

**100%** Money Back  
**Guarantee**

**Vendor:** Oracle

**Exam Code:** 1Z0-528

**Exam Name:** Oracle Database 11g Security Essentials

**Version:** Demo

**QUESTION 1**

Which of the following tasks is the first task to perform when implementing Oracle Database Vault?

- A. Create command rules
- B. Create command rule sets
- C. Create protection realms
- D. Define master keys

**Correct Answer: C**

**Explanation****Explanation/Reference:**

Explanation:

From Vault Administrator Guide

What Are Realms?

...

After you create a realm, you can register a set of schema objects or roles (secured objects) for realm protection and authorize a set of users or roles to access the secured objects.

...

**QUESTION 2**

Why would you use an auto-open wallet instead of a standard encryption wallet?

- A. To save on storage space
- B. To increase the level of security on your encrypted data
- C. To avoid manual intervention to allow access to encrypted data after an automatic system restart
- D. You must use an auto-open wallet with tablespace-based Transparent Data Encryption (TDE)

**Correct Answer: C**

**Explanation****Explanation/Reference:**

Explanation:

Because wallet is closed after restart and it has to be opened again for using TDE. You must enable auto login if you want single sign-on access to multiple Oracle databases: such access is normally disabled, by default. Sometimes the obfuscated auto login wallets are called "SSO wallets" because they support single sign-on capability.

**QUESTION 3**

Which two of the following features or options give you the ability to set fine-grained access control?

- A. Advanced Security Option
- B. Oracle Database Vault
- C. Oracle Audit Vault
- D. Virtual Private Database
- E. Oracle Label Security

**Correct Answer: AE**

**Explanation****Explanation/Reference:**

Explanation:

Label Security is used to implement security based on data values in individual rows

**QUESTION 4**

When will the changes in Database Vault access permissions take effect?

- A. Immediately

- B. The next time the database server is stopped and started
- C. After the next database backup
- D. After an ALTER SYSTEM DBV is issued

**Correct Answer:** A

**Explanation**

**Explanation/Reference:**

Explanation:

Changes to Database Vault permissions take effect immediately.

#### **QUESTION 5**

Your customer wants to add an additional level of security to their data, based on values in individual records.

They can specify a group of records for access control with a simple WHERE clause. Which security feature or option will give them this capability for the lowest cost?

- A. Advanced Security Option
- B. Oracle Database Vault
- C. Oracle Audit Vault
- D. Oracle Data Masking Pack
- E. Virtual Private Database
- F. Oracle Label Security

**Correct Answer:** E

**Explanation**

**Explanation/Reference:**

Explanation:

Oracle Virtual Private Database (VPD). This feature restricts data access by creating a policy that enforces a WHERE clause for all SQL statements that query the database. You create and manage the VPD policy at the database table or view level, which means that you do not modify the applications that access the database.

#### **QUESTION 6**

Which of the following tasks is the first task to perform when implementing Oracle Database Vault?

- A. Create command rules
- B. Create command rule sets
- C. Create protection realms
- D. Define master keys

**Correct Answer:** C

**Explanation**

**Explanation/Reference:**

Explanation:

After you create a realm, you can register a set of schema objects or roles (secured objects) for realm protection and authorize a set of users or roles to access the secured objects.

#### **QUESTION 7**

Which of the following is NOT a responsibility defined within Oracle Database Vault?

- A. Account Management
- B. Database Administration
- C. Security Administration
- D. RAC Administration

**Correct Answer:** B

## Explanation

### Explanation/Reference:

Explanation:

You can add/delete and configure Vault on RAC nodes. Can manage accounts and security.

### QUESTION 8

What data masking technique ensures that a customer number gets masked to the same value across all databases?

- A. Condition-based masking
- B. Compound masking
- C. Deterministic masking
- D. Relationship masking

**Correct Answer: D**

### Explanation

### Explanation/Reference:

Explanation:

According to labels

### QUESTION 9

When implementing Transparent Data Encryption (TDE), which of the following answers describes the correct order of the listed operations?

- A. Create a wallet, create a master key, and create tables that contain encrypted columns.
- B. Create tables that contain encrypted columns, create a wallet, create a master key, and open the wallet.
- C. Create a wallet, open the wallet, create a master key, and create tables that contain encrypted columns.
- D. Create a master key, create a wallet, open the wallet, and create tables that contain encrypted columns.

