NetApp NS0-304 Practice Questions

Shared by Hicks on 22-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An administrator is asked to set up a Cloud Volumes ONTAP (CVO) with high availability in AWS using all default configuration settings. Where is the IAM role created?

Options:

A- Cloud Volumes ONTAP
B- BlueXP
C- AWS Systems Manager
D- AWS console

Answer:

D

Explanation:

When setting up Cloud Volumes ONTAP (CVO) with high availability in AWS, the creation of an IAM role associated with CVO is performed in the AWS console. Here's the process:

Role Creation in AWS Console: The IAM role must be created within the AWS console. This role is crucial as it grants the Cloud Volumes ONTAP instance the necessary permissions to access other AWS services as required by its configuration and operational needs.

Permissions Configuration: The IAM role should be configured with policies that provide the appropriate permissions for services that CVO needs to interact with, such as S3 for storage, EC2 for compute resources, and others depending on the specific setup.

Associate IAM Role with CVO: Once created, the IAM role is then associated with the CVO instance during its setup process in the AWS console or through BlueXP, which automates and manages NetApp configurations in cloud environments.

For detailed guidelines on creating and configuring IAM roles for Cloud Volumes ONTAP in AWS, please consult the AWS documentation and NetApp setup guides for CVO: NetApp CVO AWS Documentation.

Question 2

Question Type: MultipleChoice

Which two network connections are required by the Connector to enable Cloud Tiering from on-premises to a public cloud? (Choose two.)

Options:

A- An HTTPS connection to the ONTAP cluster management LIF
B- An SSH connection to the ONTAP cluster management LIF
C- An inbound Internet connection to the Cloud Tiering service
D- An outbound Internet connection to the Cloud Tiering service

Answer:

A, D

Explanation:

To enable Cloud Tiering from on-premises to a public cloud, the Connector requires two specific network connections:

HTTPS Connection to ONTAP Cluster Management LIF: This connection allows the Connector to communicate securely with the management interface of the ONTAP cluster. It's essential for managing storage operations and configuring cloud tiering.

Outbound Internet Connection to the Cloud Tiering Service: This is necessary for the Connector to reach the Cloud Tiering service hosted in the cloud. It ensures that data can be moved between the on-premises environment and the cloud tiering service, facilitating storage tiering operations.

These connections ensure that the on-premises systems can effectively interact with cloud services, maintaining operational continuity and enabling efficient data management.

For additional information on setting up network connections for Cloud Tiering, you can refer to the NetApp Cloud Tiering documentation: NetApp Cloud Tiering Documentation.

Question 3

Question Type: MultipleChoice

An administrator needs to move several volumes that contain iSCSI LUNs from an ONTAP AFF cluster to CVO. Which method should be used?

Options:

A- SnapMirror
B- XCP
C- Foreign LUN Import (FLI)
D- CloudSync

Answer:

A

Explanation:

To move several volumes containing iSCSI LUNs from an ONTAP AFF cluster to Cloud Volumes ONTAP (CVO), the most appropriate method is using SnapMirror. Here's the process:

Utilizing SnapMirror for LUN Migration: SnapMirror is NetApp's replication technology that is ideally suited for efficiently transferring data between ONTAP systems, including from AFF to CVO. It is capable of handling complex data structures like iSCSI LUNs, ensuring data integrity and consistency during the transfer.

Configuration of SnapMirror: Set up a SnapMirror relationship between the source AFF cluster and the destination CVO instance. This involves configuring the SnapMirror policy, scheduling the replication, and initializing the transfer of data.

Advantages for iSCSI LUNs: SnapMirror maintains the layout and attributes of the iSCSI LUNs during replication, which is crucial for ensuring that the storage is ready for immediate use upon completion of the replication to the CVO environment.

For step-by-step instructions on configuring and using SnapMirror for transferring iSCSI LUNs, consult the NetApp documentation on SnapMirror: NetApp SnapMirror Documentation.

Question 4

Question Type: MultipleChoice

An administrator has two Kubernetes clusters: one uses GKE, and the other uses AKS. The administrator wants to migrate from Google to Azure. The migration must be application aware and move all components and data for the application.

Which product should the administrator use?

Options:

A- BlueXP Copy and Sync
B- SnapMirror
C- Astra Control Service
D- Cloud Backup Service

Answer:

C

Explanation:

For migrating applications between Kubernetes clusters---specifically from Google Kubernetes Engine (GKE) to Azure Kubernetes Service (AKS)---and ensuring that all components and data are moved in an application-aware manner, the best product to use is Astra Control Service. Here's why:

Application-Aware Migration: Astra Control Service is designed to manage, protect, and move applications in Kubernetes environments. It understands the structure of Kubernetes applications and can manage the entire lifecycle, including migration of application data along with its configuration and state.

Cross-Platform Capability: Astra Control Service supports multiple Kubernetes platforms, making it suitable for migrations from GKE to AKS. It ensures that all parts of the Kubernetes application, including persistent volumes and configurations, are consistently replicated to the new environment.

Seamless Migration Process: The service automates much of the migration process, reducing the complexity and potential for error when moving applications between different cloud providers or Kubernetes services.

For more detailed guidance on using Astra Control Service for Kubernetes migrations, refer to the NetApp documentation: NetApp Astra Control Service Documentation.

Question 5

Question Type: MultipleChoice

How many VPCs are required to deploy CVO in Google Cloud?

Options:

A- 4

B- 6
C- 2
D- 3

Answer:

C

Explanation:

To deploy Cloud Volumes ONTAP (CVO) in Google Cloud, typically two Virtual Private Clouds (VPCs) are required. This configuration generally involves:

A VPC for the management of CVO operations, handling management traffic, control plane operations, and other administrative activities.

A VPC dedicated to data traffic, ensuring data security and optimal network performance for storage operations.

This dual-VPC architecture helps in isolating management operations from data operations, providing enhanced security and performance. The management VPC can handle tasks like software updates and system monitoring, while the data VPC focuses purely on serving storage requests, thereby optimizing traffic flows and security policies accordingly.

For more detailed deployment instructions and VPC configuration guidelines, the official NetApp documentation on deploying Cloud Volumes ONTAP in Google Cloud provides comprehensive guidance.

Question 6

Question Type: MultipleChoice

An administrator wants to use BlueXP Observability to generate notifications whenever a volume in a FlexGroup on a GCP CVO system is nearing capacity.

Which option should the administrator use?

Options:

A- Data Collection API
B- Service Level Annotation
C- Log Monitor
D- AIQ ConfigAdvisor

Answer:

A

Explanation:

To generate notifications whenever a volume in a FlexGroup on a GCP CVO system is nearing capacity using BlueXP Observability, the Data Collection API should be utilized. This option allows for the configuration of customized monitoring and alerting based on specific data points and thresholds. Here's the process:

Setup Data Collection API: Configure the Data Collection API to monitor volume capacity metrics within your FlexGroup. This involves setting up the API to pull or receive data points related to storage utilization.

Define Alerts: Set thresholds for when capacity is considered nearing its limit (e.g., 80% full). Configure alerts to be triggered when these thresholds are approached, ensuring administrators are notified in advance to take necessary actions.

Implement Notification System: Integrate the alerting mechanism with your organization's notification system (e.g., email alerts, SMS, or a dashboard) to inform the relevant stakeholders or administrators promptly.

For detailed instructions on configuring the Data Collection API and setting up monitoring and alerting in BlueXP Observability, refer to the NetApp BlueXP documentation and API guides: NetApp BlueXP Documentation.

Question 7

Question Type: MultipleChoice

Which hyperscaler offers annual contracts for Cloud Tiering?

Options:

A- Azure
B- Oracle Cloud
C- GCP
D- AWS

Answer:

A

Explanation:

Azure offers annual contracts for Cloud Tiering services. This contract model can be particularly appealing for organizations looking to manage costs while still leveraging the cloud for scalable storage solutions. Here's why:

Azure Subscription and Billing Flexibility: Azure provides various subscription models that include reserved capacity options, which can be used for cloud tiering. These options typically come with cost benefits associated with longer-term commitments, such as annual contracts.

Cost Management: By committing to an annual contract, organizations can benefit from lower pricing compared to pay-as-you-go rates, helping manage and predict cloud storage costs more effectively.

For specific details on Azure's pricing models and contract options for services like Cloud Tiering, it's recommended to review the Azure pricing page or contact Azure support for the most current information and offers: Azure Pricing.

Question 8

Question Type: MultipleChoice

An administrator is running a modern workload using Red Hat OpenShift in AWS. The administrator uses Cloud Volumes ONTAP for persistent volumes. The administrator now needs to back up all required application data.

Which solution should the administrator use?

Options:

A- Astra Control Center
B- Cloud Backup Service
C- Astra Control Service
D- Astra Trident

Answer:

B

Explanation:

For backing up application data in an environment running Red Hat OpenShift on AWS with

Cloud Volumes ONTAP providing persistent storage, the best solution is Cloud Backup Service. Here's why:

Integration with Cloud Volumes ONTAP: Cloud Backup Service is seamlessly integrated with Cloud Volumes ONTAP, making it a suitable choice for backing up data stored on ONTAP volumes. This service supports backups directly to cloud storage services like Amazon S3, providing an efficient and scalable storage solution.

Protection for OpenShift Applications: Cloud Backup Service can efficiently handle the backup needs of containerized applications managed by OpenShift, ensuring that all persistent data associated with these applications is regularly backed up.

Ease of Use and Configuration: Cloud Backup Service offers a straightforward setup and management experience through BlueXP, allowing administrators to easily configure and monitor backup policies and schedules.

For more detailed information on using Cloud Backup Service with Cloud Volumes ONTAP in AWS, refer to NetApp's official documentation: NetApp Cloud Backup Service Documentation.

Question 9

Question Type: MultipleChoice

An administrator is preparing to automate firmware updates with the help of Active IQ Digital Advisor. Which automation tool should the administrator use?

Options:

A- Puppet
B- Terraform
C- Ansible
D- Pulumi

Answer:

C

Explanation:

To automate firmware updates effectively using Active IQ Digital Advisor, the best tool to use is Ansible. Here's why:

Ansible Integration with NetApp: Ansible is widely recognized for its powerful automation

capabilities across various IT environments. NetApp provides specific Ansible modules designed to interact with its storage solutions and services, including the automation of firmware updates.

Active IQ Digital Advisor Integration: Active IQ Digital Advisor offers predictive analytics, actionable intelligence, and proactive recommendations. By using Ansible, administrators can automate the implementation of these recommendations, including firmware updates, to enhance efficiency and reliability in operations.

To implement this, the administrator needs to leverage the NetApp Ansible modules that are specifically designed for storage management tasks. This can be found in the NetApp Automation Store, where administrators can access pre-built playbooks for firmware updates, simplifying the automation process.

For further details and specific implementation steps, please refer to the NetApp Automation Store and the official NetApp documentation on Ansible integration: NetApp Ansible Modules Documentation.

Question 10

Question Type: MultipleChoice

Refer to the exhibit.



An administrator is deploying the latest version of CVO via BlueXP. What will be the result of leaving the option disabled?

Options:

A- After applying a license, the feature will automatically be activated.
B- BlueXP will automatically configure new volumes with encryption.
C- BlueXP will include this option again during new volume creation.
D- BlueXP will automatically create future volumes as non-SnapLock.

Answer:

D

Explanation:

In the context of deploying Cloud Volumes ONTAP (CVO) via BlueXP, if the administrator chooses to leave the WORM (Write Once Read Many) option disabled, the default behavior for newly created volumes will be as non-SnapLock volumes. Here's what this implies:

Non-SnapLock Volumes: Leaving the WORM feature disabled means that new volumes will not be created with the SnapLock compliance feature activated. SnapLock is used to ensure data immutability for compliance and regulatory purposes, protecting files from being altered or deleted before a predetermined retention period expires.

Volume Configuration Flexibility: Administrators will have the option to activate SnapLock or other data protection features on a per-volume basis in the future if needed, but this would need to be explicitly configured.

Impact on Data Management: This choice affects how data is managed in terms of compliance and security. Without SnapLock enabled by default, the volumes will operate under standard data management policies, which do not include immutability protections.

For more information on the implications of enabling or disabling SnapLock and how it affects volume creation in Cloud Volumes ONTAP, please refer to the NetApp BlueXP and SnapLock documentation: NetApp SnapLock Documentation.

P2P exams

To Get Premium Files for NS0-304 Visit

https://www.p2pexams.com/products/ns0-304

For More Free Questions Visit

https://www.p2pexams.com/netapp/pdf/ns0-304

