PassQueen
a.k.a dumpsqueen.com

Oracle Autonomous Database Cloud 2026 Professional

Oracle 1z0-931-25

Version Demo

Total Demo Questions: 15

Total Premium Questions: 153

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

Which method does NOT permit you to change the database ADMIN user's password of an Oracle Autonomous Database on Shared Infrastructure?

A. Admin page of the Cloud Service Console

B. OCI CLI

C. OS command line from the database server

D. SQL Developer

ANSWER: C

Explanation:

OS command line from the database server does not permit changing the ADMIN password because Oracle Autonomous Database on Shared Infrastructure is a fully managed service. Oracle manages and secures the underlying compute hosts, operating system, database software installation, and infrastructure administration. Database users and service administrators are not given shell, SSH, or operating-system command-line access to the database server. Consequently, no host-based password-management workflow is available to an Autonomous Database customer.

Instead, ADMIN password administration is performed through supported Autonomous Database management interfaces. Oracle documents changing the administrator password through the Oracle Cloud Console as part of Autonomous Database administration, and the Autonomous Database update API/CLI operation includes an `adminPassword` attribute for this managed update. These mechanisms allow Oracle to apply the change while preserving the service's managed operating model and separation between customer database administration and Oracle infrastructure administration.

Oracle's documentation on changing the Autonomous Database administrator password describes the supported management process. The corresponding UpdateAutonomousDatabase API reference documents the managed API operation and its administrator-password field.

QUESTION NO: 2

You need to create a new database by using the Oracle Cloud Infrastructure (OCI) Command Line Interface (CLI) with the following requirements: Autonomous Transaction Processing, License Included, Shared Infrastructure. Which parameter would you NOT use?

A. db-type

B. is-dedicated

C. db-workload

D. license-model

ANSWER: A

Explanation:

`db-type` is the parameter that would not be used. The OCI CLI command for creating an Autonomous Database is `oci db autonomous-database create`, and its supported arguments define the Autonomous Database workload with `--db-workload`, rather than with a parameter named `--db-type`. For an Autonomous Transaction Processing database, the workload value is `OLTP`. The creation request also accepts a license model through `--license-model`; the License Included requirement maps to the `LICENSE_INCLUDED` value. Shared Infrastructure is represented by setting `--is-dedicated` to `false` when that parameter is supplied. These arguments are part of the Autonomous Database create operation and enable the CLI request to describe the specified service configuration accurately. Oracle's CLI reference lists the supported arguments for the create command, including workload, license model, and dedicated-infrastructure settings,

but does not list `db-type`. See the OCI CLI autonomous-database create command reference and the Oracle Autonomous Database creation documentation.

QUESTION NO: 3

What two actions can you do when a refreshable clone passes the refresh time limit? (Choose two.)

A. You can manually refresh the clone

B. You can disconnect from the source to make the database a read/write database

C. You can use the instance as a read-only database

D. You can extend the refresh time limit

ANSWER: B C

Explanation:

A refreshable clone is designed to provide a queryable, read-only copy of its source while it is within its configured refresh window. When that refresh time limit has passed, it cannot continue receiving refreshes from the source, but its existing data remains available for read-only use. This lets teams continue to run reports, validation queries, comparisons, or other analysis against the clone's last available refreshed state without changing the source database.

If a writable, independent database is required instead, the clone can be disconnected from its source. Disconnecting ends the refreshable-clone relationship and converts the clone into a standalone read/write Autonomous Database. This is useful when a temporarily refreshed copy must become an environment for development, testing changes, or another workload that requires DML operations. Oracle documents that a refreshable clone can be disconnected to make it a read/write database, and its cloning documentation describes the refreshable-clone lifecycle and refresh limit behavior. See Oracle Autonomous Database cloning documentation and OCI CLI autonomous-database update reference.

QUESTION NO: 4

Which three capabilities are provided by Oracle Data Safe for an Autonomous Database? (Choose three.)

