Free Questions for C1000-172 by actualtestdumps

Shared by Owen on 10-09-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which two options describe the capabilities of IBM Cloud Block Storage for VPC?

Options:

A- Provides a highly available, durable, and secure platform for storing unstructured data

B- Stores volume data redundantly across multiple physical disks in an availability zone

C- Provides storage in a separate zone to the compute resources and on a high-speed communication channel

D- Provides primary boot volumes and secondary data volumes

E- Provides fast, flexible network-attached, NFS-based storage

Answer:

B, D

Explanation:

The capabilities of IBM Cloud Block Storage for VPC are:

Stores Volume Data Redundantly Across Multiple Physical Disks in an Availability Zone: IBM Cloud Block Storage is designed to provide redundancy and durability by storing data across multiple physical disks within the same availability zone. This ensures data availability and protection against disk failures.

Provides Primary Boot Volumes and Secondary Data Volumes: Block Storage in IBM Cloud VPC can be used as both primary boot volumes for the operating system and secondary data volumes for storing additional data.

Reference from IBM Cloud Professional Architect Materials:

IBM documentation on IBM Cloud Block Storage for VPC outlines these capabilities, including redundant data storage and support for both boot and data volumes.

Other options are incorrect:

A . Provides a highly available, durable, and secure platform for storing unstructured data describes object storage, not block storage.

C . Provides storage in a separate zone is incorrect; storage is typically within the same zone as compute resources.

E . Provides fast, flexible network-attached, NFS-based storage describes a different type of storage.

Therefore, the correct answers are B. Stores volume data redundantly across multiple physical disks in an availability zone and D. Provides primary boot volumes and secondary data volumes.

Question 2

Question Type: **MultipleChoice**

What is used to allow provisioning of a large number of virtual server instances at the same time when using IBM Cloud Virtual Private Cloud?

Options:

A- Instance Models

B- Instance Replication Policies

C- Instance Groups

D- Instance Scaling Policies

Answer:

C

Explanation:

Instance Groups are used to allow provisioning of a large number of virtual server instances at the same time when using IBM Cloud Virtual Private Cloud (VPC).

IBM Cloud VPC Instance Groups: Instance Groups provide a way to manage a group of identical virtual server instances within a VPC. They support auto-scaling, load balancing, and rolling updates, making it easier to manage a large number of instances.

Use Case for Large Deployments: When an organization needs to deploy multiple instances simultaneously, Instance Groups simplify the process by providing a template and scaling policies.

Reference from IBM Cloud Professional Architect Materials:

IBM documentation on Instance Groups for VPC describes how they are used for managing large-scale deployments.

Other options are incorrect:

A . Instance Models refer to the types or configurations of instances, not to mass provisioning.

B . Instance Replication Policies do not exist in this context.

D . Instance Scaling Policies manage scaling but are not used for the initial provisioning of multiple instances.

Question 3

Question Type: **MultipleChoice**

An organization is using IBM Log Analysis to manage operating system logs, application logs, and platform logs in IBM Cloud. A developer discovered their Red Hat OpenShift on IBM Cloud instance is not being captured in the service.

What could be a reason Log Analysis is missing the Red Hat OpenShift on IBM Cloud instance logs?

Options:

A- The developer needs at least editor IAM role to the Log Analysis instance

B- The administrator needs at least reader access to the Red Hat OpenShift instance

C- The Red Hat OpenShift on IBM Cloud instance is running in a different region from the Log Analysis instance

D- The logging agents were not created and deployed to this OpenShift instance

Answer:

D

Explanation:

The likely reason IBM Log Analysis is missing the Red Hat OpenShift on IBM Cloud instance logs is that the logging agents were not created and deployed to this OpenShift instance.

IBM Log Analysis with Sysdig: To collect logs from a Red Hat OpenShift cluster, specific logging agents must be deployed on the cluster. These agents are responsible for forwarding logs to the IBM Log Analysis service.

