NetApp NS0-528 Practice Questions

Shared by Powell on 22-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Your IT company is using NetApp FlexClone on a two node AFF cluster with 20TB of data to rapidly provision environments for each developer.

Each environment is replicated to an eight node AFF C-Series cluster at a DR site using SnapMirror. You notice that the environments are consuming significantly more disk space on the destination cluster than on the source cluster.

In this scenario, which action will minimize the disk usage on the destination cluster?

Options:

A- Consolidate the SnapMirror destination volumes onto a single aggregate.
B- Distribute the SnapMirror destination volumes evenly across the available aggregates.
C- Enable SnapMirror network compression.
D- Enable Flexclone copies on the DR side.

Answer:

D

Explanation:

FlexClone volumes are space-efficient on the source cluster because they share blocks with the parent. However, SnapMirror transfers them as full physical copies by default unless you re-create them as FlexClone volumes on the DR site.

Enabling FlexClone copies on the destination will preserve their space efficiency and minimize disk usage on the DR cluster.

Question 2

Question Type: MultipleChoice

What NetApp data protection solution ensures that data cannot be accessed if a disk shelf is stolen?

Options:

A- snapshot volume
B- IPsec
C- disk encryption
D- SnapLock volume

Answer:

B

Explanation:

Disk encryption (such as NetApp Storage Encryption or NetApp Volume Encryption) ensures that data stored on disks is inaccessible if a disk or disk shelf is stolen, because the data is encrypted at rest and requires keys that are not stored on the hardware itself.

Question 3

Question Type: MultipleChoice

A ransomware attack has compromised all files on a CIFS share. The volume had a retention policy of five daily Snapshot copies, but unfortunately, no Snapshot copies were available. It was confirmed that the cybercriminal accessed only the share and did not gain access to the NetApp ONTAP cluster.

What command should be executed to prevent the quick restore strategy from being compromised?

Options:

A- volume autosize -autogrow disable
B- security multi-admin-verify modify -enabled true
C- volume modify -snapdir-access false
D- volume snapshot -autodelete disabled

Answer:

C

Explanation:

Setting snapdir-access to false prevents users accessing the CIFS/NFS share from viewing or deleting Snapshot copies via the .snapshot directory. This secures the Snapshot restore mechanism from being exposed or tampered with in case of another attack through file shares.

Question 4

Question Type: MultipleChoice

A customer wants to enable tamper-proof Snapshot copies on volume LockingVolume, which is hosted on SVM LockingSVM. They have created the Snapshot policy, including the required retention set. However, when they apply the policy to a volume, the Snapshot copies are not locked.

Which command must the customer issue before tamper-proof Snapshot copies can be enabled?

Options:

A- volume modify -volume LockingVolume -anti-ransomware-state enable
B- volume modify -volume LockingVolume -snapdir-access false
C- snaplock event-retention apply -vserver LockingSVM
D- snaplock compliance-clock initialize -node *

Answer:

D

Explanation:

To enable tamper-proof (locked) Snapshot copies using SnapLock, the SnapLock Compliance Clock must be initialized on all nodes in the cluster. Without initializing this clock, locked Snapshots cannot be created, even if the policy and retention settings are configured.

Question 5

Question Type: MultipleChoice

When backing up on-premises NetApp ONTAP volumes to tape using NDMP, which two engines are supported by ONTAP software? (Select two.)

Options:

A- tar
B- SMTape
C- cpio
D- dump

Answer:

B, D

Explanation:

When using NDMP (Network Data Management Protocol) to back up ONTAP volumes to tape, ONTAP supports two backup engines:

SMTape: Used for block-level backups.

dump: Used for file-level backups.

These are the only engines supported by ONTAP for NDMP-based tape backups.

Question 6

Question Type: MultipleChoice

Your customer replicates between two on-premises NetApp ONTAP clusters with an hourly schedule. Two days ago they made network changes, and nobody checked the ONTAP clusters. Today they notice a SnapMirror replication lag time of two days. To avoid this happening again, they want to receive an email alert if the replication lag time will be more than 1.5 hours.

Which NetApp tool can send a lag threshold alert?

Options:

A- Active IQ Config Advisor
B- Active IQ OneCollect
C- ONTAP System Manager
D- Active IQ Unified Manager

Answer:

D

Explanation:

Active IQ Unified Manager can monitor SnapMirror relationships and generate email alerts based on lag threshold policies. You can configure it to trigger an alert when the replication lag exceeds 1.5 hours, helping prevent unnoticed replication issues.

Question 7

Question Type: MultipleChoice

An administrator is setting up SnapMirror SVM replication. One of the source data volumes uses cloud tiering with the snapshot-only tiering policy.

Which cloud tiering policy is supported on the destination volume?

Options:

A- none
B- auto
C- all
D- snapshot-only

Answer:

D

Explanation:

When using SnapMirror SVM replication, the cloud tiering policy on the destination volume must match the source if tiering is to be preserved. The only supported tiering policy in this context is snapshot-only, which moves cold Snapshot blocks to cloud tier. This ensures compatibility during replication.

Question 8

Question Type: MultipleChoice

A customer wants to replicate between their two NetApp ONTAP clusters but is concerned that replication traffic might slow down normal data traffic. They still have two unused network ports on every node. You recommend using dedicated ports for the Intercluster LIFs, and you are tasked with creating the Intercluster LIFs so that they are on dedicated ports at all times.

Which command must you use before creating InterCluster LIFs?

Options:

A- system services firewall policy create
B- network interface failover-groups create
C- network ipspace create -ipspace
D- network interface service-policy create

Answer:

D

Explanation:

To ensure Intercluster LIFs are bound to dedicated ports and used only for replication traffic, you must first create a service policy that defines the LIF's role (e.g., intercluster). The network interface service-policy create command allows you to specify that the LIF is intended strictly for intercluster services, ensuring it's isolated from data traffic.

Question 9

Question Type: MultipleChoice

What NetApp tool helps you with the configuration for the cluster switches, when you are expanding an existing 4-node MetroCluster IP setup?

Options:

A- Active IQ Config Advisor
B- Interoperability Matrix Tool
C- RCF generator
D- Active IQ Upgrade Advisor

Answer:

C

Explanation:

The RCF (Reference Configuration File) generator is the NetApp tool used to create the appropriate switch configuration files for MetroCluster IP setups. When expanding a MetroCluster IP configuration (e.g., from 4 nodes to more), you use the RCF generator to ensure the cluster and interconnect switches are properly configured.

P2P exams

Question 10

Question Type: MultipleChoice

You need to upgrade to NetApp ONTAP 9.12.1 software on your source cluster in a SnapMirror relationship. The source cluster differs from the destination cluster and you want to take advantage of version-flexible SnapMirror replication.

Which option should you Choose?

Options:

A- SnapMirror automatically converts existing DP-type relationships to XDP-type relationships.
B- Run the command snapmirror resync and set the type to XDP.
C- Delete the XDP-type relationship and create a new DP-type relationship.
D- Delete the DP-type relationship and create a new XDP-type relationship.

P2P exams

Answer:

D

Explanation:

To take advantage of version-flexible SnapMirror (introduced with XDP-type relationships), you must delete the existing DP-type relationship and create a new one using type XDP. DP-type relationships do not support version flexibility, which allows the source and destination clusters to run different ONTAP versions.

Question 11

Question Type: MultipleChoice

Your customer wants to use tamper-proof Snapshot copies on a SnapMirror destination volume only.

You successfully created a SnapMirror relationship using a SnapMirror policy that contains the following rules:

```
Rules:
SnapMirror Label  Keep Preserve Warn  Schedule Prefix Retention Period
----------------- ---- -------- ----  -------- ------ ----------------
sm_created           1 false       0  -        -                     -
hourly               5 false       0  -        -                     -
daily                5 false       0  -        -                  5days
```

After initializing, you are able to delete a daily Snapshot copy.

Which command did you need to modify to enable the tamper-proof Snapshot copies as specified in the policy?

Options:

A- volume modify -snapshot-locking-enabled
B- volume snaplock modify -privileged-delete
C- vserver modify -snapshot-policy
D- volume snapshot modify -expiry-time

Answer:

A

Explanation:

Although the SnapMirror policy includes rules for retaining Snapshot copies, the ability to make them tamper-proof (i.e., locked) depends on enabling snapshot locking on the destination volume. You must explicitly run:

volume modify -volume <vol_name> -snapshot-locking-enabled true

Without this setting, SnapMirror-created Snapshot copies can still be deleted manually. Enabling snapshot-locking ensures that retention rules (like the 5-day daily rule in your policy) are enforced and Snapshots are immutable.

To Get Premium Files for NS0-528 Visit

https://www.p2pexams.com/products/ns0-528

For More Free Questions Visit

https://www.p2pexams.com/netapp/pdf/ns0-528