**Correct Answer: A**

### Explanation

### Explanation/Reference:

Explanation:

Step 2: Create the Wallet

To create the wallet, use the ALTER SYSTEM SQL statement. By default, the Oracle wallet stores a history of retired master keys, which enables you to change them and still be able to decrypt data that was encrypted under an old master key ...

ALTER SYSTEM SET ENCRYPTION KEY IDENTIFIED BY "password"; This statement generates the wallet with a new encryption key and sets it as the current transparent data encryption master key.

...

Immediately after you create the wallet key, the wallet is open, and you are ready to start encrypting data.

### QUESTION 10

When is Transparent Data Encryption invoked?

- A. When triggered by an administrator
- B. During all I/O operations
- C. Automatically in batches
- D. Only when the data is initially loaded into the database

**Correct Answer: B**

### Explanation

### Explanation/Reference:

Explanation:  
How Transparent Data Encryption Works

...

Afterward, when a user enters data into an encrypted column, Oracle Database performs the following steps:

- 1.Retrieves the master key from the wallet.
- 2.Decrypts the encryption key of the table from the data dictionary.
- 3.Uses the encryption key to encrypt the data the user entered into the encrypted column.
- 4.Stores the data in encrypted format in the database.

#### **QUESTION 11**

Oracle Data Masking Pack allows you to perform which three actions?

- A. Use predefined mask formats
- B. Back up your data
- C. Preview sample data before masking
- D. Define application masking templates

**Correct Answer:** ACD

**Explanation**

**Explanation/Reference:**

Explanation:

It's not a backup solution but it has an opportunity to share data, where sensitive information is masked.

#### **QUESTION 12**

Based on which four factors can a Oracle Database Vault prevent access?

- A. Time of day
- B. IP address
- C. Program name
- D. Custom-designed factor
- E. Values in a column

**Correct Answer:** ABCD

**Explanation**

**Explanation/Reference:**

Explanation:

With Database Vault organizations can define authorization rules based on internal and external factors, such as ip address, time of day, application being used, authentication type, etc. Database Vault rules can be associated with over two dozen individual database commands, such as create table, create view, drop table and comes with many built-in factors, all of which can be extended via APIs

#### **QUESTION 13**

Which of the following requires values in a specific column in targeted tables?

- A. Database Vault realms
- B. Database Vault command rules
- C. Virtual Private Database
- D. Label Security

**Correct Answer:** C

**Explanation**

**Explanation/Reference:**

Explanation:

VPD Provides column-level security (column masking)

**QUESTION 14**

To implement a rigorous separation of duties policy, you should have separate named accounts defined for which three of the following areas?

- A. Database account management
- B. Database security management
- C. Batch users
- D. Backup

**Correct Answer:** ABD

**Explanation****Explanation/Reference:**

Explanation:

Oracle Database Vault defines the following main responsibilities:

Account management. Account management entails creating, modifying, and dropping user accounts.

Security administration. Security administration covers basic security tasks such as creating realms and command rules, setting security policies for database users' access, and authorizing database users for jobs they are allowed to perform. Resource management. Resource management refers to managing the database system but not accessing business data. It includes the following operations:

Backup operations require a predefined time to perform the backup using predefined tools. Tuning and monitoring operations require ongoing performance monitoring and analysis. Patching operations require temporary access only during the time the patching takes place

**QUESTION 15**

Which of the following statements about Transparent Data Encryption (TDE) is NOT true?

- A. For a partitioned table, you can have some partitions in encrypted tablespaces and some in non-encrypted tablespaces.
- B. For a partitioned table, you can encrypt a column in some partitions and not in others.
- C. A range-based selection condition can use an index with tablespace-based Transparent Data Encryption (TDE).
- D. An index on a value in an encrypted tablespace does not have to be encrypted.

**Correct Answer:** A

**Explanation****Explanation/Reference:**

Explanation:

ORA-28346: an encrypted column cannot serve as a partitioning column Cause: An attempt was made to encrypt a partitioning key column or create partitioning index with encrypted columns.

Action: The column must be decrypted.

