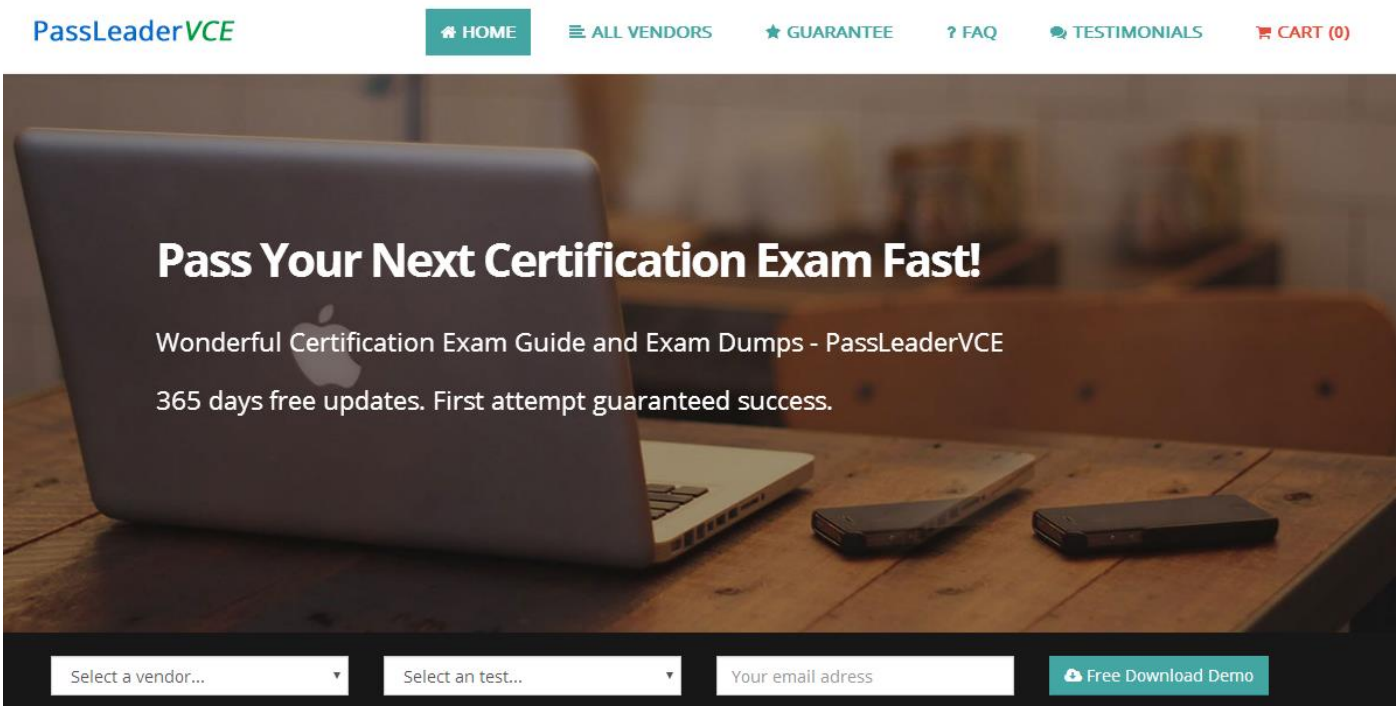
PassleaderVCE



http://www.passleadervce.com/

Wonderful Certification Exam Guide and Exam Dumps- PassLeaderVCE

Exam : **NS0-093**

Title : NetApp Accredited Hardware Support Engineer

Vendor : Network Appliance

Version : DEMO

NO.1 Which type of core file is generated when a node panics?
A. mgwd core
B. user space core
C. sync core
D. kernel core
Answer: D
Explanation:
When a node panics in ONTAP, a kernel core file is generated. This core file contains information about the kernel's state at the time of the panic and is essential for debugging system crashes.
* A kernel core file is produced during a node panic to capture information about the kernel, memory, and processes that led to the crash.
* The core file is stored on the root aggregate by default and can be uploaded to NetApp Support using the autosupport invoke-core-upload command.
Key Details:
* A. mgwd core:
* This is related to the Management Gateway daemon, which handles management traffic. It does not generate a core file during a panic.
* B. user space core:
* User space cores are generated for processes running in user space, not for kernel panics.
* C. sync core:
* Sync cores refer to synchronized cores for debugging but are not the primary type generated during a node panic.
Why Other Options Are Incorrect:
* "ONTAP Panic Troubleshooting Guide" specifies kernel core files as the output of a node panic.
* "ONTAP Core File Management Guide" details the handling of kernel core files after a crash.
References:

NO.2 Which two commands confirm whether an aggregate is WAFL inconsistent? (Choose two.)
A. wafiron show <aggregate>
B. node run -node <node> sysconfig -r
C. storage aggregate show
D. node run -node <node> sysconfig -a
Answer: A B
Explanation:
To determine whether an aggregate is WAFL (Write Anywhere File Layout) inconsistent, the following two commands can be used:
* What it does:This command directly checks the WAFL consistency status of the specified aggregate. If an aggregate is WAFL inconsistent, it will report the inconsistency in the output.
* How to use:
* Run the command: wafiron show <aggregate> (replace <aggregate> with the name of the aggregate).
* Look for indications of WAFL inconsistency in the output.
* Why it's relevant:The wafiron utility is specifically designed to provide WAFL status and diagnostics. It is the most accurate and direct way to confirm whether an aggregate is inconsistent.
* References:

* "WAFL Troubleshooting Guide" from NetApp highlights the wafiron show command as a primary tool for checking aggregate consistency.
1. wafiron show <aggregate>
* What it does:This command displays RAID information for all aggregates on the specified node. If an aggregate is WAFL inconsistent, it will be explicitly mentioned in the output.
* How to use:
* Run the command: node run -node <node> sysconfig -r.
* Check the output for the phrase "WAFL inconsistent" under the corresponding aggregate.
* Why it's relevant:This command provides additional context, such as the RAID group details, which can help understand whether the inconsistency is isolated or part of a larger issue.
* References:
* "ONTAP CLI Commands Guide" specifies sysconfig -r as a method to verify aggregate status, including WAFL consistency.
2. node run -node <node> sysconfig -r
* C. storage aggregate show:
* This command displays aggregate configuration and usage information but does not report WAFL inconsistency.
* D. node run -node <node> sysconfig -a:
* While this command shows detailed hardware configuration information, it does not include WAFL consistency status for aggregates.
Why Other Options Are Incorrect:

NO.3 After a panic, the customer asks you to explain the error "watchdog timeout." Which explanation would be appropriate?
A. An optional software that monitors system performance.
An overloaded system fails to reset the watchdog and watchdog induces a system panic.
B. 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.
C. A service that detects and recovers from computer malfunctions.
A hardware or software error prevents update of watchdog and it induces a system panic.
D. A service that monitors network activity and protects data.
A watchdog induces system panic to protect data if malicious activity is detected.
Answer: C
Explanation:
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.

NO.4 Which two statements are correct when describing L1 and L2 Watch Dog Resets (WDR)? (Choose two.)

A. L2 WDR requests creation of a core dump before reset.

B. L1 WDR is initiated after 0.5 seconds from the event.

C. L1 WDR performs a soft reset.

D. L2 WDR is initiated after 2 seconds from the event.

Answer: A D

Explanation:

* Description:

* L1 WDR is a hardware-initiated reset that occurs when the system detects an unrecoverable error or lockup lasting 0.5 seconds.

* Key Characteristics:

* It performs a hard reset, meaning the system immediately reboots without creating a core dump.

1. L1 Watchdog Reset (WDR):

* Description:

* L2 WDR is initiated when the system fails to recover from a critical fault after 2 seconds.

* Key Characteristics:

* It requests a core dump to capture the system state for diagnostic purposes before performing a reset.

2. L2 Watchdog Reset (WDR):

* B. L1 WDR is initiated after 0.5 seconds from the event:

* This is incorrect because L1 WDR performs a hard reset and does not initiate after 2 seconds.

* C. L1 WDR performs a soft reset:

* This is incorrect because L1 WDR performs a hard reset, not a soft reset.

Why Other Options Are Incorrect:

* "ONTAP Panic Analysis Guide" describes the behavior and timing of L1 and L2 WDR events.

* NetApp Support documentation on system resets explains the differences between L1 and L2 watchdog resets.

References:

NO.5 Which two NetApp tools should be used when troubleshooting the root cause of an unexpected controller reboot? (Choose two.)

A. Active IQ Unified Manager

B. Active IQ Digital Advisor

C. ONTAP CLI

D. ONTAP Mediator

E. Active IQ Config Advisor

Answer: A C

Explanation:

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:

NO.6 What are two valid commands that can be used to trigger an AutoSupport? (Choose two.)
A. ::> autosupport history show-upload-details -node <nodename>
B. ::> system node coredump upload -node <nodename>
C. ::> autosupport invoke -node <nodename> -type all
D. ::> autosupport invoke-core-upload -node <nodename>
Answer: C D
Explanation:
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: