DUMPSBOSS.

NetApp Certified Support Engineer (NCSE)

Netapp NS0-194

Version Demo

Total Demo Questions: 8

Total Premium Questions: 84

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

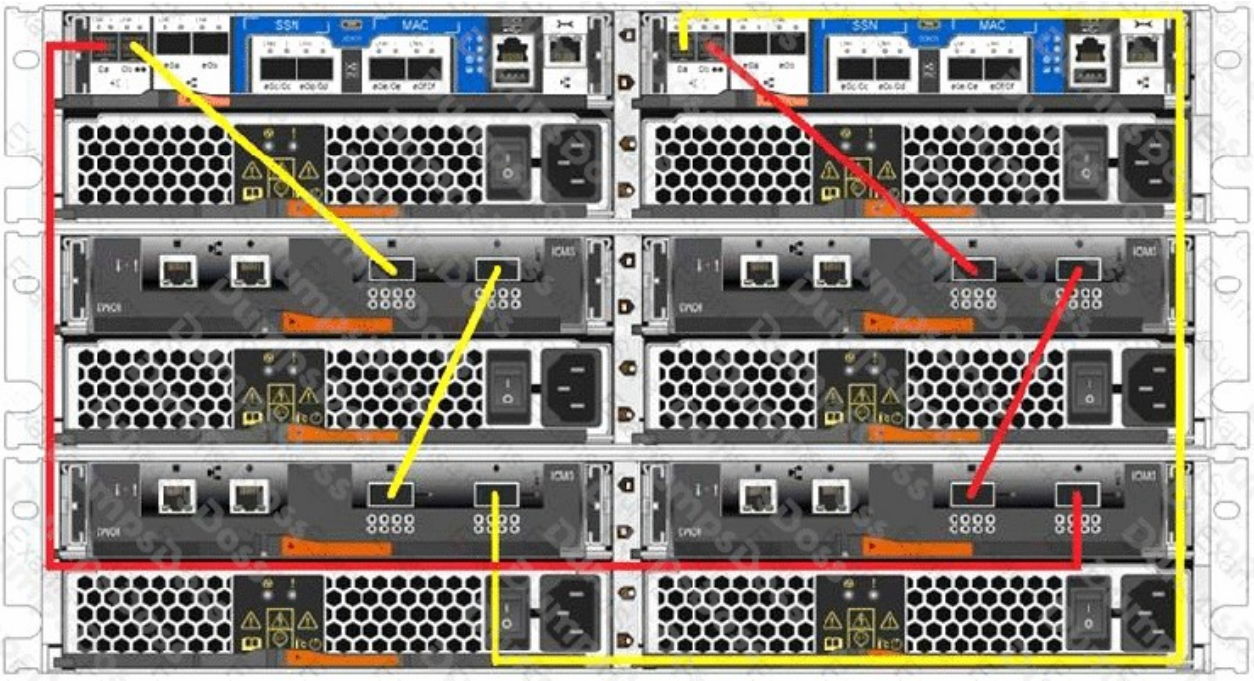
Topic	No. of Questions
Topic 1, Support Processes	6
Topic 2, ONTAP Administration	45
Topic 3, ONTAP Troubleshooting	17
Topic 4, Hardware Troubleshooting	16
Total	84

QUESTION NO: 1

You receive the error shown below on a FAS2750 HA pair.

Mon Jun 24 00:27:30 UTC [NetappA: scsi_cmdblk_strthr_admin: scsi.cmd.checkCondition:error]: Unknown device 0a.00.99: Check Condition: CDB 0x12: Sense Data SCSI:hardware error - (0x4 - 0x44 0x0 0x0) (0).

The system is cabled as shown in the exhibit.



What should you do to clear the error?

A. Replace the cable connected to controller A's 0a port.

B. Replace the controller of controller

C. Replace the controller of controller

D. Re-cable the system per the FAS2750 installation guide.

ANSWER: D

Explanation:

Re-cable the system per the FAS2750 installation guide. The event identifies a SCSI inquiry/check-condition failure for a device reached through SAS port 0a. In a FAS2750 high-availability configuration, each controller's SAS paths must be connected to the prescribed shelf I/O modules and ports so that ONTAP can discover the expected devices through redundant, valid SAS paths. An incorrect SAS connection can cause a controller to probe an unexpected target address, resulting in an "Unknown device" message and SCSI hardware-error sense data even when the controller and cable themselves are functional.

Restoring the documented cabling topology removes the invalid path and permits correct device discovery. After correcting the connections, allow time for SAS discovery to complete, then review system health and event logs to confirm that the condition no longer recurs. The FAS2700-series installation documentation provides the supported cabling procedures and diagrams for the platform, while the ONTAP documentation describes monitoring system health and hardware status after maintenance. Follow the applicable documented procedure for the installed shelf configuration and avoid changing cabling while the system is not prepared for the maintenance action.

References: NetApp FAS2700 Series detailed installation guide; NetApp ONTAP system health management documentation.

QUESTION NO: 2

A customer has reported an unexplained reboot of an ONTAP node that did not generate a panic string or a core file.

In this scenario, which two sets of logs do you collect to further diagnosis the issue? (Choose two.)

A. system core

B. sp status

C. events all

D. sp status -d

ANSWER: C D

Explanation:

`events all` and `sp status -d` provide the most useful evidence for investigating a node reboot that did not produce a panic string or core dump. The complete event output captures EMS events around the reboot window, including node-state transitions, hardware- or environmental-condition messages, service failures, and other cluster activity that can establish a timeline for the incident. EMS is ONTAP's central event-management mechanism, so its records are essential for correlating the reboot with conditions observed by the node and cluster.

The detailed Service Processor output obtained through `sp status -d` supplies diagnostic information from the out-of-band controller. Because the Service Processor remains independently available during many node operating-system failures and resets, its detailed status and log information can preserve evidence of power, watchdog, reset, hardware, or boot-related activity that is not present in a core file. Together, these collections give Support both the ONTAP-side event history and the independent management-controller view needed to determine the reboot path. See NetApp's EMS event management documentation and Service Processor management documentation.

QUESTION NO: 3

A customer is showing disk utilization is at 100% in Active IQ even though there are low protocol operations on the controller. You review the data shown in the exhibit.

disk	ut%	xfers	ureads--chain-usecs		writes--chain-usecs		
/aggr0/plex0/rg0:							
6b.34	1	2.18	0.17	1.00 10700	0.98	13.49	490
6a.19	1	2.35	0.17	1.00 36600	1.15	11.83	504
6a.45	13	17.98	16.88	2.13 5810	0.53	8.81	887
6b.18	13	17.57	16.55	2.17 5357	0.42	11.00	1189
6a.29	12	16.70	15.30	2.15 5820	0.60	6.75	1996
6b.25	13	18.31	17.13	2.17 5611	0.48	7.59	1709
6b.39	100	15.44	15.07	2.22 191927	0.00	....	.
6a.17	12	16.75	15.52	2.10 6126	0.50	8.63	1475
6b.38	12	16.98	15.95	2.09 5614	0.43	9.92	1349

In this situation, what should you do?

A. Replace disks 6b.34 and 6a.19.

B. Add disks to the aggregate to bring down the average utilization.

C. Replace disk 6b.39.

D. Reseat shelf module

ANSWER: C

Explanation:

Replace disk 6b.39. The exhibit indicates that this individual disk is sustaining 100% utilization despite the controller receiving relatively little protocol workload. This pattern points to a disk-level performance or media problem rather than normal aggregate demand: a single disk can become saturated by retries, recovery activity, or abnormal internal I/O while client-facing operations remain low. The appropriate support action is therefore to replace the identified disk, using the documented ONTAP disk-replacement procedure and confirming the replacement disk is suitable for the affected aggregate or RAID group. After replacement, ONTAP reconstructs the required data onto the spare disk and the disk-level utilization condition should be monitored to verify that it clears. Before physically removing hardware, follow standard NetApp maintenance practice: identify the disk by its exact ownership and location, validate its state and relevant event messages in ONTAP, and ensure that a suitable spare is available. NetApp documents the workflow for identifying and replacing failed or suspect disks, including the requirement to use a compatible replacement and allow reconstruction to complete. See ONTAP: Replace a failed disk and ONTAP: Manage spare disks.

QUESTION NO: 4

What are two supported cabling methods for a NetApp HCI compute node? (Choose two.)

A. 1-cable configuration

B. 2-cable configuration

C. 6-cable configuration

D. 4-cable configuration

ANSWER: B C

Explanation:

NetApp HCI compute nodes support both the 2-cable configuration and the 6-cable configuration. The 2-cable configuration uses the node's paired network connections to carry the required storage and management-related connectivity through an appropriate network design, reducing the physical cable count. This model is useful where a consolidated network design is planned while still providing the network connectivity needed for compute-node operation in an HCI deployment.

The 6-cable configuration is also supported and provides dedicated physical connections for the required traffic paths. It is intended for environments that use a more physically separated network design, including dedicated links for storage traffic and other host and management connectivity. NetApp's deployment planning guidance documents these supported compute-node cabling choices and requires that the selected design be applied consistently with the switch, VLAN, and network-service prerequisites for the installation.

Choosing between these two designs depends on the customer's network architecture, redundancy requirements, available switch ports, and traffic-separation policy. The cabling method must be established before deployment because it determines the switch-port and network configuration used during compute-node installation. See the NetApp HCI network cabling requirements and the NetApp HCI network configuration requirements.

QUESTION NO: 5

You want to configure ONTAP NAS auditing for file access events.

Which two NAS protocols can generate ONTAP audit events? (Choose two.)

A. SMB

B. NFS

C. FCP

D. iSCSI

ANSWER: A B

Explanation:

ONTAP auditing supports file and directory audit events for SMB and NFS access. SMB auditing can record Windows security events, while NFS auditing records supported NFS file and directory access events. Audit records are written in EVTX or XML format according to the audit configuration.

FCP and iSCSI are block protocols and do not generate NAS file-access audit events. See the ONTAP NAS auditing documentation.

QUESTION NO: 6

What is the consequence of a loss of connectivity between a Cloud Volumes ONTAP (CVO) instance and Cloud Manager for four or more days?

A. The CVO instance sends an AutoSupport message.

B. The CVO instance must be added back manually to Cloud Manager.

C. Cloud Manager removes the CVO instance from its inventory.

D. The CVO instance is stopped.

ANSWER: C

Explanation:

Cloud Manager removes the CVO instance from its inventory. More precisely, the Cloud Volumes ONTAP working environment is removed from the Cloud Manager inventory after Cloud Manager has been unable to communicate with it for four or more days. This inventory action prevents Cloud Manager from continuing to display and manage a working environment whose current state it can no longer verify. The Cloud Volumes ONTAP system itself and its cloud resources are not deleted by this inventory removal; the event concerns the management representation maintained by Cloud Manager. Once connectivity and the required management communications are restored, the existing system can be discovered and added back to management without recreating its storage configuration. This behavior is important during troubleshooting because it separates a management-plane connectivity issue from the operational state of the deployed storage system. NetApp's Cloud Volumes ONTAP documentation describes Cloud Manager/BlueXP management of working environments and the procedures used to manage an existing system. See the NetApp Cloud Volumes ONTAP overview and NetApp documentation for managing Cloud Volumes ONTAP state.

QUESTION NO: 7

While troubleshooting client access issues to a CIFS share, you notice that the issue only occurs when the data LIF that the clients are accessing is on a specific node in the cluster.

In this scenario, which configuration should you review to determine why this issue is happening?

A. cluster health

B. Kerberos

C. share path

D. export policies

ANSWER: B

Explanation:

Kerberos is the appropriate configuration to review because SMB/CIFS client authentication to an Active Directory domain normally uses Kerberos. A node-specific symptom can occur when the affected node cannot properly communicate with a domain controller or KDC, has an issue obtaining or validating Kerberos tickets, or has domain-controller discovery and

connectivity behavior that differs from the rest of the cluster. Since clients succeed when the data LIF is hosted elsewhere, validating the Kerberos and Active Directory authentication path from the affected node is a focused way to isolate the issue.

Review the SVM's CIFS server domain membership, the discovered domain controllers, DNS resolution, network reachability to the KDC services, and the event logs for authentication failures. Also confirm that the CIFS server computer account and its secure channel with Active Directory remain healthy. ONTAP provides commands and event information for viewing domain-controller configuration and diagnosing SMB authentication behavior. NetApp documents how to manage the domain controllers used by an SMB server in Modify domain controller configuration and provides broader SMB administration guidance in the ONTAP SMB administration documentation.

QUESTION NO: 8

You are configuring an external KMIP key manager for an ONTAP cluster.

Which two certificate types are required to establish the secure key-management relationship? (Choose two.)

A. a client certificate

B. a server CA certificate

C. an SSH host key

D. an IPsec certificate

ANSWER: A B

Explanation:

ONTAP requires a client certificate and a server CA certificate when configuring an external KMIP key manager. The client certificate identifies and authenticates the ONTAP cluster to the external key manager. The server CA certificate allows ONTAP to validate the certificate presented by the KMIP server.

These certificates establish the mutually trusted TLS connection used for external key-management operations. See the ONTAP external key management documentation.