ORA-28347: encryption properties mismatch

Cause: An attempt was made to issue an ALTER TABLE EXCHANGE PARTITION | SUBPARTITION command, but encryption properties were mismatched. Action: Make sure encryption algorithms and columns keys are identical. The corresponding columns must be encrypted on both tables with the same salt and non-salt flavor. You can create an index on an encrypted column if it has been encrypted without salt. TDE tablespace encryption also allows index range scans on data in encrypted tablespaces. This is not possible with TDE column encryption.

If you need to perform range scans over indexed, encrypted, columns, then you should use TDE tablespace encryption in place of TDE column encryption.

**QUESTION 16**

Which two of the following are reasons to use Oracle Audit Vault?

- A. To consolidate audit reports from multiple databases
- B. To reduce the performance impact of auditing across multiple databases
- C. To limit space required for audit trails
- D. To ensure consistent auditing across multiple databases

**Correct Answer:** AC

**Explanation**

**Explanation/Reference:**

Explanation:

Audit repository exists for Oracle database (Release 10.2.0.4) to consolidate and manage audit trail records.

By default, ARCHIVELOG mode is enabled in the Audit Vault Server database. The ARCHIVELOG mode copies filled online redo logs to disk. This enables you to back up the database while it is open and being accessed by users, and to recover the database to any desired point in time. You should monitor the disk space usage for the redo logs.

**QUESTION 17**

The data in the primary database is encrypted using TDE. With which type of Data Guard standby must you have a wallet open on the standby server?

- A. Physical standby
- B. Logical standby
- C. Both physical and logical standby
- D. Neither physical nor logical standby requires an open wallet

**Correct Answer:** C

**Explanation**

**Explanation/Reference:**

Explanation:

Oracle Data Guard supports Transparent Data Encryption (TDE). If the primary database uses TDE, then each standby database in a Data Guard configuration must have a copy of the encryption wallet from the primary database. If you reset the master encryption key in the primary database, then the wallet containing the master encryption key needs to be copied to each standby database.

**QUESTION 18**

In terms of security, what use case is a classic example of separation of duties?

- A. Denying users access to administrative functions
- B. Denying managers access to employee data
- C. Denying administrators access to data values
- D. Allowing administrators to back up data from only one department
- E. Allowing administrators to back up data from an entire enterprise

**Correct Answer:** C

**Explanation**

**Explanation/Reference:**

Explanation:

Separation of duties is denying administrators access to data values.

**QUESTION 19**

Your customer realizes that they must implement more robust and flexible auditing for their enterprise databases. However, based on the specific requirements of their particular industry, they are concerned that they may not be able to achieve their goals with Oracle Audit Vault. Which three features does Oracle Audit Vault provide to allow them to achieve their very specific goals?

- A. You can use Oracle Audit Vault to compare security policies with current settings on target databases.
- B. You can use Oracle Audit Vault to create custom audit reports to span audit information from multiple databases.
- C. You can use Oracle Audit Vault to provide custom auditing for many different types of databases.
- D. You can use Oracle Audit Vault to collect data from multiple types of databases.

**Correct Answer:** BCD

## Explanation

### Explanation/Reference:

Explanation:

This section provides guidelines for selecting the correct Oracle Audit Vault collector for the source databases from which you want to extract audit data. In brief, for Oracle Database, the type of collector that you select depends on the type of auditing that you have enabled in the source database. The Microsoft SQL Server, Sybase ASE, and IBM DB2 databases each use one collector specific to each of these database products.

### QUESTION 20

How do you handle Oracle audit trails after the audit records have been inserted into Oracle Audit Vault?

- A. Audit trails must be deleted manually
- B. Oracle Audit Vault automatically cleans up audit trails after the audit records have been inserted into the Vault.
- C. You cannot delete any audit trails when using Oracle Audit Vault.
- D. You schedule Oracle Audit Vault jobs to clean up audit trails on a scheduled basis.

**Correct Answer:** D

### Explanation

### Explanation/Reference:

Explanation:

Oracle Audit Vault is integrated with the DBMS\_AUDIT\_MGMT package on a source database. This integration automates the purging of audit records from the AUD\$ and FGA\_LOG\$ files, and from the operating system .aud and .xml files after they have been successfully inserted into the Audit Vault repository by the Audit Vault collector.

