Oracle

Exam 1z0-528

Oracle Database 11g Security Essentials

Version: 6.2

[Total Questions: 77]

Question No : 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

Answer: C

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 realmprotection and authorize a set of users or roles to access the secured objects.

Question No : 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)

Answer: C

Explanation:

Beacose 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 Oracledatabases: such access is normally disabled, by default. Sometimes the obfuscated autologin wallets are called "SSO wallets" because they support single sign-on capability.

Question No : 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

Answer: A,E

Explanation:

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

Question No : 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

Answer: A

Explanation:

Changes to Database Vault permissions take effect immediately.

Question No : 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

Answer: E

Explanation:

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

Question No : 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

Answer: C

Explanation:

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

Question No : 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

Answer: B

Explanation:

You can add\delete and configure Vault on RAC nodes. Can manage accounts andsecurity.

Question No : 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

Answer: D

Explanation:

According to labels

Question No : 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.

Answer: A

Explanation:

Step 2: Create the Wallet

To create the wallet, use the ALTER SYSTEM SQL statement. By default, the Oracle wallet stores a history ofretired master keys, which enables you to change them and still be able to decrypt data that was encryptedunder 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 dataencryption master key.

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

Question No : 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

Answer: B

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 No : 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

Answer: A,C,D

Explanation:

It's not abackupsolution but it has anopportunityto share data, wheresensitiveinformationis masked.

Question No : 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

Answer: A,B,C,D

Explanation:

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

Question No : 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

Answer: C

Explanation:

VPD Provides column-level security (column masking)

Question No : 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

Answer: A,B,D

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 andcommand rules, setting security policies for database users' access, and authorizing database users for jobsthey are allowed to perform.

Resource management. Resource management refers to managing the database system but not accessingbusiness 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 No : 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- encryptedtablespaces.
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.

Answer: A

Explanation:

ORA-28346: an encrypted column cannot serve as a partitioning column
Cause: An attempt was made to encrypt a partitioning key column or createpartitioning 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 weremismatched.
Action: Make sure encryption algorithms and columns keys are identical. Thecorresponding columns must be encrypted on both tables with the same salt andnon-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 encryptedtablespaces. 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 ofTDE column encryption.

Question No : 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

Answer: A,C

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 modecopies filled online redo logs to disk. This enables you to back up the database while it is open and beingaccessed by users, and to recover the database to any desired point in time. You should monitor the diskspace usage for the redo logs.

Question No : 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

Answer: C

Explanation:

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

Question No : 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

Answer: C

Explanation:

Separation of duties is denying administrators access to data values.

Question No : 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 Orade Audit Vault to create custom audit reports to span audit information from multipledatabases.
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.

Answer: B,C,D

Explanation:

This section provides guidelines for selecting the correct Oracle Audit Vault collectorfor the source databases from which you want to extract audit data. In brief, for OracleDatabase, the type of collector that you select depends on the type of auditing that youhave enabled in the source database. The Microsoft SQL Server, Sybase ASE, and IBMDB2 databases each use one collector specific to each of these database products.

Question No : 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 theVault.
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.

Answer: D

Explanation:

Oracle Audit Vault is integrated with the DBMS_AUDIT_MGMT package on a sourcedatabase. This integration automates the purging of audit records from the AUD$ andFGA_LOG$ files, and from the operating system .aud and .xml files after they havebeen successfully inserted into the Audit Vault repository by the Audit Vault collector.

Question No : 21

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

A. TRUE
B. FALSE

Answer: A

Explanation:

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