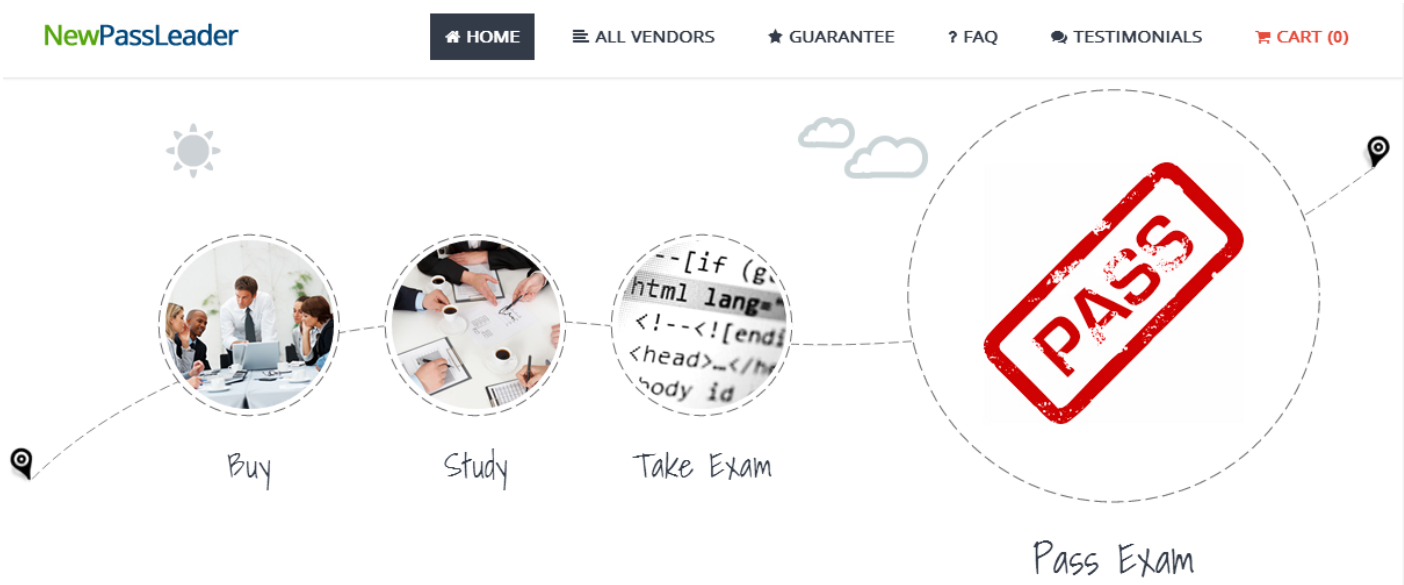
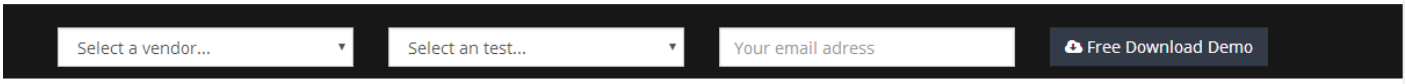
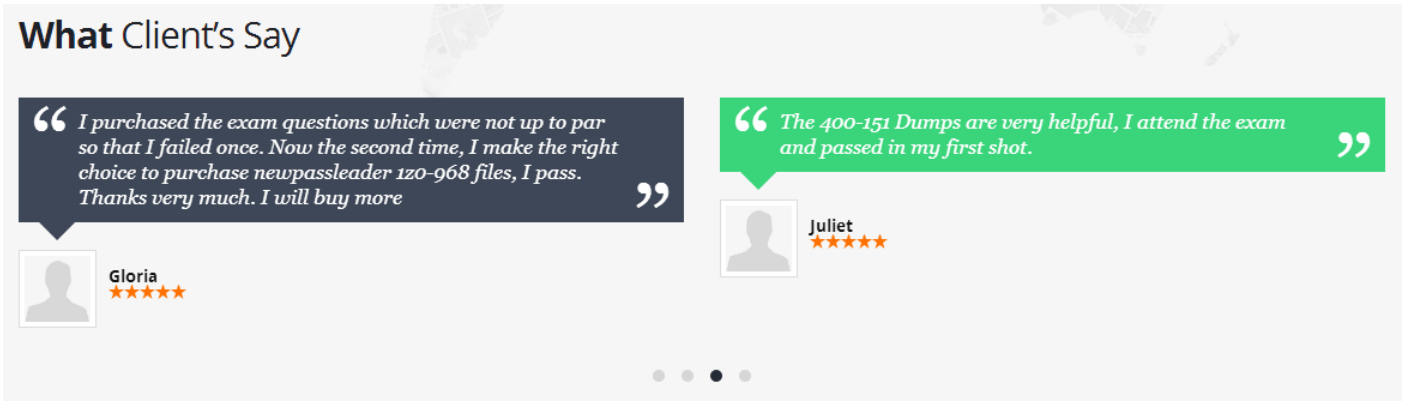
NewPassleader





Try **PDF Demo** before you buy

Online Test Engine: Online Tool, Convenient, easy to study. Instant Online Access. Supports All Web Browsers.
PDF format: Easy to read and print learning materials, our products are available in PDF file format.
Desktop Test Engine: Installable Software Application. Simulates Real Exam Environment. Practice Offline Anytime.



http://www.newpassleader.com/

Attentive Service Exam Torrent and Valid Dumps - NewPassLeader

Exam : **D-PE-OE-01**

Title : Dell PowerEdge Operate v2 Exam

Vendor : EMC

Version : DEMO

NO.1 You are in a dark site with a PowerEdge server that shows an amber light. iDRAC Is not configured for network access but the OS is installed and has RACADM for access to the iDRAC card. What RACADM command can be used to help identify the cause of the amber light?

A. getsel

B. getssninfo

C. getsysinfo

D. get led

Answer: A

Explanation:

Operating within an isolated dark-site facility without out-of-band management network connectivity requires technicians to use alternative local diagnostic tools to investigate hardware alerts. When a physical server chassis displays a warning via a solid or flashing amber light, it signals an active hardware exception has been generated by the monitoring system. If the local host operating system remains operational and has the Dell OpenManage RACADM command-line utility installed, the technician can communicate with the iDRAC using local in-band execution paths. Executing the specific command racadm getsel allows the engineer to dump and read the System Event Log (SEL) directly from the command prompt. The SEL contains an indexed historical record of low-level component sensor data, detailing exactly which hardware tracking metric-such as a fan failure, voltage drop, or memory channel fault-triggered the amber chassis alarm. This precise terminal output allows for rapid troubleshooting without requiring external network routing or system reboots. Study Guide References: Troubleshooting; In-Band Systems Management; Local RACADM Operations and Log Retrieval.

NO.2 On a Dell PowerEdge 16G server, iDRAC is configured to use a shared LOM port. What happens if the Auto- Dedicated NIC option is enabled and a dedicated NIC becomes available?

A. iDRAC uses both the shared LOM and dedicated NIC simultaneously for redundancy

B. iDRAC automatically switches to the dedicated NIC without requiring a reboot

C. iDRAC disables network connectivity until manually reconfigured

D. iDRAC continues using the shared LOM port until the next reboot

Answer: B

Explanation:

Dell PowerEdge 16G servers feature intelligent networking behaviors designed to simplify access management and maintain control-plane connectivity during physical infrastructure changes. When the iDRAC is configured to route management traffic through a shared LAN-on-Motherboard (LOM) port, it utilizes the physical connections of the host operating system's network adapter. Enabling the "Auto- Dedicated NIC" feature directs the internal management processor to actively track the physical status of the server's dedicated out-of-band network port. If a network cable connected to a live switch is plugged into that dedicated port, the iDRAC detects an active link signal and dynamically shifts its network stack over to the dedicated physical port. This transition happens entirely in the background without needing a system reboot or manual network configuration adjustments. Moving management traffic away from the host production ports onto an isolated network segment enhances overall security profiles while keeping existing management sessions active throughout the port transition.