### QUESTION 21

Changing the master key uses fewer resources than changing table keys.

- A. TRUE
- B. FALSE

**Correct Answer:** A

### Explanation

### Explanation/Reference:

Explanation:

Changing the master key requires fewer resources than changing the table keys, which require rekeying the data.

### QUESTION 22

Which four are Oracle Data Masking Pack primitives?

- A. Random numbers
- B. Random digits IS
- C. Random images
- D. Random dates
- E. Random strings

**Correct Answer:** ABDE

### Explanation

### Explanation/Reference:

Explanation:

Using the Data Masking Pack sensitive data irreversibly replaced with realistic-looking but scrubbed data based on rules and templates. The original data cannot be retrieved, recovered, or restored. By masking sensitive data it is no longer sensitive or subject to regulatory requirements and can be shared with

internal or external groups.

The DMP offers uses an extensible format library for consistent masking of fields. The out-of- the-box format library can be extended by customers and third-parties based on application specific best practices. The masking rules are applied automatically across all databases in the enterprise maintaining referential integrity for applications.

#### **QUESTION 23**

How many masking operations must be performed to mask six columns in a table?

- A. None
- B. One
- C. Three
- D. Six

**Correct Answer:** D

**Explanation**

**Explanation/Reference:**

Explanation:  
1 per column

#### **QUESTION 24**

Which utilizes a two-tier architecture?

- A. Advanced Security
- B. Oracle Database Vault
- C. Oracle Audit Vault
- D. Oracle Label Security
- E. Oracle Data Masking Pack
- F. Virtual Private Database

**Correct Answer:** A

**Explanation**

**Explanation/Reference:**

Explanation:  
Advanced Security Option uses a two-tier architecture for key management.

#### **QUESTION 25**

Why would a merger or acquisition lead to the need for Oracle Audit Vault?

- A. Larger amounts of data would require more resources for auditing
- B. Heterogeneous databases could benefit from a centralized audit repository
- C. Oracle Audit Vault can help identify differences in security schemes
- D. Oracle Audit Vault can help to consolidate database schemas.

**Correct Answer:** B

**Explanation**

**Explanation/Reference:**

#### **QUESTION 26**

Your customer wants to add an additional level of security to their data, based on values in individual records.

The good news is that they have a column in the target table that lists the application role they would like to use to control access. Which security feature or option will give them this capability in the most efficient way?

- A. Advanced Security Option
- B. Oracle Database Vault
- C. Oracle Audit Vault
- D. Oracle Data Masking Pack
- E. Virtual Private Database
- F. Oracle Label Security

**Correct Answer:** F  
**Explanation**

**Explanation/Reference:**

Explanation:

With Oracle Label Security, you restrict user access to data by focusing on row data, and designing different levels of access based on the sensitivity of your data.

**QUESTION 27**

How can you protect Oracle Database Vault Audit records?

- A. By restricting access to the DBV.AUDIT tables
- B. You don't have to - Oracle Database Vault audit records are protected.
- C. With standard separation of duties
- D. By defining using the Audit role defined within Oracle Database Vault.

**Correct Answer:** B  
**Explanation**

**Explanation/Reference:**

Explanation:

By default, Oracle Database Vault is enabled in the Audit Vault Server. Oracle Database Vault restricts access to the data in the Audit Vault Server from any user, including users who have administrative access. For Oracle Audit Vault, Oracle Database Vault protects the Audit Vault Server by using a realm. To ensure that the data in the Audit Vault Server is protected, do not disable Oracle Database Vault.

**QUESTION 28**

Which two of the following Oracle Audit Vault collectors require the db to be open to start?

- A. Operating system audit collector
- B. Database audit collector
- C. Redo collector
- D. ODBC collector

**Correct Answer:** CD  
**Explanation**

**Explanation/Reference:**

Explanation:

Applies to all collectors, as follows:

Oracle Database DBAUD, OSAUD, and REDO collectors. Contains monitoring information, such as whether the collector is active and how many records were sent. For the REDO collector, the Streams framework performs the actual collection, so the Oracle Audit Vault agent has no knowledge of the collection.

Non-Oracle Database collectors. Contains a log of all collection operations for the MSSQLDB, SYBDB, and DB2 collectors.