Missing Logs Due to Missing Agents: If the agents are not deployed, the service will not capture logs from the cluster, resulting in missing log data from that instance.

Reference from IBM Cloud Professional Architect Materials:

IBM documentation on Setting up Log Analysis explains the requirement of deploying logging agents to the respective resources to ensure log collection.

Other options are incorrect:

A . The developer needs at least editor IAM role does not affect the log capture.

B . The administrator needs at least reader access does not address the missing agents.

C . The instance running in a different region does not prevent log capture if agents are configured correctly.

Question 4

Question Type: MultipleChoice

An organization wants to secure its exposed APIs running on IBM Cloud API Connect Reserved Instances using OAuth and OpenID.

Which capabilities can help in this case?

Options:

A- Authentication and authorization capabilities are offered by IBM API Connect itself

B- IBM API Connect APIs must be secured by a third party as API Connect is responsible for managing the API life cycle only

C- IBM API Connect is providing authentication, but authorization can be provided by IAM

D- IBM API Connect creates user registries, but OAuth isn't allowed in API Connect, and this can be done by a third-party provider

Answer:

A

Explanation:

IBM API Connect offers both authentication and authorization capabilities to secure APIs using OAuth and OpenID.

IBM API Connect Security Features: IBM API Connect provides built-in capabilities for managing OAuth and OpenID Connect authentication and authorization flows. It allows users to define security policies that enforce these protocols to protect APIs.

Use of OAuth and OpenID: API Connect enables organizations to create user registries, apply security policies, and manage tokens for OAuth 2.0 and OpenID Connect, providing end-to-end security management for APIs.

Reference from IBM Cloud Professional Architect Materials:

IBM documentation on API Security in IBM API Connect confirms that API Connect handles both authentication and authorization for securing APIs.

Other options are incorrect:

B . IBM API Connect APIs must be secured by a third party is false; API Connect itself provides these capabilities.

C . IBM API Connect is providing authentication, but authorization can be provided by IAM is incorrect because API Connect manages both.

D . IBM API Connect creates user registries, but OAuth isn't allowed is incorrect; OAuth is fully supported.

Question 5

Question Type: MultipleChoice

What describes a feature of IBM Cloud Transit Gateway when interconnecting multiple virtual private clouds (VPC)?

Options:

A- Client designates which traffic remains within the private IBM Cloud backbone

B- Provides private interconnectivity for on-premises workloads and the designated VPC

C- Provisions and defines connections between resources on the IBM Cloud network

D- Provides a decentralized hub for better regional connectivity and load balancing

Answer:

C

Explanation:

IBM Cloud Transit Gateway provides the ability to provision and define connections between resources on the IBM Cloud network.

IBM Cloud Transit Gateway: This service allows you to connect multiple Virtual Private Clouds (VPCs) and on-premises networks to a central gateway. It simplifies network management by providing a single entry point for interconnecting multiple resources across the IBM Cloud.

Connectivity Between Resources: By creating connections through the Transit Gateway, an organization can establish a scalable and flexible network architecture that integrates various cloud resources.

Reference from IBM Cloud Professional Architect Materials:

According to IBM documentation on IBM Cloud Transit Gateway, it provides centralized management and provisioning of connections across different IBM Cloud environments.

Other options are incorrect:

A . Client designates which traffic remains within the private IBM Cloud backbone is not specifically managed by the Transit Gateway.

B . Provides private interconnectivity for on-premises workloads and the designated VPC is more related to Direct Link.

D . Provides a decentralized hub for better regional connectivity and load balancing is incorrect since Transit Gateway is a centralized solution.

Question 6

Question Type: MultipleChoice

Monitoring data can be considered sensitive by some clients. How can a client configure IBM Cloud Monitoring so that sensitive monitoring data is not traveling across the public internet?

Options:

A- Encrypt all monitoring data with a user-controlled key from Key Protect or Hyper Protect Crypto Services

B- Configure the monitoring instance and monitoring agents to only use private endpoints

C- Ensure that all resources being monitored are in the same region as the IBM Cloud monitoring instance

D- Use only private endpoints to store monitoring data in IBM Cloud Object Storage

Answer:

B

Explanation:

To ensure that sensitive monitoring data does not travel across the public internet, a client can configure the monitoring instance and monitoring agents to only use private endpoints.

IBM Cloud Monitoring Private Endpoints: IBM Cloud Monitoring with Sysdig allows users to configure their monitoring instance and agents to communicate only over private endpoints. This configuration ensures that monitoring data remains within IBM's private network, thus avoiding exposure to the public internet.

Private Endpoints for Data Security: Using private endpoints is crucial for clients who require that their sensitive data, such as monitoring metrics, never leave the secure IBM Cloud network, enhancing overall security.

Reference from IBM Cloud Professional Architect Materials:

IBM Cloud documentation on Configuring Private Endpoints for IBM Cloud Monitoring confirms that monitoring data can be restricted to private endpoints to avoid exposure to the public internet.

Other options are incorrect:

A . Encrypt all monitoring data with a user-controlled key from Key Protect or Hyper Protect Crypto Services does not prevent data from traveling across the public internet.

C . Ensure that all resources being monitored are in the same region as the IBM Cloud monitoring instance is a good practice for performance but does not specifically ensure that data doesn't travel over the public internet.

D . Use only private endpoints to store monitoring data in IBM Cloud Object Storage is related to storage, not monitoring data transmission.

Therefore, the correct answer is B. Configure the monitoring instance and monitoring agents to only use private endpoints.

Question 7

Question Type: MultipleChoice

Which encryption option allows clients to have control over the keys used to encrypt their block storage volumes, file shares, and custom images?

Options:

A- Provider-managed encryption

B- Client-managed encryption

C- IBM-managed encryption

D- Custom encryption

Answer:

B

Explanation:

Client-managed encryption allows clients to have full control over the encryption keys used to protect their block storage volumes, file shares, and custom images on IBM Cloud. This option ensures that only the client has access to the keys and, therefore, to the data.

Benefits of Client-Managed Encryption: Clients retain control over key management, including generation, rotation, and deletion, ensuring compliance with security policies and regulatory requirements.

Comparison with Other Options:

A (Provider-managed encryption): Managed by IBM, not by the client.

C (IBM-managed encryption): Similar to provider-managed, where IBM controls the keys.

D (Custom encryption): Not a specific term used in IBM Cloud documentation for this feature.

IBM Cloud Data Encryption Documentation

IBM Cloud Architect Exam Study Guide

Question 8

Question Type: **MultipleChoice**

Which two are benefits of using the IBM Cloud Transit Gateway to connect IBM Cloud VPCs?

Options:

A- Connectivity over the internet

B- Connectivity between multiple VPCs and PowerVS

C- Default connectivity to services in multiple regions

D- Direct Link connectivity to multiple VPCs and classic networking

Answer:

B, D

Explanation:

IBM Cloud Transit Gateway provides secure and scalable connectivity between multiple IBM Cloud VPCs (Virtual Private Clouds) and other IBM Cloud resources, including PowerVS (Power Virtual Servers) and classic networking environments.

Benefits:

Connectivity Between Multiple VPCs and PowerVS: Allows seamless networking between VPCs and PowerVS, supporting hybrid and multi-cloud architectures.

Direct Link Connectivity: Supports direct, high-speed private connectivity between VPCs and classic IBM Cloud infrastructure, enabling secure communication without traversing the public internet.

Comparison with Other Options:

A (Connectivity over the internet): Transit Gateway provides private connectivity, not public internet connectivity.

C (Default connectivity to services in multiple regions): Not a direct benefit of Transit Gateway, as regional connectivity may require additional configuration.

IBM Cloud Transit Gateway Documentation

IBM Cloud Architect Exam Study Guide