Vendor: Network Appliance

Exam Code: NS0-304

Exam Name: NetApp Certified Hybrid Cloud - Administrator

Version: DEMO

QUESTION 1
An administrator is troubleshooting a Cloud Data Sense deep scan that failed on a Cloud Volumes ONTAP (CVO) NFS export. The scan worked a day ago with no errors. The administrator notices that the NFS export is on a volume with a recently modified export policy rule. Which export policy rule modification will resolve this issue?

A. superuser
B. krb
C. read
D. anon

Answer: C
Explanation:
If a Cloud Data Sense deep scan of an NFS export fails after a recent modification to the export policy rule, the most critical setting to check and adjust is the read permission. Here's how to resolve the issue:
Review the Modified Export Policy: Access the export policy settings for the NFS volume that Cloud Data Sense is attempting to scan. Check for recent changes that might have restricted read access. Modify Export Policy to Allow Read Access: Ensure that the export policy rule specifically permits read access. This permission is essential for Cloud Data Sense to read the data stored on the NFS export and perform the scan effectively.
Apply Changes and Re-test the Scan: After adjusting the export policy to ensure read access, re-run the Cloud Data Sense scan to confirm that the issue is resolved and that the scan completes successfully.

QUESTION 2
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?

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.

QUESTION 3
ONTAP's Autonomous Anti-ransomware engine reports a potential ransomware attack. The administrator finds the majority of the files appear encrypted and disables the share. What should the administrator do to minimize data loss?

A. Create a FlexClone using the locked snapshot and re-enable the share
B. Perform a SnapRestore using the weekly snapshot and re-enable the share
C. Rehost the volume to a different SVM and create a new share
D. Take a manual snapshot and re-enable the share

Answer: B
Explanation:
When dealing with a potential ransomware attack where files appear encrypted, it is crucial to restore the affected data to a point before the corruption occurred. The best course of action in this scenario is to perform a SnapRestore using a known good weekly snapshot and then re-enable the share.
Assess the Snapshots: Verify that you have snapshots that predate the ransomware attack. These snapshots should be intact and free from encryption or corruption. Perform a SnapRestore: Use the SnapRestore operation to quickly revert the entire volume to the state captured in the selected weekly snapshot. SnapRestore is efficient because it does not involve data movement; it simply reverts pointers in the filesystem. Re-enable the Share: After successfully reverting the volume to a good state, the share can be safely re-enabled, allowing users to access the clean, restored data. Verify System Integrity and Security: Before re-enabling the share, ensure that all system vulnerabilities are addressed to prevent future attacks. Implement improved security measures as needed.

QUESTION 4
An outbound Internet connection is not available to send AutoSupport messages. BlueXP has automatically configured the Cloud Volumes ONTAP systems to use the Connector as a proxy server. The Connector requires an inbound connection on port 3128.
What must the administrator do?

A. Add the Internet gateway IP to the allow list
B. Modify the associated security group
C. Modify the policy on the cluster-mgmt LIF
D. Configure BlueXP with an external IP address

Answer: B
Explanation:
When BlueXP has configured Cloud Volumes ONTAP systems to use the Connector as a proxy server, and the Connector requires an inbound connection on port 3128, the necessary action is to modify the associated security group. Here's what to do:
Identify Security Group: Determine which security group is associated with the Cloud Volumes ONTAP or the Connector instance.
Modify Security Group Rules: Update the security group rules to allow inbound traffic on port 3128. This is crucial to enable the Connector to receive connections as a proxy server for sending AutoSupport messages.
Apply and Verify Changes: After updating the security group, apply the changes and verify that the Connector can successfully transmit AutoSupport messages through the specified port.

QUESTION 5
An administrator is using the NetApp BlueXP API to perform actions within an CI/CD process.
What information is needed for authentication?

A. API endpoint and Java web token
B. API endpoint and API token
C. API endpoint and username/password

D. API endpoint with bearer token

Answer: D
Explanation:
For authenticating with the NetApp BlueXP API, particularly within a CI/CD process, you will need the API endpoint and a bearer token. Here's why this is important:
API Endpoint: The API endpoint is the URL where the API requests are sent. It serves as the access point for the BlueXP services.
Bearer Token: A bearer token is a type of access token that is often used in OAuth 2.0 authentication. It must be included in the header of each API request to authenticate and authorize the request. This token ensures that the person or system making the API request has the correct permissions. Setup Authentication: To set up authentication, you must first obtain a bearer token, typically through a login API endpoint that provides this token after verifying your credentials. Subsequently, include this token in the "Authorization" header of your API requests.

QUESTION 6
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?

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.

QUESTION 7
Which option is supported with SnapLock Compliance?

A. Aggregate Rename
B. Audit Logging
C. System Reinitialization
D. MetroCluster Configuration

Answer: B
Explanation:

SnapLock Compliance is a feature in NetApp ONTAP systems that ensures data immutability for compliance with regulatory standards. Among the options listed, Audit Logging is supported with SnapLock Compliance.
Purpose of Audit Logging: Audit Logging in the context of SnapLock Compliance records access and modification attempts on immutable files. This is crucial for compliance purposes, as it provides a traceable log of all operations performed on protected data. Compliance Requirements: Many regulatory frameworks require audit trails for access and changes to sensitive data. SnapLock's integration with audit logging features helps organizations meet these requirements by ensuring that all data interactions are logged and reviewable.

QUESTION 8
An administrator has iSCSI LUNs on an AWS FSxN instance. The administrator is unable to mount the LUNs from a Linux host in the same AWS region. The Linux host is in a different VPC than FSxN. What must the administrator configure to resolve this issue?

