Free Questions for NS0-604

Shared by Patel on 16-04-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which administrator can customize Alerts and Notification settings in NetApp BlueXP?

Options:

A- Tenant Administrator
B- Connector Administrator
C- Account Administrator
D- Workspace Administrator

Answer:

C

Explanation:

In NetApp BlueXP, the Account Administrator has the authority to customize alerts and notification settings. The Account Administrator role is responsible for managing the overall configuration of the BlueXP environment, including setting up and modifying alerts to monitor system health and performance, ensuring that the appropriate notifications are sent when issues arise.

Other roles like Tenant Administrator (A), Connector Administrator (B), and Workspace Administrator (D) have more limited scopes of control, and they are not responsible for managing global alert and notification settings.

Question 2

Question Type: MultipleChoice

A company has finished migrating all data to NetApp Cloud Volumes ONTAP. An application administrator needs to make sure that there are no interruptions in service for this new NFSv4 application.

Which feature must be registered on the Azure subscription to reduce unplanned failover times?

Options:

A- multipath HA
B- high availability
C- fault tolerance
D- redundancy

Answer:

B

Explanation:

NetApp Cloud Volumes ONTAP provides a High Availability (HA) configuration, which is crucial for ensuring that services remain available even during unplanned outages. When using NetApp Cloud Volumes ONTAP in environments such as Azure, ensuring continuous availability, especially for NFSv4 workloads, is vital.

The 'High Availability' (HA) feature creates a pair of ONTAP instances configured as an active-passive cluster. This setup reduces failover times by allowing one node to take over if the other fails, providing minimal service disruption. HA is designed to manage failovers automatically, which is essential for applications requiring constant availability, such as those using NFSv4. In Azure, enabling this feature via the appropriate subscription registration ensures that when an unexpected failure occurs, the system will automatically failover to the standby node, minimizing downtime and ensuring that the application continues to function smoothly without manual intervention.

In this case, 'multipath HA,' 'fault tolerance,' and 'redundancy' are related concepts, but they don't directly address the specific need to register and enable the high-availability feature in Azure. Registering HA on the Azure subscription ensures that the Cloud Volumes ONTAP can perform its failover processes effectively, keeping the application running.

Question 3

Question Type: MultipleChoice

When considering security for Azure NetApp Files, what is a key security consideration to avoid a breach of confidentiality?

Options:

A- application of network security groups
B- Virtual Network Encryption
C- encryption using Kerberos with AES-256
D- double encryption at rest

Answer:

D

Explanation:

For securing Azure NetApp Files and ensuring the confidentiality of data, a critical security feature is double encryption at rest. This technique involves encrypting the data twice at rest, once at the storage level using Azure's default encryption and again using NetApp's built-in encryption features such as NetApp Volume Encryption (NVE). Double encryption provides an additional layer of protection, significantly reducing the risk of data breaches or unauthorized access.

While network security groups (A) and Kerberos encryption (C) play roles in protecting network traffic and securing authentication, they do not address the need for data encryption at rest, which is critical for confidentiality. Virtual Network Encryption (B) is also related to encrypting network data but doesn't focus on encryption at rest.

In highly regulated environments where data confidentiality is paramount, double encryption at rest ensures that even if one encryption layer is compromised, the data remains protected by the second encryption layer, thereby greatly enhancing security.

Question 4

Question Type: MultipleChoice

A company needs to efficiently do a one-time, non-NetApp file migration to Amazon FSx for NetApp ONTAP with millions of files. The company needs to view file analytics to get better insights.

Which NetApp tool should the company use?

Options:

A- BlueXP copy & sync
B- BlueXP replication
C- XCP

D- BlueXP volume caching

Answer:

C

Explanation:

For a one-time, non-NetApp file migration to Amazon FSx for NetApp ONTAP, especially with millions of files, XCP is the most suitable tool. XCP (NetApp's eXtensible Copy Program) is optimized for high-performance file migrations and can handle large-scale migrations efficiently. Additionally, it provides file analytics, which can help the company gain better insights into the data being migrated.

BlueXP copy & sync (A) and BlueXP replication (B) are not designed for large-scale one-time migrations like XCP, and BlueXP volume caching (D) is not relevant for migrations or analytics.

Question 5

Question Type: MultipleChoice

A company wants to save on AWS infrastructure costs for NetApp Cloud Volumes ONTAP. They want to tier to Amazon Simple Storage Service (Amazon S3).

What is the best way for the company to create a connection to S3 without incurring egress charges?

Options:

A- peering
B- gateway endpoint
C- AWS PrivateLink
D- network address translation (NAT) device

Answer:

B

Explanation:

When setting up NetApp Cloud Volumes ONTAP to tier to Amazon S3, minimizing infrastructure

costs, especially egress charges, is critical. The best way to create a connection to S3 without incurring egress charges is by using an AWS gateway endpoint.

Gateway endpoints enable a private connection between Amazon S3 and your Amazon Virtual Private Cloud (VPC), eliminating the need for internet-based routing, which would incur data transfer charges (egress fees). With this private connection, data is transferred directly between the VPC and S3 without crossing the public internet, thus avoiding egress costs.

Other options such as peering and PrivateLink are viable for connecting VPCs but do not specifically address the elimination of egress charges when connecting to S3. A NAT device is also unnecessary for this scenario and would not eliminate egress charges but could instead introduce additional costs. Therefore, the gateway endpoint is the most cost-effective and direct method for achieving the desired outcome.

P2P exams