A. Perform Security Assessments of database configuration

B. Perform User Assessments of users and privileges

C. Discover sensitive data in database tables

D. Apply database Release Updates manually

E. Manage Transparent Data Encryption master keys manually

ANSWER: A B C

Explanation:

Security Assessment, **User Assessment**, and **Data Discovery** are Oracle Data Safe capabilities. Security Assessment evaluates database configuration against security best practices. User Assessment evaluates database users, roles, privileges, and related risks. Data Discovery identifies sensitive data in database tables and columns.

Data Safe also supports Data Masking and Activity Auditing. It does not require administrators to manually apply Autonomous Database security patches or manage database encryption keys before provisioning.

QUESTION NO: 5

Which statement is correct with respect to the required action to move Oracle Autonomous Database resources to a different compartment?

A. Moving an Autonomous Database instance does not include its automatic backups.

B. You do not require sufficient access permissions on the compartment that the resource is being moved to.

C. Autonomous Exadata Infrastructure instances and Autonomous Container Databases have no dependent resources that move with them. Associated (non-dependent) resources remain in their current compartments.

D. Moving the compartment of the Autonomous Database also moves the Autonomous Container Database and Autonomous Exadata Infrastructure.

ANSWER: C

Explanation:

“Autonomous Exadata Infrastructure instances and Autonomous Container Databases have no dependent resources that move with them. Associated (non-dependent) resources remain in their current compartments.” is correct. OCI resource moves are governed by dependency relationships: when a resource has dependent resources, those dependencies can be moved together where OCI supports that behavior. For Autonomous Exadata Infrastructure and Autonomous Container Database resources, however, Oracle documents that there are no dependent resources included in the move operation. Consequently, moving either of these dedicated Autonomous Database infrastructure resources changes only that resource’s compartment association. Resources merely associated with it, rather than defined as dependent resources, retain their existing compartment placement. This distinction is important for compartment-based organization, access policy design, cost tracking, and operational planning. Administrators should inventory associated resources and deliberately move any that also need to reside in the destination compartment, subject to the individual resource type’s move support and IAM requirements. The move process therefore should not be treated as a blanket relocation of an entire dedicated Autonomous Database environment; it is a resource-specific OCI operation with explicitly defined dependency behavior. Oracle’s compartment-moving guidance explains that supported resources can be moved and identifies dependency considerations, while the Autonomous Database documentation provides the service-specific rules for moving Autonomous Database resources. See Moving Resources Between Compartments and Oracle Autonomous Database Documentation.

QUESTION NO: 6

Which statement is true about connecting a marketplace Oracle Cloud Infrastructure (OCI) image to an Autonomous Database on Shared Infrastructure?

A. The Autonomous Database must belong to a Network Security Group (NSG).

B. The marketplace OCI image can be used with an Always Free Autonomous Database account.

C. A Private Endpoint is required to connect to the Autonomous Database on Shared Exadata infrastructure.

D. The marketplace OCI image does not support connecting to an Autonomous Database on Shared Infrastructure.

ANSWER: B

Explanation:

The marketplace OCI image can be used with an Always Free Autonomous Database account. An Always Free Autonomous Database is an Autonomous Database deployment on shared infrastructure, and its database connectivity model is the same fundamental model used for other Autonomous Database Serverless instances. A workload running on an OCI Compute instance created from a Marketplace image can connect by using the Autonomous Database service credentials and connection information, including the client wallet when wallet-based mutual TLS connectivity is used. The image itself does not impose a requirement to use a paid Autonomous Database service; the relevant requirements are that the Compute instance has a network path to the database endpoint and that the client is configured with valid database credentials and the appropriate connection files. This makes Always Free useful for development, demonstrations, and evaluations involving Marketplace-based application or tool images. Oracle documents that Autonomous Database clients connect using downloadable client credentials and service connection strings, and Oracle’s Always Free program includes Autonomous Database resources. See Oracle Autonomous Database: Connecting to Autonomous Database and Oracle Cloud Free Tier documentation.

QUESTION NO: 7

Which two statements are true about the Oracle Cloud Infrastructure (OCI)? (Choose two.)

A. Regions are dependent on other regions and must be located within 5 thousand kilometers of each other.

B. An OCI region is a localized geographic area, and an availability domain is one or more data centers located within a region.

C. A single fault domain can be associated with multiple regions and availability domains.

D. Because availability domains do not share infrastructure such as power or cooling, or the internal availability domain network, a failure at one availability domain within a region is unlikely to impact the availability of the others within the same region.

ANSWER: B D

Explanation:

“An OCI region is a localized geographic area, and an availability domain is one or more data centers located within a region” is correct because OCI organizes its global cloud footprint into regions, each of which is a localized geographic area. A region contains one or more availability domains. Availability domains are isolated, fault-tolerant groupings of one or more data centers within that region. This architecture lets customers deploy resources across availability domains when designing highly available applications.

“Because availability domains do not share infrastructure such as power or cooling, or the internal availability domain network, a failure at one availability domain within a region is unlikely to impact the availability of the others within the same region” is also correct. OCI designs availability domains as physically separate and independently resilient environments. They use separate power, cooling, and internal networks, providing strong fault isolation. Consequently, distributing redundant application tiers and database components across availability domains can protect a workload from an availability-domain-level disruption while retaining low-latency connectivity within the same region. Oracle documents these regional and availability-domain characteristics in its Regions and Availability Domains documentation and its Availability Domains overview.

QUESTION NO: 8

Which is an Autonomous Database critical event?

A. Maintenance Begin

B. Database Connection

C. Schedule Maintenance Warning

D. Admin Password Warning

E. New Maintenance Schedule

ANSWER: D

Explanation:

Admin Password Warning is an Autonomous Database critical event because it alerts the service administrator that the ADMIN account password is approaching expiration. The ADMIN account is the principal administrative database account and is needed for essential administration tasks, including creating users and managing database access. Addressing the warning promptly by changing the password prevents an expiration from interrupting administrative access and helps maintain the database’s secure operational state.

Autonomous Database integrates with Oracle Cloud Infrastructure event notifications so administrators can receive and act on significant service events. Password-expiration notifications are especially important because they provide advance notice rather than waiting until an administrator urgently needs privileged access. Oracle documents that the ADMIN password expires after a defined period and that it must be changed through supported Autonomous Database

administration methods. This makes the warning an event that requires timely customer action, which is the key characteristic of a critical event in this context.

For Oracle's guidance on managing the ADMIN password, see Manage the ADMIN Password. For details about Autonomous Database event notifications, see Autonomous Database Events.

QUESTION NO: 9

Which three methods can be used to migrate your existing Oracle database to Autonomous Database? (Choose three.)

A. Using SFTP to copy CSV files into an Autonomous Database

B. Using Oracle Zero Downtime Migration (ZDM)

C. Using GoldenGate

D. Using Data Pump

E. Using Recovery Manager (RMAN)

ANSWER: B C D

Explanation:

Using Oracle Zero Downtime Migration (ZDM), using GoldenGate, and using Data Pump are established Oracle-supported approaches for moving an existing Oracle database to Autonomous Database. Oracle Zero Downtime Migration orchestrates migration workflows and is designed to reduce service interruption, making it appropriate when an organization needs a controlled migration process with minimal downtime. Oracle documents Autonomous Database as a supported target for logical online migration workflows with ZDM.

Using GoldenGate supports online migration by replicating committed source changes to the target while the initial data load and cutover are completed. This approach is especially useful for databases that must remain available throughout most of the migration, because replication keeps the target synchronized until the planned switchover.

Using Data Pump is the standard logical export/import approach. It can export database objects and data into dump files and import them into Autonomous Database through supported Object Storage-based workflows. This is a practical method for planned migrations where a maintenance window is available and a logical copy of schemas and data is required. Oracle's migration guidance covers these methods and their associated preparation and cutover considerations. See Oracle Autonomous Database migration documentation and Oracle Zero Downtime Migration documentation.

QUESTION NO: 10

To whom, and in which order, are dedicated Exadata Infrastructure resources provisioned?

A. Fleet Administrator, Autonomous Exadata Infrastructure - > Autonomous VM Cluster - > Autonomous Container DB - > Database Administrator - > Autonomous DB

B. Fleet Administrator, Autonomous Exadata Infrastructure - > Database Administrator - > Autonomous Container DB - > Autonomous DB

C. Database Administrator, Autonomous Container DB - > Autonomous DB - > Fleet Administrator - > Autonomous Exadata Infrastructure

D. Database Administrator, Autonomous Exadata Infrastructure - > Fleet Administrator - > Autonomous Container DB - > Autonomous DB

ANSWER: A

Explanation:

Dedicated Autonomous Database provisioning follows a hierarchy that separates fleet-level infrastructure administration from database-level administration. The Fleet Administrator first provisions the Autonomous Exadata Infrastructure, the dedicated physical Exadata resource that supplies the underlying compute and storage capacity. The Fleet Administrator then creates an Autonomous VM Cluster and an Autonomous Container Database within that infrastructure. The Autonomous Container Database provides the multitenant environment in which Autonomous Databases are hosted. After those fleet resources are available, the Database Administrator provisions an individual Autonomous Database in the Autonomous Container Database. This sequence ensures that database creation occurs only after the required Exadata, virtual-machine-cluster, and container-database layers have been configured and made available by the responsible fleet administrator. Oracle documents this Dedicated Exadata Infrastructure resource hierarchy and distinguishes the fleet administration tasks from the Autonomous Database administration tasks. See Oracle's Autonomous Database on Dedicated Exadata Infrastructure documentation and the Dedicated infrastructure overview.

QUESTION NO: 11

Which two options are available for restoring an Autonomous Database? (Choose two.)

A. Selecting the backup from which restore needs to be done.

B. Selecting the snapshot of the backup.

C. Specifying the archived custom image.

D. Specifying the point in time (timestamp) to restore.

ANSWER: A D

Explanation:

Autonomous Database provides two supported restore choices in the Oracle Cloud Infrastructure Console. **Selecting the backup from which restore needs to be done.** supports recovery by choosing an available automatic backup as the source for the restore operation. This is appropriate when the required recovery state corresponds to a listed backup and the administrator wants to select that backup directly.

Specifying the point in time (timestamp) to restore. supports point-in-time recovery. The administrator supplies a timestamp within the database's available recovery window, and Autonomous Database restores the database to its state at that time. This provides finer-grained recovery when the desired state is between the displayed backup timestamps, such as immediately before an accidental data change. Oracle manages Autonomous Database backups and recovery operations, while the restore workflow lets the user choose either a backup-based restore or a timestamp-based restore. The restore target must be within the available backup retention period for the database. Oracle's restore documentation describes both the option to select a backup and the option to specify a timestamp for recovery. See Restore an Autonomous Database and Autonomous Database Backup and Restore Overview.

QUESTION NO: 12

Which two statements are true regarding active transactions when scaling OCPUs in an Autonomous Database? (Choose two.)

A. Active transactions are terminated and rolled back

B. Scaling can happen while there are active transactions in the database

C. Active transactions continue running unaffected

D. Active transactions are paused

ANSWER: B C

Explanation:

Scaling OCPUs is an online Autonomous Database operation, so an OCPU scaling request can be submitted while application sessions have active work in progress. The service remains available to users during the operation; scaling does not require stopping the Autonomous Database or draining all sessions before the request can be made. Consequently, “Scaling can happen while there are active transactions in the database” is correct.

Oracle also designs OCPU scaling to preserve transaction continuity. Work that has already begun is allowed to continue, and the scaling workflow manages the resource transition without requiring applications to terminate, roll back, or manually suspend those transactions. This means “Active transactions continue running unaffected” correctly describes the transaction behavior from the application’s perspective. In particular, the availability of the database and integrity of in-flight transactional work are maintained while the service adjusts its compute allocation. Oracle documentation describes manual compute scaling as an online operation and notes that Autonomous Database continues to be available during scaling. See Oracle’s Scale an Autonomous Database Manually documentation and the Autonomous Database Serverless overview for the service’s availability and scaling model.

QUESTION NO: 13

Which Oracle package is used to load data to an Autonomous Database from object storage?

A. DBMS_RPC

B. DBMS_LOAD

C. DBMS_MIGRATE

D. DBMS_CLOUD

ANSWER: D

Explanation:

DBMS_CLOUD is the Oracle-supplied PL/SQL package for accessing cloud object storage and loading its files into Autonomous Database tables. In the standard Autonomous Database ingestion workflow, you first create a credential with `DBMS_CLOUD.CREATE_CREDENTIAL`. That credential securely stores the authentication information required to access the object store. You then call `DBMS_CLOUD.COPY_DATA`, providing the target table, credential name, object URI or URI list, and a format definition. The procedure reads the referenced object-storage files and inserts the parsed data into the database table.

This is designed specifically for Autonomous Database’s cloud-based loading model and supports common delimited-text formats as well as supported structured and columnar formats. It also offers load controls through the format JSON, such as delimiters, header handling, date formats, error handling, and character-set settings. For OCI Object Storage, the file location can be supplied as an object URL, while the credential enables authorized access without embedding secrets in each load statement. Oracle documents `DBMS_CLOUD.COPY_DATA` as the procedure used to copy data from cloud storage into an Autonomous Database table. See the Oracle Autonomous Database documentation for loading data from cloud storage and the DBMS_CLOUD package documentation.

QUESTION NO: 14

While creating an Autonomous Container Database on dedicated infrastructure through the Oracle Cloud Infrastructure (OCI) console, which patch type is offered to be applied during maintenance?

A. Quarterly Bundle Patch (QBP)

B. Prior Release Update Revision (PRUR)

C. Prior Release Update (PRU)

D. Release Update (RU)

ANSWER: D

Explanation:

Release Update (RU) is the patch type offered for maintenance when creating an Autonomous Container Database on Autonomous Database Dedicated infrastructure. An RU is Oracle's regular, cumulative database patching vehicle. It incorporates security fixes, bug fixes, and functional improvements that Oracle has released for the applicable database version. Selecting this maintenance patch type establishes the update stream that Oracle uses to keep the Autonomous Container Database platform current over its lifecycle.

This model fits Autonomous Database Dedicated because Oracle manages the underlying database infrastructure and coordinates maintenance through OCI. During Autonomous Container Database provisioning, the console presents maintenance configuration details, including the database patching choice and its schedule. The RU selection enables the environment to receive Oracle's supported cumulative release maintenance while preserving the managed, automated operational model expected for Autonomous Database.

Oracle's documentation for administering Autonomous Database Dedicated describes configuring and maintaining Autonomous Container Databases, including maintenance-related settings, at Manage Autonomous Container Databases. Oracle also defines the Release Update patching model and its cumulative content in its Database Patching Guide.

QUESTION NO: 15

An organization plans an offline migration of an application schema to Autonomous Database by using Data Pump and protected Oracle Cloud Infrastructure Object Storage. Which three actions are required for this approach? (Choose three.)

A. Create a Data Pump export from the source database.

B. Upload the Data Pump dump files to Oracle Cloud Infrastructure Object Storage.

C. Create a database credential for the protected Object Storage location.

D. Restore the source database backup by using RMAN.

E. Create a Data Guard physical standby database.

ANSWER: A B C

Explanation:

Create a Data Pump export from the source database, **upload the dump files to Object Storage**, and **create a database credential for the Object Storage location** are required parts of this migration pattern. The export creates logical dump files, Object Storage provides accessible staging for the files, and the named credential allows Autonomous Database Data Pump operations to authenticate to protected Object Storage.

RMAN physical restore is not the Data Pump migration workflow for Autonomous Database. Creating a physical standby database is a Data Guard operation, not a prerequisite for importing Data Pump dump files.