Oracle 1Z0-997-26 Dumps

Shared by Puckett on 20-11-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which statement is true regarding the network access and connectivity model of an Oracle Cloud Infrastructure (OCI) Cache with Redis cluster?

Options:

A- It is deployed with a mandatory public IP address to allow external application services to securely connect via TLS.
B- It is deployed exclusively within a virtual cloud network (VCN) and is accessed via a private endpoint within a specific subnet.
C- It requires an official OCI API Gateway to route external and internal application traffic to its primary and replica nodes.
D- It relies on a public load balancer to distribute read and write traffic across different availability domains.
B . It is deployed exclusively within a virtual cloud network (VCN) and is accessed via a private endpoint within a specific subnet.
s
Why B is TRUE:
* Private Isolation by Design: OCI Cache with Redis is a fully managed, secure in-memory database service. For security compliance and low-latency performance, instances are provisioned strictly inside a private subnet within your Virtual Cloud Network (VCN).
* Private Endpoint Access: It exposes a private IP address (private endpoint) within that subnet. Any application or service trying to connect to the Redis cluster must reside within the same VCN, be connected via VCN peering, or route through a secure corporate VPN/FastConnect.
Why the other options are FALSE:
* A is FALSE: OCI Cache with Redis cannot be assigned a public IP address directly. Exposing an in-memory caching layer directly to the public internet is a severe security risk. While it supports encryption in transit via TLS, access remains entirely private.
* C is FALSE: An API Gateway is used to expose, secure, and manage RESTful APIs, not for low-level Redis RESP protocol routing. The application clients connect directly to the Redis private endpoint nodes or use internal Redis cluster routing, without requiring an OCI API Gateway.
* D is FALSE: The service handles internal replication and clustering natively. It does not use or require a public load balancer to distribute traffic. External public load balancers are intended for HTTP/HTTPS web traffic, whereas Redis clients use specialized clustering protocols to discover and route read/write traffic directly to the appropriate primary or replica nodes.

Answer:

B

Question 2

Question Type: MultipleChoice

A retail organization uses OCI Full Stack Disaster Recovery (FSDR) to protect their online storefront, which uses a co-managed Virtual Machine (VM) Database System. The storefront has Data Guard enabled between Region A and Region B, and administrators want to automate role transitions during unplanned outages. To comply with strict security standards, the database team prohibits storing or hardcoding any database administrative credentials within any disaster recovery plans. Which design approach should the architect select to orchestrate database failovers while satisfying this administrative credential security requirement?

Options:

A- Utilize an OCI Function that invokes the OCI Command Line Interface utility to trigger database failover, passing the system user password as an encrypted target environment parameter.
B- Store the administrative database credentials inside OCI Vault, and deploy a custom FSDR user-defined script step that securely retrieves the secrets during the active plan failover execution.
C- Add the co-managed VM Database directly to the DR Protection Group, because FSDR natively integrates with OCI Database service APIs without needing any database administrator user passwords.
D- Register the co-managed VM Database as a non-managed member, and require operators to manually initiate the Data Guard role transition before running the active standby DR plan
C . Add the co-managed VM Database directly to the DR Protection Group, because FSDR natively integrates with OCI Database service APIs without needing any database administrator user passwords.
* C is CORRECT: OCI Full Stack Disaster Recovery (FSDR) features deep, native integration with the OCI Database service control plane for co-managed databases (such as VM and Bare Metal Database Systems). When you add a co-managed VM Database directly as a member of a DR Protection Group, FSDR executes Data Guard role transitions (switchovers and failovers) by communicating directly with the underlying OCI platform service APIs. Because these operations are handled securely at the cloud infrastructure control plane layer, FSDR does not require, store, or mandate the input of database-level administrative credentials (like SYS passwords) to orchestrate the failover.
Incorrect Answers
* A is INCORRECT: Hardcoding or passing passwords---even as encrypted environment parameters---violates the strict security standards requested by the database team and introduces unnecessary operational overhead when native control plane API methods are available.
* B is INCORRECT: While OCI Vault is an excellent solution for managing secrets, creating a custom user-defined script step to retrieve credentials and pass them to the database is completely redundant for a co-managed VM Database System, as FSDR performs this natively

without credentials.
* D is INCORRECT: Registering the database as a 'non-managed member' defeats the fundamental purpose of using Full Stack Disaster Recovery automation, as it forces operators to manually execute the failover step outside of the central DR plan during a high-stress outage.

Answer:

C

Question 3

Question Type: MultipleChoice

Your organization has developed a serverless data processing pipeline using Oracle Functions that executes code in response to user uploads. The function must programmatically read files from a secure OCI Object Storage bucket, perform transformations, and write results back to a different bucket. Security guidelines strictly prohibit the use of static user credentials, auth tokens, or API private keys within the function container or application configuration. As a solutions architect, which design pattern should you recommend to implement secure authentication for the function?

Options:

A- Create a dynamic group containing the function, assign an IAM policy granting it bucket access, and utilize the Instance Principal provider inside the function.
B- Create a dynamic group containing the function, assign an IAM policy granting it bucket access, and utilize the Resource Principal provider inside the function.
C- Create a user group containing a service account user, assign policies for bucket access, and generate a pre-signed request URL to execute inside the function.
D- Create a federated group matching your identity provider, assign policies for bucket access, and configure custom SAML assertion exchanges inside the function.
B . Create a dynamic group containing the function, assign an IAM policy granting it bucket access, and utilize the Resource Principal provider inside the function.
Why it is Correct
* To securely access OCI resources without hardcoding static credentials, OCI Functions relies on Resource Principals.
* Dynamic Group Definition: You define a dynamic group that matches the function or the application containing the function using matching rules (e.g., ALL {resource.type = 'fnfunc', resource.compartment.id = 'ocid1.compartment...'}).
* IAM Policy: You grant this dynamic group permission to manage or read/write objects in the specific Object Storage buckets (e.g., Allow dynamic-group MyFunctionsGroup to manage objects in compartment DevCompartment where all {target.bucket.name='OutputBucket'}).
* Resource Principal Provider: Inside the Python/Go/Java function code, you instantiate the OCI

SDK client using the native Resource Principal Authentication Provider. The OCI runtime automatically handles the token exchange and rotation seamlessly behind the scenes.
Why the Other Options are Incorrect
* A is incorrect: Instance Principals are used to give identity to Compute Instances (virtual machines or bare metal servers). They cannot be used natively within serverless OCI Functions to inherit permissions.
* C is incorrect: Pre-signed URLs are valid workarounds for external consumers, but creating service accounts and managing pre-signed URLs within the pipeline violates the core security directive to avoid managing tokens, user keys, or static account overhead.
* D is incorrect: SAML federation is designed for human user authentication via external identity providers (IdPs). It is not utilized for machine-to-machine or resource-to-resource authentication within OCI serverless components.

Answer:

B

Question 4

Question Type: MultipleChoice

An organization wants to achieve maximum high availability with node failure protection and zero-downtime software maintenance for their workloads on Oracle Cloud Infrastructure (OCI) Base Database Service. Which database edition should they select to support a multi-node Oracle Real Application Clusters (RAC) DB system?

Options:

A- Oracle Database Standard Edition, which allows only single-node virtual machine deployments and does not support any clustering capabilities.
B- Oracle Database Enterprise Edition - High Performance, which contains comprehensive diagnostic packs but does not support multi-node RAC configurations.
C- Oracle Database Enterprise Edition - Extreme Performance, which natively supports two-node RAC configurations alongside Active Data Guard and In-Memory features.
D- Oracle Database Enterprise Edition - Developer, which permits full database features for non-production environments but prohibits multi-node RAC deployments.
C . Oracle Database Enterprise Edition - Extreme Performance, which natively supports two-node RAC configurations alongside Active Data Guard and In-Memory features.
Why C is Correct
* To achieve maximum high availability with active node-failure protection and zero-downtime rolling maintenance on OCI Base Database Service, you must deploy a multi-node Oracle Real Application Clusters (RAC) system.
Within the OCI Base Database Service framework:

* The Extreme Performance Edition is the only software package that includes the licensing options required for clustering, specifically Oracle RAC (which provisions a two-node virtual machine DB system by default).
* It also includes advanced high-availability and optimization features like Active Data Guard, Database In-Memory, and Application Continuity, satisfying maximum availability architecture (MAA) patterns.
Why the Other Options are Wrong
* A is incorrect: Standard Edition 2 on OCI only supports single-node virtual machine deployments and is completely restricted from provisioning or using clustering/RAC features.
* B is incorrect: While the High Performance edition includes diagnostic, tuning, and advanced security packs, it does not include the Real Application Clusters (RAC) package. It is restricted to single-node deployments.
* D is incorrect: The Developer edition is a restricted, single-instance package tailored exclusively for low-cost, non-production R&D environments on Ampere A1 shapes. It does not support RAC, multi-node setups, or Data Guard associations.

Answer:

C

Question 5

Question Type: MultipleChoice

Which capability is NOT natively supported by Oracle Cloud Infrastructure (OCI) Logging when configuring log retention and management?

Options:

A- Organizing different categories of logs, such as service logs and custom logs, into a single logical container called a log group.
B- Configuring a standard log group to natively retain custom log data for up to seven years without using external storage integration.
C- Searching across multiple log groups within a compartment using a unified Logging query language expression.
D- Enabling ingestion of operating system events from compute instances using the Unified Monitoring Agent.
B . Configuring a standard log group to natively retain custom log data for up to seven years without using external storage integration.
Analysis of OCI Logging Capabilities
* Why B is NOT a valid capability: OCI Logging provides fixed retention settings for log groups. Currently, the maximum retention period for logs stored within an OCI Log Group is up to 12 months (365 days). To meet a seven-year retention requirement, you must configure a Service

Connector to automatically archive the log data to an OCI Object Storage bucket, which supports lifecycle policies for long-term archival.
* Why A is valid: Log groups serve as logical containers to organize logs, allowing you to manage retention policies, access control (IAM), and search boundaries for diverse log sources (service, audit, and custom) within a single management entity.
* Why C is valid: OCI Logging supports cross-log-group searching. You can use the Logging Search feature and the Logging Query Language to query multiple log groups simultaneously, provided you have the appropriate IAM permissions across the requested compartments.
* Why D is valid: The Unified Monitoring Agent is the native OCI tool used to collect, process, and ingest OS-level logs (such as Syslog, Windows Event Logs, and application-specific logs) from Compute instances directly into OCI Logging.

Answer:

B

Question 6

Question Type: MultipleChoice

An organization is deploying an Oracle Base Database Service instance inside a secured compartment to host financial transactions. The security compliance team mandates that all database lifecycle operations and management events must be audited and aggregated centrally. Furthermore, access must be restricted so that database administrators cannot modify or delete these event records. As a solutions architect, which approach should you direct your team to follow to fulfill this tracking and compliance requirement?

Options:

A- Enable OCI Audit Logs for the compartment containing the database, and use IAM policies to grant read-only access to the security team while restricting write or delete permissions on the log groups.
B- Configure the Unified Monitoring Agent on the database host to write all control plane events into a custom log file, and give database administrators full ownership of the file to ensure fast local troubleshooting.
C- Deploy an external OCI Streaming pool inside the database compartment to capture api calls, and configure the database instance to directly stream its control plane operations via local shell scripts.
D- Enable OCI Service Logs specifically for the database instance, and configure the database administrators' IAM group with administrative control over the log group to allow flexible log purging.
A . Enable OCI Audit Logs for the compartment containing the database, and use IAM policies to grant read-only access to the security team while restricting write or delete permissions on the

log groups.
Key Architectural Concepts
* OCI Audit Service: This service automatically records all API calls made against OCI resources (Control Plane events) within a compartment. It is the primary mechanism for meeting financial compliance and governance mandates.
* Immutable Integrity via IAM: The core of this solution is the Separation of Duties. By using OCI Identity and Access Management (IAM) policies, you decouple the Database Administrators (who manage the DB) from the Security/Compliance team (who monitor the logs).
* Restriction: You explicitly deny the DBAs the LOG_WRITE or LOG_DELETE permissions for the log groups, ensuring that once an audit record is created, it cannot be tampered with by those managing the database.
* Centralized Aggregation: Audit logs are collected at the tenancy or compartment level, providing a centralized, tamper-evident record of all lifecycle operations (creation, patching, deletion, configuration changes).
Why the other options are incorrect:
* B is incorrect: Granting DBAs 'full ownership' of log files on the host is a severe security violation. It allows them to modify or delete logs to hide unauthorized activity. Furthermore, OCI Audit logs are handled at the platform/control plane level, not through manual local host files.
* C is incorrect: OCI Streaming is a real-time data ingestion platform; it is not a native audit logging service. Configuring database instances to stream control plane events via local scripts is brittle, non-compliant, and introduces significant operational risk.
* D is incorrect: Granting DBAs 'administrative control' (including the ability to purge logs) directly violates the compliance requirement that administrators must not be able to modify or delete audit event records.

Answer:

A

Question 7

Question Type: MultipleChoice

An enterprise uses OCI Full Stack Disaster Recovery (FSDR) to automate cross-region recovery of an application that relies on an external third-party API gateway. During a DR execution, the operations team must run a custom validation script on a specific Linux compute instance in the standby region. The script requires root privileges to restart the gateway service, but the security team strictly prohibits using SSH connections between regions. Which method should the architect select to execute this validation script while satisfying the strict cross-region security constraint?

Options:

A- Deploy an OCI Function that establishes an active SSH connection to the standby instance using a temporary private application key retrieved from OCI Vault at runtime.
B- Configure a user-defined Run Script step in the DR plan that executes the command on the instance via the Oracle Cloud Agent without requiring SSH connections.
C- Utilize OCI Ansible Engine to remotely deploy and run the gateway service script using WinRM or standard SSH protocols across the peered regional network VCN connection.
D- Set up an OCI Event service rule that triggers an automatic email notification prompting standby region operators to log in and manually run the validation script.
B . Configure a user-defined Run Script step in the DR plan that executes the command on the instance via the Oracle Cloud Agent without requiring SSH connections.
* B is CORRECT: OCI Full Stack Disaster Recovery (FSDR) has built-in orchestration capabilities that utilize the Oracle Cloud Agent (specifically the Compute Instance Run Command plugin) natively installed on OCI compute instances. When you add a user-defined 'Run Script' step to an FSDR plan, the execution command is sent securely through the OCI control plane API directly to the Cloud Agent running locally inside the VM. The agent executes the script with root/administrator privileges. This completely eliminates the need to enable, manage, or establish inbound network SSH connections between regions, fully satisfying the security team's constraints.
Incorrect Answers
* A is INCORRECT: This method still relies on establishing an active SSH connection to the standby instance, which directly violates the security team's strict prohibition of cross-region SSH traffic.
* C is INCORRECT: Ansible Engine typically depends on standard SSH (for Linux) or WinRM (for Windows) network communication to connect from a control node to target instances. This approach requires open network paths and protocol access that violate the security policy.
* D is INCORRECT: Forcing operators to log in and manually run a script defeats the objective of using OCI Full Stack Disaster Recovery to create an fully automated, end-to-end orchestrated disaster recovery runbook.

Answer:

B

To Get Premium Files for 1Z0-997-26 Visit
https://www.p2pexams.com/products/1z0-997-26

For More Free Questions Visit
https://www.p2pexams.com/oracle/pdf/1z0-997-26

