Oracle 1Z0-931-25 Practice Questions

Shared by Watts on 10-11-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

For someone that is not a service administrator to use SQL Developer Web, what package would you need to use to give them access?

Options:

A- ORDS_ADMIN.GRANT_SCHEMA
B- ORDS_ADMIN.ENABLE_SCHEMA
C- ORDS_PRIV.ENABLE_SCHEMA
D- SQLDEV_ADMIN.GRANT_SCHEMA

Answer:

B

Explanation:

SQL Developer Web in Autonomous Database relies on Oracle REST Data Services (ORDS) for access. The correct package is:

ORDS_ADMIN.ENABLE_SCHEMA (B): To allow a non-admin user (e.g., ANALYST1) to use SQL Developer Web, the ADMIN user executes ORDS_ADMIN.ENABLE_SCHEMA to enable the schema for ORDS access. This procedure activates the schema for RESTful services, granting privileges like CONNECT and SELECT implicitly for web-based SQL execution. Example:

BEGIN

ORDS_ADMIN.ENABLE_SCHEMA(p_schema => 'ANALYST1');

END;

After this, the user accesses SQL Developer Web via a URL (e.g., https:///ords/analyst1/_sdw), logging in with their database credentials. This is necessary because SQL Developer Web runs on ORDS, and only enabled schemas can interact with it. For instance, an analyst might query SELECT * FROM sales in the web interface post-enablement, without needing full admin rights.

The incorrect options are:

ORDS_ADMIN.GRANT_SCHEMA (A): No such procedure exists in ORDS_ADMIN. Granting is handled via database roles/privileges (e.g., GRANT CONNECT), not a specific ORDS grant function.

ORDS_PRIV.ENABLE_SCHEMA (C): There's no ORDS_PRIV package; this might confuse with ORDS_ADMIN. The correct package is ORDS_ADMIN for schema enablement.

SQLDEV_ADMIN.GRANT_SCHEMA (D): No SQLDEV_ADMIN package exists. SQL Developer Web access is managed through ORDS, not a separate SQL Developer-specific package.

ORDS_ADMIN.ENABLE_SCHEMA is the standard, secure way to enable non-admin access to this tool in ADB.

Question 2

Question Type: MultipleChoice

Which four levels of access can be defined in policies? (Choose four.)

Options:

A- Create
B- Read
C- Manage
D- Inspect
E- Use

Answer:

B, C, D, E

Explanation:

Oracle Cloud Infrastructure (OCI) Identity and Access Management (IAM) defines four verb levels for policy permissions:

Read (B): Allows viewing resource details without modification (e.g., read autonomous-databases).

Manage (C): Permits full control, including creating, updating, and deleting resources (e.g., manage autonomous-databases).

Inspect (D): Enables listing resources and basic metadata without detailed access (e.g., inspect autonomous-databases).

Use (E): Allows interaction with resources (e.g., connecting to a database) without altering their configuration.

Incorrect Option:

Create (A): ''Create'' is not a standalone verb; it's part of the manage verb, which includes

creation, update, and deletion actions.

These levels provide granular control over resource access in OCI.

Question 3

Question Type: MultipleChoice

Which option should you use to create a graph with Graph Studio?

Options:

A- Tables in an Autonomous Database instance
B- Graph analytics algorithms
C- NoSQL configuration
D- Graph created by a special tool downloaded from oracle.com
E- A graph license key

Answer:

A

Explanation:

Graph Studio in Autonomous Database enables graph creation and analysis:

Correct Answer (A): ''Tables in an Autonomous Database instance'' are used to create graphs. Graph Studio builds property graphs from relational tables by defining vertices (nodes) and edges (relationships) based on existing data, leveraging the database's schema.

Incorrect Options:

B: Graph analytics algorithms analyze existing graphs, not create them.

C: NoSQL configuration is unrelated; Graph Studio uses relational data.

D: No external tool from oracle.com is required; Graph Studio is a built-in feature.

E: A license key isn't a creation method; graph features are included with Autonomous Database.

This integrates graph capabilities with existing data.

Question 4

Question Type: MultipleChoice

Which three options are supported when migrating to Autonomous Database (ADB)? (Select three.)

Options:

A- GoldenGate on-premise installation
B- RMAN Cross-Platform backup and restore
C- Data Guard Physical Standby
D- GoldenGate Cloud Service
E- Data Pump export/import
F- PDB unplug/plug operation

Answer:

A, D, E

Explanation:

Migrating to Autonomous Database supports multiple methods. The three correct options are:

GoldenGate on-premise installation (A): Oracle GoldenGate (on-prem) replicates data from source databases (e.g., Oracle, MySQL) to ADB, supporting real-time or batch migration. You install GoldenGate on-prem, configure extract/replicat processes (e.g., extracting from an Oracle 19c source), and target an ADB instance using credentials and wallet. For example, it might sync an on-prem ORDERS table to ADB with near-zero latency, ideal for live migrations.

GoldenGate Cloud Service (D): GoldenGate Cloud Service, a managed OCI offering, performs the same replication but runs in the cloud. You provision it via OCI Marketplace, configure it to pull from a source (e.g., on-prem or another cloud), and push to ADB. For instance, it could replicate a SaaS database to ADB for analytics, minimizing on-prem overhead. Both GoldenGate options support initial loads and continuous sync.

Data Pump export/import (E): Data Pump exports data/schemas from a source (e.g., expdp hr/hr schemas=HR directory=DATA_PUMP_DIR) to a dump file, which you upload to OCI Object Storage. Then, import into ADB using DBMS_CLOUD.COPY_DATA (e.g., targeting a HR schema). It's great for one-time migrations, like moving a 12c database to ADB, with flexibility to exclude objects (e.g., indexes).

The incorrect options are:

RMAN Cross-Platform backup and restore (B): RMAN restores physical backups, but ADB's managed nature prevents direct RMAN restores---users can't access the file system. RMAN is used for ADB backups internally by Oracle, not customer migrations.

Data Guard Physical Standby (C): Data Guard creates physical standbys for HA, not migration to ADB. ADB uses Autonomous Data Guard internally, but it's not a migration tool from external sources.

PDB unplug/plug operation (F): Unplugging/plugging PDBs requires file-level access, unsupported in ADB due to its managed storage. You'd use Data Pump instead for PDB data.

These methods offer robust, flexible migration paths to ADB.

Question 5

Question Type: MultipleChoice

Which two license types does the customer need to benefit from BYOL when leveraging on-premise Enterprise Database licenses in Oracle Autonomous Database?

Options:

A- Exadata
B- Active Data Guard
C- Real Application Clusters (RAC), but only when scaling beyond 16 OCPUs
D- Multitenant
E- Transparent Data Encryption (TDE)

Answer:

C, D

Explanation:

Full Detailed In-Depth Explanation:

Bring Your Own License (BYOL) allows using existing on-premises Oracle licenses in the cloud:

A: False. Exadata is included in Autonomous Database; no separate license is needed.

B: False. Active Data Guard is an optional feature, not required for BYOL.

C: True. RAC is needed for BYOL when scaling beyond 16 OCPUs, as Autonomous Database uses RAC for high availability in larger deployments.

D: True. Multitenant is mandatory, as Autonomous Database uses a multitenant architecture (CDB/PDB).

E: False. TDE is included by default, not a BYOL requirement.

Question 6

Question Type: MultipleChoice

Which is NOT needed to manage Oracle Autonomous Database with REST APIs?

Options:

A- User's OCID
B- Tenancy's OCID
C- Fingerprint of the public key
D- Database ADMIN password

Answer:

D

Explanation:

Managing Autonomous Database via REST APIs relies on OCI authentication:

Correct Answer (D): ''Database ADMIN password'' is not needed. REST API access uses OCI IAM credentials, not database-level credentials like the ADMIN password.

Required Items:

A: User's OCID identifies the API caller.

B: Tenancy's OCID specifies the cloud environment.

C: Fingerprint of the public key authenticates API requests with a private-public key pair.

This ensures secure, external management without exposing database credentials.

Question 7

Question Type: MultipleChoice

Which two actions can be performed when an Autonomous Database is stopped? (Choose two.)

Options:

A- Change administrator password
B- Start
C- Update License type
D- Update Network Access

P2P exams

Answer:

B, C

Explanation:

When an Autonomous Database is stopped, limited actions are available:

Correct Answer (B): Start is possible to bring the database back online via the OCI Console or API.

Correct Answer (C): Update License type (e.g., from License Included to Bring Your Own License) can be performed while stopped, as it's a configuration change not requiring database activity.

Incorrect Options:

A: Changing the admin password requires the database to be running for security validation.

D: Updating network access (e.g., ACLs) requires an active instance to apply changes.

These options reflect the stopped state's constraints.

P2P exams

To Get Premium Files for 1Z0-931-25 Visit

https://www.p2pexams.com/products/1z0-931-25

For More Free Questions Visit

https://www.p2pexams.com/oracle/pdf/1z0-931-25

