Mar-2025 FREE Network Appliance NS0-093 PRACTICE QUESTIONS AND ANSWERS UPDATES [Q14-Q35

Mar-2025 FREE Network Appliance NS0-093 PRACTICE QUESTIONS AND ANSWERS UPDATES
DEMO FREE BEFORE YOU BUY NS0-093 DUMPS

The NS0-093 certification exam is a comprehensive exam that consists of multiple-choice questions, simulations, and other interactive question types. NS0-093 exam is designed to test the candidate's practical skills and knowledge related to NetApp hardware systems. NetApp Accredited Hardware Support Engineer certification is a great way to validate your skills and knowledge as a hardware support engineer and demonstrate your commitment to your profession.

QUESTION 14

You have created a case with NetApp Support for an issue with a DS4246 shelf on an ONTAP 9.12.1 system.

They have requested that you provide shelf logs.

What action do you need to take to collect the shelf logs?

* Provide the output of the nodeshell command rdfile/etc/log/shelflog.
* Invoke an autosupport of type all using Active IQ Unified Manager.
* Invoke a diagnostic AutoSupport with the subsystem storage.
* Invoke a diagnostic autosupport with the subsystem log_files.

To collect shelf logs for a DS4246 shelf in an ONTAP 9.12.1 system, you must invoke a diagnostic AutoSupport specifically targeting the storage subsystem. This action ensures that detailed storage logs, including shelf logs, are included in the AutoSupport bundle.

* Use the following command:

Steps to Collect Shelf Logs:bash

Copy code

system node autosupport invoke -node <node_name> -type diagnostic -subsystem storage Replace <node_name> with the name of the node experiencing the issue.

* This command generates an AutoSupport message that includes logs related to storage subsystems, such as disk shelves and adapters.

* Provide the AutoSupport case number to NetApp Support for further analysis.

* A. Provide the output of the nodeshell command rdfile /etc/log/shelflog:

* While this command allows manual reading of shelf logs, it is not a recommended or comprehensive approach for collecting logs for NetApp Support cases.

* B. Invoke an AutoSupport of type all using Active IQ Unified Manager:

* This action generates a generic AutoSupport bundle, which may not include detailed shelf logs unless explicitly targeted.

* D. Invoke a diagnostic AutoSupport with the subsystem log_files:

* The log_files subsystem targets general system logs, not storage-specific logs like shelf logs.

Why Other Options Are Incorrect:

* “ONTAP 9 AutoSupport and Diagnostics Guide” outlines the use of the subsystem storage option for collecting shelf logs.

* The “Troubleshooting Storage Subsystems” documentation specifies diagnostic AutoSupport as the method for gathering shelf-related logs.

References:

QUESTION 15

At what stage is a write acknowledged to a client?
* when the write is present in the local node RAM and NVRAM
* when the write has been flushed to disk

* when the write is present in the NVRAM on the local node and its HA partner
* when the write has been flushed from NVRAM to RAM
* In a clustered ONTAP system, write requests are acknowledged to the client only after they are securely stored in NVRAM on both the local node and its HA (High Availability) partner.

* This ensures redundancy and data protection in case of a node failure.

Write Acknowledgment in NetApp ONTAP:

* A. when the write is present in the local node RAM and NVRAM:

* Writes are not acknowledged until the HA partner also stores the data in its NVRAM.

* B. when the write has been flushed to disk:

* Writes are acknowledged before they are written to disk, as NVRAM ensures durability.

* D. when the write has been flushed from NVRAM to RAM:

* Data is not acknowledged based on RAM; NVRAM on both nodes is the requirement.

Why Other Options Are Incorrect:

* NetApp’s “ONTAP Write I/O Processing Guide” explains the role of NVRAM and HA in write acknowledgment.

* “Data Protection in ONTAP” highlights the synchronization of NVRAM between HA partners.

References:

QUESTION 16

Where is a kernel core file stored on a FAS9000 system that is running ONTAP 9.12.1 software?
* on the partner root aggregate
* on the root aggregate
* on the mailbox disk
* on the boot device
On a FAS9000 system running ONTAP 9.12.1, the kernel core file is stored on the root aggregate. This is the default location where ONTAP writes kernel core files for system-level failures.