A. BGP peering
B. SVM peering
C. Cluster peering
D. VPC peering

Answer: D
Explanation:
If an administrator has iSCSI LUNs on an AWS FSxN instance and is unable to mount these LUNs from a Linux host in the same AWS region due to the host being in a different Virtual Private Cloud (VPC), the solution is to configure VPC peering.
VPC Peering Setup: VPC peering allows two VPCs to communicate with each other as if they are in the same network. This enables the Linux host to connect to the AWS FSxN instance across different VPCs.
Configuration Steps: To set up VPC peering, the administrator must create a peering connection between the two VPCs in the AWS Management Console, and then update the route tables in each VPC to allow traffic to and from each other.
Mounting iSCSI LUNs: Once VPC peering is configured, the network route will be established, allowing the Linux host to successfully mount the iSCSI LUNs located on the FSxN instance.

QUESTION 9
An administrator must configure a fan-out SnapMirror architecture from an on-premises, four-node cluster to highly available instances of Cloud Volumes ONTAP (CVO) in both Azure and GCP. How many Intercluster LIFs are required to connect the three clusters?

A. 8
B. 3
C. 12
D. 6

Answer: C
Explanation:
When configuring a fan-out SnapMirror architecture from an on-premises four-node cluster to highly available instances of Cloud Volumes ONTAP (CVO) in both Azure and GCP, you will need to establish intercluster LIFs (Logical Interface) to connect the three clusters.
Intercluster LIFs per Node: Typically, at least one intercluster LIF is required per node in a cluster to facilitate SnapMirror replication. This is necessary for network communication dedicated to data replication between clusters.
Total LIFs Calculation:

On-premises four-node cluster: 4 LIFs (one per node)
Each CVO instance in Azure and GCP: Assuming each is a two-node setup, 4 LIFs per CVO instance (2 nodes x 2 LIFs each for redundancy and high availability). Total LIFs = 4 (on-prem) + 4 (Azure CVO) + 4 (GCP CVO) = 12 LIFs. Redundancy and Availability: Given the critical nature of maintaining connectivity for HA instances in both Azure and GCP, configuring two LIFs per node in the cloud environments ensures redundancy and enhances reliability.
This setup ensures that each node in every cluster can maintain an independent connection for data replication, vital for a robust and efficient fan-out architecture.

QUESTION 10
Which hyperscaler offers annual contracts for Cloud Tiering?

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.
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.

QUESTION 11
In an environment using Cloud Backup Service, a user reports that an urgently needed file cannot be found. The end user knows the file name but does not know when the file was last accessed or when it was deleted.
Which feature should be used?

A. Restore Volume
B. Browse & Restore
C. Search & Restore
D. Previous Versions

Answer: C
Explanation:
In a situation where an end user needs to find and restore a file whose last access or deletion time is unknown, the best feature to use within the Cloud Backup Service is Search & Restore.
Search Functionality: The Search & Restore feature allows users to quickly locate files within backup datasets using just the file name or other metadata. This is particularly useful when the exact details of the file, such as its last access date or deletion date, are unknown. Efficient File Restoration: Once the file is located using the search functionality, it can be selectively restored to the desired location without the need to restore an entire volume, making the process efficient and tailored to the specific recovery need.
User-Friendly Interface: Cloud Backup Service typically provides a user-friendly interface for conducting searches and performing restores, making it accessible even to users who may not be deeply technical.

QUESTION 12
An administrator deploys FSx for ONTAP as a storage solution in their cloud environment. The administrator cannot mount the file system to their cloud instances in the same VPC.
What should the administrator do?

A. Configure a new Transit Gateway dedicated to FSx for ONTAP data traffic
B. Verify the inbound/outbound rules of the security group for the VPC
C. Make sure that autofs is enabled on the cloud instance operating system
D. Create a new virtual private gateway dedicated to FSx for ONTAP data traffic

Answer: B
Explanation:
When an administrator is unable to mount the file system from FSx for ONTAP to cloud instances within the same Virtual Private Cloud (VPC), the issue often lies with the network security settings. Specifically, verifying and adjusting the inbound and outbound rules of the security group associated with the VPC can resolve the issue. Here's the recommended approach:
Check Security Group Settings: Examine the security group rules associated with the cloud instances and the FSx for ONTAP system. Ensure that the rules allow NFS (or SMB/CIFS, depending on the protocol used) traffic between the instances and the FSx for ONTAP. Adjust Rules as Necessary: If the current settings do not permit the required network traffic, modify the security group rules to allow the appropriate ports and protocols (e.g., TCP/UDP for NFS on port 2049).
Test Connectivity: After updating the security group settings, attempt to mount the file system again to confirm that the issue has been resolved.

QUESTION 13
An administrator is using application templates to deploy and configure volumes in BlueXP. They try to use a template to discover existing volumes and scan them for PII by enabling BlueXP Classification. The template fails to execute.
What should the administrator do?

A. Create new volume templates with BlueXP Classification enabled
B. Add a tag to the application template to enable BlueXP Classification
C. Make sure that the BlueXP Classification service is active and licensed
D. List each volume they want to scan in the template definition

Answer: C
Explanation:
If an administrator encounters issues with executing an application template designed to discover existing volumes and enable BlueXP Classification, it's essential to ensure that the BlueXP Classification service itself is active and properly licensed. Here's the process:
Verify Service Activation: Check within the BlueXP management console to confirm that the Classification service is enabled and functioning as expected. Check Licensing: Ensure that the correct licenses are in place for using the Classification service. This may require reviewing your service agreement or contacting NetApp support for license verification. Resolve Service Issues: If the service is not active or properly licensed, take the necessary steps to activate or procure the appropriate licenses. Once this is done, retry the template execution.

Thank You for Trying Our Product

Passleader Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.passleader.com/all-products.html

10% Discount Coupon Code: **ASTR14**