**QUESTION 29**

Which two of the following benefits of enhanced data security can increase the opportunities for your solution?

- A. Lower costs for your development

- B. Greater efficiency in using your solution
- C. Access to opportunities that require some form of compliance
- D. Added value for your solution

**Correct Answer:** CD

**Explanation**

**Explanation/Reference:**

**QUESTION 30**

Which of the following encryption algorithms is the default for Transparent Data Encryption (TDE) tablespace encryption?

- A. AES128
- B. AES192
- C. AES256
- D. 3DES168

**Correct Answer:** B

**Explanation**

**Explanation/Reference:**

Explanation:

By default, TDE uses the AES encryption algorithm with a 192-bit key length (AES192).

**QUESTION 31**

Which security requirements can affect companies regardless of their location in the world?

- A. PCI
- B. HIPAA
- C. ISO-9000
- D. GLBA

**Correct Answer:** A

**Explanation**

**Explanation/Reference:**

Explanation:

Payment Card Industry security standards can affect companies worldwide.

**QUESTION 32**

Which four types of agents are supported by Oracle Audit Vault for Oracle databases?

- A. Redo
- B. Database audit files
- C. Oracle audit trail from OS
- D. Operating system SYSLOG files
- E. ODBC audit files

**Correct Answer:** ABCD

**Explanation**

**Explanation/Reference:**

Explanation:

Audit Vault supports redo, database and operating system based auditing for the Oracle database.

**QUESTION 33**

How do you handle partitions with encrypted tablespaces?

- A. You cannot have partitions in encrypted tablespaces.
- B. You can have different partitions in different tablespaces, both encrypted and not encrypted.
- C. All partitions must be in the same encrypted tablespace.
- D. You can have partitions in multiple tablespaces, as long as all of them are encrypted.

**Correct Answer: B**

**Explanation**

**Explanation/Reference:**

Explanation:

You can have different partitions in different tablespaces, both encrypted and not encrypted.

**QUESTION 34**

Which component of Oracle Audit Vault may require multiple instances per targeted database server machine?

- A. Collector
- B. Agent
- C. Oracle Audit Vault Server
- D. Oracle Audit Vault consolidator

**Correct Answer: A**

**Explanation**

**Explanation/Reference:**

Explanation:

You configure one collection agent for each host and one or more collectors for each individual source database. For example, if a host contains four databases, then you would configure one collection agent for that host and one or more collectors for each of the four databases. The number of collectors that you configure and the collection agent that you use to manage them depends on the source database type and the audit trails that you want to collect from it.

**QUESTION 35**

The following actions are part of the data masking process:

- A. Re-create masked table copy & populate using renamed original table and mapping table.
  - B. Disable constraints on table & rename table.
  - C. Build mapping table containing original sensitive and masked values using masking routines.
  - D. Drop renamed table and mapping table.
  - E. Restore constraints based on original table & collect statistics.
- In which order are these actions performed?
- F. A-B-C-D-E
  - G. E-D-C-B-A
  - H. A-C-E-B-D
  - I. C-B-A-D-E
  - J. C-A-B-E-D

**Correct Answer: E**

**Explanation**

**Explanation/Reference:**

Explanation:

The following basic steps guide you through the data masking process, with references to other sections for supporting information.

Review the application database and identify the sources of sensitive information. Define mask formats for the sensitive data. The mask formats may be simple or complex depending on the information security needs of the organization. For more information, see "Creating New Masking Formats" and "Using Oracle-supplied Predefined Masking Formats".

To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

# Trying our product !

- ★ **100%** Guaranteed Success
- ★ **100%** Money Back Guarantee
- ★ **365 Days** Free Update
- ★ **Instant Download** After Purchase
- ★ **24x7** Customer Support
- ★ Average **99.9%** Success Rate
- ★ More than **69,000** Satisfied Customers Worldwide
- ★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

## Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



 <b>One Year Free Update</b> <p>Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 <b>Money Back Guarantee</b> <p>To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <b>Security &amp; Privacy</b> <p>We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information &amp; peace of mind.</p>
---	---	--

## [Guarantee & Policy](#) | [Privacy & Policy](#) | [Terms & Conditions](#)

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.

Copyright © 2004-2015, All Rights Reserved.