* The root aggregate is the aggregate that contains the root volume for a given node in the cluster. This aggregate is used for critical system files and logs, including kernel core files.

* When a kernel panic or other critical failure occurs, the core dump is written to the root aggregate for later analysis by NetApp Support.

Key Details:

* A. on the partner root aggregate: The partner root aggregate is not used for storing core files unless explicitly configured (which is not the default behavior).

* C. on the mailbox disk: The mailbox disk is used for cluster quorum and configuration information, not for storing core files.

* D. on the boot device: The boot device contains ONTAP software and boot files but does not store kernel core dumps.

* “ONTAP System Administration Guide” specifies that core files are stored on the root aggregate.

* NetApp’s “Troubleshooting and Diagnostics Guide” confirms the default behavior for kernel core file storage.

Why Other Options Are Incorrect:References:

QUESTION 17

What is the default amount of time that a volume is available for recovery from the volume recovery queue following a volume deletion?
* 12 hours
* 48 hours
* 72 hours
* 24 hours
When a volume is deleted in a NetApp ONTAP system, it is placed in the Volume Recovery Queue. By default, the volume remains in this recovery queue for 12 hours before being permanently deleted. This allows administrators to recover mistakenly deleted volumes within the set retention period.

Explanation of Default Behavior:

* Volume Recovery Queue:

* This is a feature in NetApp ONTAP that acts as a safety mechanism, providing a grace period for recovering deleted volumes.

* The default retention period for volumes in the recovery queue is 12 hours, as confirmed by the NetApp KB: “How to use the Volume Recovery Queue.”

* How to Recover a Deleted Volume:

* Administrators can recover a deleted volume as long as it remains in the recovery queue and the retention period has not expired.

* Use the ONTAP CLI command:

arduino

Copy code

cluster::> volume recovery-queue recover -vserver <vserver_name> -volume <volume_name>

* This command restores the volume back to its original state.

* How to Check the Volume Recovery Queue:

* To view volumes in the recovery queue and their expiration times, use:

arduino

Copy code

cluster::> volume recovery-queue show

* Changing the Default Retention Period:

* While the default period is 12 hours, it can be adjusted by administrators to fit specific organizational requirements. This is done via system settings or policies.

Why the Other Options Are Incorrect:

* B. 48 hours: Incorrect. The default retention period is not 48 hours; it is 12 hours by default.

* C. 72 hours: Incorrect. While a custom configuration could allow this, it is not the default.

* D. 24 hours: Incorrect. Although this was previously thought to be the default, NetApp documentation explicitly states it is 12 hours.

References:

* NetApp Knowledge Base Article: “How to use the Volume Recovery Queue”.

* NetApp ONTAP Documentation: Volume Recovery and Data Management Procedures.

QUESTION 18

What happens when the command diskcopy is run from nodeshell?
* It pre-fails a drive in an aggregate and copies it to a spare.
* It performs a low-level copy of the disk to another disk.
* It copies the disk content to a specified volume.
* It triggers a RAID reconstruction of that disk.

Purpose of the diskcopy Command:

* The diskcopy command is used in the ONTAP nodeshell environment to perform a low-level sector-by- sector copy of data from one disk to another. This is typically used during data recovery or diagnostics.

How It Works:

* The command copies all sectors from the source disk to the destination disk without any regard for file system or metadata structures.

* It is commonly used when replicating the exact state of a failing disk to a spare for further analysis or recovery.

Key Notes:

* The destination disk must be of the same or larger capacity than the source disk.

* The operation is typically disruptive and not suitable for production use.

NetApp Reference Documentation:

* Found in the “ONTAP Command Line Manual” for nodeshell utilities. The diskcopy process is highlighted as a low-level disk cloning operation.

QUESTION 19

Which two of the following methods are valid ways to access a node which is not booting? (Choose two.)
* node management port
* cluster management port
* Service Processor
* serial console
If a node is not booting, the following methods can be used to access the system for troubleshooting:

* What it does:The SP provides out-of-band management access to the node, even if the node is not booting.

* How to use:

* Connect to the SP using SSH or a direct console connection.

* Use SP commands to gather logs or perform diagnostics.

1. Service Processor (SP)

* What it does:The serial console provides direct access to the node’s bootloader or maintenance mode.

* How to use:

* Connect to the serial port using a terminal emulator.

* Use console commands to interact with the system.

2. Serial Console

* A. node management port:

* The node management interface is only accessible if the node is booted and ONTAP is running.

* B. cluster management port:

* The cluster management interface requires the cluster to be operational, which is not possible if the node is not booting.

Why Other Options Are Incorrect:

* NetApp “Service Processor and Serial Console Guide” provides instructions for accessing a non- booting node.

References:

QUESTION 20

Which command can you use to confirm successful completion of an ONTAP upgrade?
* system controller sp upgrade show
* cluster image show-update-progress
* job show -jobtype upgrade
* system node upgrade-revert upgrade-task -node <nodename> -version <ontap Version>
To confirm the successful completion of an ONTAP upgrade, the cluster image show-update-progress command provides the necessary details.

* Command:

Key Command:cluster image show-update-progress

* Displays the status of the cluster upgrade, including which nodes have successfully upgraded and whether the process has completed.

* A. system controller sp upgrade show:

* This command displays information about SP (Service Processor) firmware upgrades, not ONTAP upgrades.

* C. job show -jobtype upgrade:

* While this command shows upgrade jobs, it does not confirm the completion of the cluster-wide ONTAP upgrade.

* D. system node upgrade-revert upgrade-task -node <nodename> -version <ontap Version>:

* This command reverts an upgrade task, not confirms completion.

Why Other Options Are Incorrect:

* NetApp “ONTAP Upgrade Guide” specifies the cluster image show-update-progress command as the primary method to verify upgrade completion.

References:

QUESTION 21

Which two statements are true about an IOM 12 module? (Choose two.)
* It has two SAS ports.
* It has four SAS ports.
* It does not have an Ethernet port for alternate control path (ACP).
* It has an Ethernet port for alternate control path (ACP).
Overview of IOM 12 Module:

* The IOM 12 module is used in NetApp storage shelves for SAS connectivity.

Key Features of IOM 12:

* SAS Ports: The IOM 12 module has four SAS ports (two IN and two OUT) to support daisy-chaining of shelves and provide

redundancy.

* ACP (Alternate Control Path): The IOM 12 includes an Ethernet port for ACP, which is used for out- of-band management and monitoring of the storage shelves.

Elimination of Other Options:

* Option A is incorrect because the module has four SAS ports, not two.

* Option C is incorrect because the module does include an Ethernet port for ACP.

NetApp Reference Documentation:

* “NetApp Hardware Universe” lists the specifications of the IOM 12 module, including its SAS and ACP capabilities.

* The “ONTAP Shelf Installation Guide” discusses ACP and its role in shelf management.

QUESTION 22

On a NetApp FAS9000 system, which two field replaceable units (FRUs) are supported for replacement without takeover? (Choose two.)
* I/O module
* DCPM module
* caching module
* NVRAM module

FRUs on FAS9000 Supporting Replacement Without Takeover:

* A (I/O Module): I/O modules can be replaced hot (without takeover) to maintain system uptime during hardware servicing.

* D (NVRAM Module): NVRAM modules on FAS9000 can also be replaced without a node takeover, ensuring data integrity during replacement.

Why Other Options Are Incorrect:

* B (DCPM Module): The DCPM (Data Center Power Management) module is not hot-swappable and requires a node takeover.

* C (Caching Module): The caching module is integrated and typically requires a node takeover or power-down for replacement.

NetApp Reference Documentation:

* Refer to the “NetApp FAS9000 Hardware Service Guide” for supported FRU replacement procedures and operational constraints.

QUESTION 23

What are two valid options for uploading a core file from a node that is running ONTAP 9.12.1 software to NetApp for analysis? (Choose two.)
* system node autosupport invoke -diagnostic
* Download via CIFS and upload to upload.netapp.com.

