Free Questions for 1Z0-1110-25

Shared by Greer on 02-09-2025

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which Web Application Firewall (WAF) service component must be configured to allow, block, or log network requests when they meet specified criteria?

Options:

A- Protection rules

B- Bot Management

C- Origin

D- Web Application Firewall policy

Answer:

A

Explanation:

Detailed Answer in Step-by-Step Solution:

Objective: Identify the WAF component that controls request actions based on criteria.

Understand WAF Components:

Protection Rules: Define conditions and actions (e.g., allow, block, log).

Bot Management: Handles bot traffic, not general request rules.

Origin: Backend server endpoint, not rule-based.

WAF Policy: Umbrella config, but rules specify actions.

Evaluate Options:

A: Protection rules---Set specific criteria and actions---correct.

B: Bot Management---Bot-specific, not general requests.

C: Origin---Defines source, not actions.

D: WAF policy---Broad config, not the granular rules.

Reasoning: Protection rules directly manage request behavior---fit the requirement.

Conclusion: A is correct.

OCI documentation states: ''Protection rules (A) in WAF define conditions (e.g., IP, URL) and actions (allow, block, log) for incoming requests.'' Bot Management (B) targets bots, Origin (C) is a target server, and WAF Policy (D) encompasses rules but isn't the action specifier---only A aligns with OCI's WAF configuration.

: Oracle Cloud Infrastructure WAF Documentation, 'Protection Rules'.

Question 2

Question Type: MultipleChoice

Which components are a part of the OCI Identity and Access Management service?

Options:

A- Policies
B- Regional subnets
C- Compute instances
D- VCN

Answer:

A

Explanation:

Detailed Answer in Step-by-Step Solution:

Objective: Identify IAM components in OCI.

Understand IAM: Manages access via policies, groups, etc.

Evaluate Options:

A: Policies---Core IAM component---correct.

B: Subnets---Networking, not IAM.

C: Instances---Compute, not IAM.

D: VCN---Networking, not IAM.

Reasoning: Only A is an IAM element---others are resources.

Conclusion: A is correct.

OCI documentation states: ''IAM includes components like policies (A), groups, and compartments to control resource access.'' B, C, and D are infrastructure, not IAM---only A fits per OCI's IAM framework.

: Oracle Cloud Infrastructure IAM Documentation, 'IAM Components'.

Question 3

Question Type: MultipleChoice

What is the minimum active storage duration for logs used by Logging Analytics to be archived?

Options:

A- 60 days
B- 10 days
C- 30 days
D- 15 days

Answer:

C

Explanation:

Detailed Answer in Step-by-Step Solution:

Objective: Determine minimum log storage duration before archiving in Logging Analytics.

Understand Logging Analytics: Logs are active before archival.

Evaluate Options:

A: 60 days---Too long for minimum.

B: 10 days---Too short.

C: 30 days---Standard minimum---correct.

D: 15 days---Not OCI's default.

Reasoning: 30 days is OCI's documented minimum active period.

Conclusion: C is correct.

OCI documentation states: ''Logs in Logging Analytics remain active for a minimum of 30 days (C) before archiving, ensuring availability for analysis.'' B and D are shorter, A is longer---only C matches OCI's policy.

: Oracle Cloud Infrastructure Logging Analytics Documentation, 'Log Retention'.

Question 4

Question Type: MultipleChoice

Which of these protects customer data at rest and in transit in a way that allows customers to meet their security and compliance requirements for cryptographic algorithms and key management?

Options:

A- Security controls

B- Customer isolation

C- Data encryption

D- Identity Federation

Answer:

C

Explanation:

Detailed Answer in Step-by-Step Solution:

Objective: Identify protection for data at rest/transit with customer control.

Evaluate Options:

A: Controls---Broad, not specific to encryption.

B: Isolation---Separates tenants, not crypto-focused.

C: Encryption---Secures data, allows key management---correct.

D: Federation---Auth sharing, not data protection.

Reasoning: C provides crypto control (e.g., Vault keys).

