Labels for data and users, along with authorizations for users and program units, govern access to specified protected objects. Labels are composed of the following:
  - Levels. Levels indicate the type of sensitivity that you want to assign to the row, for example, SENSITIVE or HIGHLY SENSITIVE.
  - Compartments. (Optional) Data can have the same level (Public, Confidential and Secret), but can belong to different projects inside a company.
  - Groups. (Optional) Groups identify organizations owning or accessing the data, for example, UK, US, Asia, Europe.
  - Policy. A policy is a name associated with these labels, rules, and authorizations.

ORACLE12C VPD AND RAS

- Oracle VPD and RAS Benefits include:
  - End-user session propagation to the database
  - Data security based upon application users, role, privileges, and various relationships
  - Audit of end-user activity
  - Simplified administration with declarative security
- RAS permits developers to:
  - Define the data security policy in the database based on business objects
  - Associate custom application privileges to authorize application-level operations on these business objects
  - Provision authorization to application users and roles which can be managed in LDAP compliant identity stores as well as in the database.

TECHNOLOGICAL CONCERNS

- Scope of solution (implementation level and completeness) in the market
- Oracle Users awareness and attitude towards preventive security technologies
- Market Leadership.

CONCLUSIONS

Functional, Technical, and Business Benefits and Motivation

#C16LV

A>D<N R&D

The Grid is the cloud. The cloud is the grid...

COLLABORATE16

ORACLE12C IAM SUITE VS. POINT-FOCUSED SOLUTIONS

GENERIC BENEFIT	KEY BENEFITS	ORACLE IAM ADVANTAGE
INCREASE END-USER PRODUCTIVITY	Emergency Access and End-User Self-Service	11% faster Emergency Access; 30% faster end-user self-service
REDUCED RISK	End-user Access Suspension, revoking, deprovisioning	46% faster
ENHANCED AGILITY	Faster application integration with IAM Infrastructure, and faster integration for a new user role into the solution	64% faster application integration; 73% faster new user role integration
ENHANCED SECURITY AND COMPLIANCE	Minimized unauthorized access and audit deficiencies	14% fewer unauthorized access; 30% fewer audit deficiencies
REDUCED TCO (FOR BEST ROI)	Reduced TCO of IAM initiatives	48% lower

ORACLE12C SECURITY COMPARISON

Comparing Virtual Private Database, Label Security, and Data Redaction

Feature	VPD	OLS	Data Redaction
Provides full masking, partial masking, and random masking	No	No	Yes
Redacts data in real-time, as the user is accessing it	No	No	Yes
Provides row-level security	Yes	Yes	No
Provides column-level security (column masking)	Yes	No	Yes
Binds a user-defined PL/SQL package to a table, view, or synonym	Yes	No[1]	No
Modifies SQL by dynamically adding a WHERE clause returned from the PL/SQL procedures	Yes	No	No
Restricts database operations by privileged users[2]	No	No	No
Controls access to a set of rows based on the sensitivity label of the row and the security level of the user	No	Yes	No
Adds a column (optionally hidden) designed to store sensitivity labels for rows in the protected table[3]	No	Yes	No
Provides a user account to manage its administration	No[4]	Yes[5]	No
Provides pre-defined PL/SQL packages for row-level security	No	Yes	No
Is provided in the default installation of Oracle Database	Yes	Yes	Yes
Is provided as an additional option to Oracle Database and must be licensed	No	No	Yes

CONCLUDING REMARKS

Utilizing Oracle12c Enterprise Security Suite leads to:

- **Improved data protection with higher reliability and model robustness**
- **Risk minimization on data security and data privacy, e.g., Private Health Information (PHI) in HIPAA regulatory compliance**
- **Reduced number of confidential data exposure and relevant vulnerabilities**
- **Optimal Total Cost of Ownership (TCO), (when utilizing an integrated solution), positively affecting both CAPEX and OPEX for the best ROI.**

QUESTIONS AND ANSWERS


#C16LV
PLEASE COMPLETE YOUR SURVEY
SESSION # 1343
ONLINE AT:
https://collaborate.zerista.com/