* Download via Service Processor Infrastructure (SPI) and upload to upload.netapp.com.
* system node autosupport invoke-core-upload

Options for Uploading Core Files:

* Core files are diagnostic dumps created during system failures for analysis by NetApp Support.

* They can be uploaded via multiple methods, depending on system configuration and access:

Option B (CIFS Download):

* Core files can be downloaded from the node using a CIFS share and then manually uploaded to upload.

netapp.com.

* This method is useful if automated processes are unavailable or connectivity is limited.

Option D (Autosupport Invoke-Core-Upload):

* The command system node autosupport invoke-core-upload automates the process of uploading the core file to NetApp.

* It uses the configured Autosupport mechanism to transfer the file to NetApp Support for analysis.

NetApp Reference Documentation:

* “ONTAP Autosupport Guide” and “ONTAP Troubleshooting Guide” provide instructions for manually and automatically uploading core files.

QUESTION 24

In a SAS stack of shelves, what is the topology of the connection between expander and disk?
* arbritrated loop
* point-to-point
* loop
* ring

In a SAS stack of shelves, the connection between the expander and the disk uses a point-to-point topology.

* Point-to-Point:

* Each SAS disk in a shelf connects directly to the expander using a dedicated channel. This ensures that communication between the disk and expander is independent of other disks, improving performance and reliability.

* Why SAS Uses Point-to-Point:

* SAS (Serial Attached SCSI) eliminates the shared bandwidth limitations of traditional bus architectures (e.g., arbitrated loop or ring) by dedicating a connection to each device.

Key Details:

* A. arbitrated loop:

* Arbitrated loop is a topology used in Fibre Channel systems, not SAS.

* C. loop:

* SAS does not use loop-based communication; this is typical of older technologies like SCSI Parallel Interface (SPI).

* D. ring:

* Ring topology is not used in SAS stacks.

Why Other Options Are Incorrect:

* “NetApp SAS Shelf and Disk Configuration Guide” specifies point-to-point communication between expanders and disks in SAS environments.

References:

QUESTION 25

How do you set environment variables to factory settings?
* set-defaults
* unsetenv all
* setenv factory
* wipeconfig

To reset environment variables to factory settings, the set-defaults command is used. This command clears all customizations and restores the environment variables to their default values.

* Command Syntax:At the LOADER prompt, type:

Key Details:arduino

Copy code

set-defaults

* Effect:This command resets all environment variables (e.g., boot arguments, diagnostic settings) to their original factory defaults.

* B. unsetenv all:

* This command clears all environment variables, but it does not restore them to factory defaults.

* C. setenv factory:

* This is not a valid command in NetApp systems.

* D. wipeconfig:

* This command is used to clear configuration and logs but does not reset environment variables.

Why Other Options Are Incorrect:

* NetApp “System Configuration Guide” confirms the use of set-defaults for restoring environment variables to factory settings.

References:

QUESTION 26

After a panic, the customer asks you to explain the error “watchdog timeout.” Which explanation would be appropriate?
* An optional software that monitors system performance.

An overloaded system fails to reset the watchdog and watchdog induces a system panic.
* An optional component included with Active IQ Unified Manager.

It notifies a user if watchdog fails to reach the storage system within a certain period.
* A service that detects and recovers from computer malfunctions.

A hardware or software error prevents update of watchdog and it induces a system panic.
* A service that monitors network activity and protects data.

A watchdog induces system panic to protect data if malicious activity is detected.
What Is a Watchdog Timeout?

* The watchdog is a software or hardware mechanism that monitors the system’s health and ensures it is operating correctly.

* If the system fails to respond or update the watchdog timer within the specified time, the watchdog triggers a system panic to avoid further corruption or damage.

Cause of Watchdog Timeout:

* This usually occurs due to:

* A hardware failure (e.g., CPU or memory issue).

* A software bug causing a system hang or crash.

* The panic ensures the system stops operation to preserve data integrity and aid in troubleshooting.

NetApp Reference Documentation:

* “ONTAP Troubleshooting Guide” and “Core Dump Analysis Guide” provide details on interpreting watchdog timeouts and recommended actions.

QUESTION 27

A SAS connection is reporting a single PHY down.

What are the two most likely causes? (Choose two.)
* improperly seated cable

* outdated I/O module (IOM1 firmware
* defective cable
* an offline shelf in the stack

Understanding a Single PHY Down Issue:

* In SAS environments, a PHY represents a physical layer connection between devices.

* When a single PHY reports a “down” status, it typically indicates an issue with the physical connectivity or the associated hardware.

Cause 1: Improperly Seated Cable

* If the SAS cable is not properly seated in the port, the connection for one or more PHYs may fail.

* Reseating the cable on both ends (controller and shelf) often resolves the issue.

Cause 2: Defective Cable

* A damaged or faulty SAS cable can cause PHY errors.

* Replacing the cable and verifying the connection resolves the issue in this case.

Why Other Options Are Not Likely:

* B. Outdated IOM firmware: While outdated firmware can cause other issues, it rarely affects only a single PHY.

* D. Offline shelf: If an entire shelf is offline, more than one PHY would typically be affected, as multiple connections are involved in SAS stacks.

NetApp Reference Documentation:

* Found in the “ONTAP SAS Cabling Guide” and “Shelf Troubleshooting Guide”. These documents detail troubleshooting for PHY errors and common SAS hardware issues.

QUESTION 28

Which two steps are required to replace a drawer in a DS460c shelf? (Choose two.)
* Evacuate all drives in the drawer.
* Power off the shelf.
* Disconnect the cable chains from the chassis.
* Shut down both nodes.

QUESTION 29

Which two commands from the Service Processor can provide information about installed field replaceable units (FRUs)? (Choose two.)
* system fru list
* system fru show
* system sensors show
* system power status

To view information about installed Field Replaceable Units (FRUs) using the Service Processor, the following commands are used:

* What it does:Displays a list of all installed FRUs, such as disks, power supplies, and fans.

* Example Usage:

1. system fru listsystem fru list

* What it does:Provides detailed information about specific FRUs, including serial numbers, statuses, and hardware details.

2. system fru showsystem fru show

* C. system sensors show:

* This command displays sensor data (e.g., temperature, voltage) but does not list FRUs.

* D. system power status:

* This command shows power supply status but does not provide FRU details.

Why Other Options Are Incorrect:

* “Service Processor Commands Guide” from NetApp provides a comprehensive overview of system fru list and system fru show.

References:

QUESTION 30

You are replacing a boot device on a FAS8300 system that is running ONTAP 9.10P6 software. You attach a USB memory stick to the external USB port on the storage controller but cannot access the memory stick.

What step needs to be performed to access the boot device?
* Set the port to “enabled” with setenv.
* You need to use ONTAP 9.11 or later software.
* Add the boot device before the BIOS is loaded.
* The external USB port is not activated on NetApp systems.

When replacing a boot device on a FAS8300 system and using a USB memory stick for recovery or installation, the external USB port must be explicitly enabled. This is done through the setenv command in the boot environment.

* Reboot the system and interrupt the boot process to access the bootloader prompt.

* At the bootloader prompt, use the following command:

Steps to Enable the External USB Port:arduino

Copy code

setenv usbport_enabled true

* Save the configuration and proceed with the boot process.

* B. You need to use ONTAP 9.11 or later software:

* ONTAP 9.10P6 fully supports external USB recovery. There is no need to upgrade to ONTAP

9.11 for this functionality.

* C. Add the boot device before the BIOS is loaded:

* While the USB device must be inserted during the boot process, this alone will not enable access unless the port is enabled via setenv.

* D. The external USB port is not activated on NetApp systems:

* This is incorrect. The external USB port is supported but must be explicitly enabled in the bootloader environment.

Why Other Options Are Incorrect:

* NetApp Hardware Installation Guide for FAS8300 systems outlines the steps for enabling the USB port during recovery.

* “ONTAP Boot Troubleshooting Guide” specifies the use of the setenv command to activate USB ports.

References:

QUESTION 31

Which type of AutoSupport message would you expect to see triggered automatically when ONTAP software detects a NetApp WAFL inconsistency on an aggregate?
* MEDIUM ERROR DURING RECONSTRUCTION
* CHECKSUM ERROR
* WAFL INCONSISTENT USER DATA BLOCK
* WAFL INCONSISTENT BLOCK
When ONTAP detects a WAFL inconsistency in an aggregate, it automatically generates an AutoSupport message with the description WAFL INCONSISTENT BLOCK.

* WAFL INCONSISTENT BLOCK:

* This error indicates that WAFL metadata or user data blocks have been found to be inconsistent.

* ONTAP triggers an automatic AutoSupport message to notify administrators and NetApp Support.

Key Details:

* A. MEDIUM ERROR DURING RECONSTRUCTION:

* This error occurs during disk reconstruction, not due to WAFL inconsistencies.

* B. CHECKSUM ERROR:

* A checksum error indicates a disk-level data integrity issue, not a WAFL inconsistency.

* C. WAFL INCONSISTENT USER DATA BLOCK:

* While related, this is not the specific AutoSupport message triggered by ONTAP.

Why Other Options Are Incorrect:

* NetApp “ONTAP WAFL Troubleshooting Guide” describes AutoSupport messages related to WAFL inconsistencies.

References:

QUESTION 32

Which three commands can be used to manually generate a kernel core file? (Choose three.)
* SP> system power cycle
* ::> reboot -node <node_name> -dump true
* ::> halt -dump true -node <node_name>
* ::> system node panic -node <node_name>
* SP> system core
To manually generate a kernel core file in ONTAP, the following commands can be used:

* What it does:Reboots the specified node and generates a core dump before rebooting.

* Example Usage:

1. ::> reboot -node <node_name> -dump truereboot -node <node_name> -dump true

* What it does:Halts the specified node and generates a core dump before shutting down.

* Example Usage:

2. ::> halt -dump true -node <node_name>halt -dump true -node <node_name>

* What it does:Forces a panic on the specified node, which triggers a kernel core dump.

* Example Usage:

3. ::> system node panic -node <node_name>system node panic -node <node_name>

* A. SP> system power cycle:

* This command reboots the system from the Service Processor but does not generate a core dump.

* E. SP> system core:

* This command displays core file information but does not generate a new core dump.

Why Other Options Are Incorrect:

* NetApp “Kernel Core Dump Guide” explains the use of reboot, halt, and panic commands to trigger core dumps.

* ONTAP CLI Reference includes the syntax for these commands.

References:

QUESTION 33

Which two NetApp tools should be used when troubleshooting the root cause of an unexpected controller reboot? (Choose two.)
* Active IQ Unified Manager
* Active IQ Digital Advisor
* ONTAP CLI
* ONTAP Mediator
* Active IQ Config Advisor

To troubleshoot the root cause of an unexpected controller reboot, the following tools are commonly used:

* What it does:Provides monitoring and performance data for the ONTAP cluster, including historical event logs that may help identify the root cause of a reboot.

1. Active IQ Unified Manager

* What it does:The CLI allows you to gather logs and status information directly from the affected node.

Commands like event log show and system core are essential for identifying the reason behind the reboot.

2. ONTAP CLI

* B. Active IQ Digital Advisor:

* This tool focuses on predictive analytics and proactive recommendations, not troubleshooting unexpected reboots.

* D. ONTAP Mediator:

* This tool is used for managing MetroCluster configurations, not for troubleshooting reboots.

* E. Active IQ Config Advisor:

* This tool checks for configuration best practices but does not provide detailed logs or reboot diagnostics.

Why Other Options Are Incorrect:

* NetApp “ONTAP System Management Guide” emphasizes the use of Unified Manager and CLI for troubleshooting system issues.

References:

QUESTION 34

While performing a health check on a cluster, you notice the following entries in the cluster event log:

```
Thu Jun 18 12:12:09 PDT [nodeA2: disk_server_0: disk.ioModiumError:notice]:
Medium error on disk 0b.64.18L2: op
0x88:00000003c1ce73d8:00000200 sector 1613434984 SCST: medium error -
Unrecovered read error - If the disk is in a RAID group, the subsystem will
attempt to reconstruct unreadable data (3 11 ff 0) (6955) Disk 0b.64.18L2
Shelf 64 Bay 18 [NETAPP X381_HLBRE10TSDB NA01]
S/N [7PGVHKSG] UID [5000CCA2:51CC0C1B:00000000: 00000000: 00000000: 00000000:
00000000: 00000000: 00000000: 00000000]
```


Referring to the exhibit, which of the following actions do you take?
* Sanitize the disk.
* Reseat the disk.
* Review the current firmware and known issues.
* Use diskcopy to copy the disk to a working spare.

Analyzing the Error in the Event Log:

* The log entry indicates a medium error on a disk, suggesting an unrecoverable read issue.

* While the RAID subsystem attempts to reconstruct unreadable data, this error might indicate a firmware issue or a compatibility problem with the disk.

Why Reviewing Firmware and Known Issues Is Important:

* Medium errors can sometimes result from outdated or incompatible firmware.

* By reviewing firmware release notes and known issues for the disk model (NETAPP X381_HLBRE10TSDB in this case), you can identify if this is a known issue and resolve it by updating the firmware.

Other Options:

* Sanitize the disk (Option A): Not relevant here, as sanitization is used for secure data erasure.

* Reseat the disk (Option B): Useful for addressing hardware seating issues, but not the first step here.

* Diskcopy to a spare (Option D): This is a last-resort recovery step and not the primary action.

NetApp Reference Documentation:

* “ONTAP Disk Management Guide” and “Disk Firmware Release Notes” detail how to handle medium errors and update firmware.

QUESTION 35

What are two valid commands that can be used to trigger an AutoSupport? (Choose two.)
* ::> autosupport history show-upload-details -node <nodename>
* ::> system node coredump upload -node <nodename>
* ::> autosupport invoke -node <nodename> -type all
* ::> autosupport invoke-core-upload -node <nodename>

To trigger an AutoSupport message in ONTAP, the following commands are valid:

* What it does:This command manually triggers a complete AutoSupport message of type “all.” This includes logs and system information from all subsystems.

* How to use:

* Run the command: autosupport invoke -node <nodename> -type all

* Replace <nodename> with the name of the node for which you want to generate the AutoSupport message.

* Why it’s relevant:This is the primary method for triggering a full AutoSupport message manually. It is commonly used during troubleshooting to provide comprehensive system data to NetApp Support.

1. ::> autosupport invoke -node <nodename> -type all

* What it does:This command is specifically used to upload core files (e.g., kernel or user space cores) from a node to NetApp Support for analysis.

* How to use:

* Run the command: autosupport invoke-core-upload -node <nodename>.

* Replace <nodename> with the name of the node for which you want to upload core files.

* Why it’s relevant:If there is a system panic or other critical issue, this command ensures that core files are included in the AutoSupport message for detailed analysis.

2. ::> autosupport invoke-core-upload -node <nodename>

* A. ::> autosupport history show-upload-details -node <nodename>:

* This command displays the history of AutoSupport uploads but does not trigger a new AutoSupport.

* B. ::> system node coredump upload -node <nodename>:

* This command uploads coredumps directly to a support server but does not trigger an AutoSupport message.

Why Other Options Are Incorrect:

* “ONTAP 9 AutoSupport Configuration Guide” confirms autosupport invoke as a valid command to trigger AutoSupport messages.

* “ONTAP CLI Reference Manual” specifies autosupport invoke-core-upload for core file uploads.

References:

The NetApp Accredited Hardware Support Engineer certification program prepares candidates for real-world scenarios and gives them the credentials they need to add more value to their organization. Companies that deploy NetApp storage solutions need engineers who can support and maintain them to ensure their efficient functioning. The NS0-093 certification ensures that individuals have the skills and knowledge required to provide effective hardware support for NetApp storage systems.

Latest Network Appliance NS0-093 Dumps with Test Engine and PDF:
https://www.test4engine.com/NS0-093_exam-latest-braindumps.html]