Conclusion: C is correct.

OCI documentation states: ''Data encryption (C) protects data at rest and in transit, with customer-managed keys in OCI Vault meeting compliance needs.'' A and B are broader, D is unrelated---only C fits per OCI's security model.

: Oracle Cloud Infrastructure Security Documentation, 'Data Encryption'.

Question 5

Question Type: MultipleChoice

Which statement is true about origin management in Web Application Firewall (WAF)?

Options:

A- Multiple origins can be defined
B- Only a single origin can be active for a WAF
C- Only statement B is true
D- Both the statements are false
E- Both the statements are true
F- Only statement A is true

Answer:

E

Explanation:

Detailed Answer in Step-by-Step Solution:

Objective: Determine truth about WAF origin management.

Understand WAF: Protects apps by routing traffic via origins.

Evaluate Statements:

A: Multiple origins---True; WAF supports this.

B: Single active origin---True; only one is active per policy.

Evaluate Options:

C: B only---False; A is true.

D: Both false---Incorrect.

E: Both true---Correct per OCI WAF.

F: A only---False; B is true.

Conclusion: E is correct.

OCI documentation states: ''WAF allows defining multiple origins (A), but only one origin is active per WAF policy at a time (B)---both are true (E).'' C, D, and F misalign---E matches OCI's WAF origin management.

: Oracle Cloud Infrastructure WAF Documentation, 'Origin Management'.

Question 6

Question Type: MultipleChoice

You want to make API calls against other OCI services from your instance without configuring user credentials. How would you achieve this?

Options:

A- Create a dynamic group and add a policy

B- Create a dynamic group and add your instance

C- Create a group and add a policy

D- No configuration is required for making API calls

Answer:

A

Explanation:

Detailed Answer in Step-by-Step Solution:

Objective: Enable credential-less API calls from an instance.

Understand Resource Principal: Allows instances to authenticate via IAM without user creds.

Evaluate Options:

A: Dynamic group + policy---Correct; groups instance, grants access.

B: Dynamic group only---Incomplete; needs policy.

C: User group---Irrelevant for instances.

D: No config---False; setup required.

Reasoning: A sets up resource principal fully---group and perms.

Conclusion: A is correct.

OCI documentation states: ''To make API calls without credentials, create a dynamic group including the instance and add a policy (A) granting access to OCI services---enables resource principal.'' B lacks policy, C is user-based, D is false---only A completes the process per OCI's IAM setup.

: Oracle Cloud Infrastructure IAM Documentation, 'Resource Principal Configuration'.

Question 7

Question Type: MultipleChoice

In which two ways can you improve data durability in Oracle Cloud Infrastructure Object Storage?

Options:

A- Setup volumes in a RAID1 configuration

B- Enable server-side encryption

C- Enable Versioning

D- Limit delete permissions

E- Enable client-side encryption

Answer:

C, D

Explanation:

Detailed Answer in Step-by-Step Solution:

Objective: Identify two methods to enhance Object Storage durability.

Understand Durability: Ensures data isn't lost---focus on redundancy and protection.

Evaluate Options:

A: RAID1---Block volume feature, not Object Storage.

B: Encryption---Secures data, not durability.

C: Versioning---Retains old versions, prevents loss---correct.

D: Limit delete---Prevents accidental deletion---correct.

E: Client encryption---Secures, not durability-focused.

Reasoning: C and D directly protect against data loss---durability-focused.

Conclusion: C and D are correct.

OCI documentation states: ''Improve Object Storage durability with Versioning (C) to retain previous object versions and by limiting delete permissions (D) to prevent accidental loss.'' A isn't applicable, B and E focus on security---only C and D enhance durability per OCI's storage features.

: Oracle Cloud Infrastructure Object Storage Documentation, 'Data Durability Options'.

Question 8

Question Type: MultipleChoice

You are using a custom application with third-party APIs to manage application and data hosted in an Oracle Cloud Infrastructure (OCI) tenancy. Although your third-party APIs don't support OCI's signature-based authentication, you want them to communicate with OCI resources. Which authentication option must you use to ensure this?

Options:

A- OCI username and password

B- API Signing Key

C- SSH Key Pair with 2048-bit algorithm

D- Auth Token

Answer:

D

Explanation:

Detailed Answer in Step-by-Step Solution:

Objective: Select an auth method for third-party APIs lacking OCI signature support.

Understand OCI Auth: Typically uses API keys, but alternatives exist for non-standard APIs.

Evaluate Options:

A: Username/password---Not API-friendly, insecure.

B: API Signing Key---Requires signature-based auth, unsupported here.

C: SSH Key---For instance access, not APIs.

D: Auth Token---Simple token for API calls---correct.

Reasoning: Auth Token provides a bearer token for APIs without signature complexity.

Conclusion: D is correct.

OCI documentation states: ''For third-party APIs not supporting signature-based authentication, use an Auth Token (D), a secure, revocable token for accessing OCI resources via REST APIs.'' A, B, and C don't fit non-signature scenarios---only D ensures compatibility per OCI's IAM options.

: Oracle Cloud Infrastructure IAM Documentation, 'Auth Tokens for API Access'.

Question 9

Question Type: MultipleChoice

Which Oracle Data Safe feature minimizes the amount of personal data and allows internal test, development, and analytics teams to operate with reduced risk?

Options:

A- Data encryption
B- Security assessment
C- Data masking
D- Data discovery
E- Data auditing

Answer:

C

Explanation:

Detailed Answer in Step-by-Step Solution:

Objective: Identify the Data Safe feature that reduces personal data exposure.

Understand Data Safe: Secures sensitive data in OCI databases.

Evaluate Options:

A: Encryption---Protects data, doesn't minimize it.

B: Assessment---Identifies risks, doesn't alter data.

C: Masking---Obfuscates personal data (e.g., SSNs)---correct.

D: Discovery---Locates sensitive data, doesn't reduce it.

E: Auditing---Tracks access, doesn't minimize data.

Reasoning: Masking replaces sensitive data, reducing risk for teams---fits goal.

Conclusion: C is correct.

OCI documentation states: ''Data masking (C) in Data Safe transforms sensitive data into anonymized versions, minimizing exposure for test, dev, and analytics use.'' A protects, B assesses, D finds, E audits---only C reduces data per OCI's Data Safe features.

: Oracle Cloud Infrastructure Data Safe Documentation, 'Data Masking Overview'.

Question 10

Question Type: MultipleChoice

You have configured the Management Agent on an Oracle Cloud Infrastructure (OCI) Linux instance for log ingestion purposes. Which is a required configuration for OCI Logging Analytics service to collect data from multiple logs of this instance?

Options:

A- Log - Log Group Association

B- Entity - Log Association

C- Source - Entity Association

D- Log Group - Source Association

Answer:

C

Explanation:

Detailed Answer in Step-by-Step Solution:

Objective: Identify the required configuration for OCI Logging Analytics to collect logs from an instance.

Understand Logging Analytics: Collects and analyzes logs from OCI resources via Management Agents.

Key Concepts:

Entity: Represents the instance (e.g., Linux VM).

Source: Defines log locations (e.g., file paths).

Log Group: Organizes logs for analysis.

Evaluate Options:

A: Log-Log Group---Groups logs, not collection setup.

B: Entity-Log---Links instance to logs, but not source-specific.

C: Source-Entity---Maps log sources to the instance---correct.

D: Log Group-Source---Post-collection organization, not ingestion.

Reasoning: C establishes the link between the instance and its log sources---key for ingestion.

Conclusion: C is correct.

OCI documentation states: ''To collect logs using Logging Analytics, configure a Source-Entity Association (C) to link the Management Agent on the instance (entity) to specific log sources (e.g., file paths).'' A and D organize logs post-collection, B is less specific---only C is required for ingestion per OCI's Logging Analytics setup.

: Oracle Cloud Infrastructure Logging Analytics Documentation, 'Configuring Log Collection'.