Study Guide References: System Administration; iDRAC Connectivity Profiles; Auto-Dedicated NIC Redirection Logic.

NO.3 A Dell PowerEdge R750 server is going into a datacenter with no network connectivity and no KVM. What is valid way to configure a static IP address for the iDRAC in this situation?

A. In-band management

B. iDRAC direct using USB-C port

C. LOM

D. LCD Control Panel

Answer: D

Explanation:

Configuring the Integrated Dell Remote Access Controller (iDRAC) with a permanent static IP address when a server is deployed into an isolated environment without network links or a local keyboard, video, and mouse (KVM) switch matrix requires physical console access. On the Dell PowerEdge R750 server, which represents a 15th-generation platform architecture, the physical LCD Control Panel embedded into the front bezel provides a localized management window. This embedded text or graphical display interacts directly with the Lifecycle Controller subsystem independent of the operational state of the host CPU or operating system. By navigating the structural hardware interface menus utilizing the integrated buttons, a technician can access the network configuration section to change the iDRAC network configuration type from DHCP to static and input IPv4 subnet parameters directly. Note that while 16th-generation platforms utilize a dedicated USB-C interface for iDRAC Direct connectivity, the 15th-generation R750 relies on a legacy Micro-USB interface, rendering the USB-C option invalid for this hardware profile.

Study Guide References: Server Deployment; Initial iDRAC Access and Provisioning; Bezel Configuration Utilities.

NO.4 Your company is decommissioning a PowerEdge 16G server to a 17G server. All the disks in the 16G server are SEDs. Your security team requires that the server is securely retired. Which feature can be used to comply with the security requirement?

A. Use LifeCycle Controller ISE feature

B. Enable Secure Boot in BIOS

C. Enable Lockdown Mode in iDRAC

D. Use SCV application feature

Answer: A

Explanation:

Retiring enterprise infrastructure assets safely requires applying reliable data sanitation routines across all persistent storage devices to prevent the unauthorized leak of sensitive corporate information. When decommissioning a Dell PowerEdge 16G server featuring Self-Encrypting Drives (SEDs), administrators can leverage the integrated Instant Secure Erase (ISE) capability built directly into the Lifecycle Controller interface. The ISE feature communicates directly with the security microchip on the SEDs, triggering an instantaneous, cryptographic erasure of the internal media encryption keys. Once these internal cryptographic keys are scrubbed and destroyed, all data blocks previously written to the storage media are rendered permanently unreadable and completely unrecoverable, returning the drives to an uninitialized factory clean state within seconds. This process provides a highly audited data sanitization workflow that achieves complete compliance with strict institutional security protocols and international data center decommissioning standards. It completes this erasure significantly faster and with less mechanical wear than traditional multi- pass

overwriting cycles or destructive physical processing methods.
Study Guide References: System Administration; Secure Component Retirement; Lifecycle Controller Cryptographic Erasure and ISE.

NO.5 Your customer requires a way to monitor a high-level and holistic view of the workload of their servers. A database server was identified as providing lower than expected performance after migrating to a PowerEdge R760 server. Which option can be selected in iDRAC to monitor this level of information?

A. CPU Utilization

B. I/O Utilization

C. Memory Utilization

D. System Level CUPS Index

Answer: D

Explanation:
When diagnosing holistic performance issues on critical enterprise database nodes, individual metrics such as standalone CPU, memory, or storage subsystem monitoring often fail to provide a complete picture of resource contention. To solve this, the Integrated Dell Remote Access Controller (iDRAC) implements the Compute Usage Per Second (CUPS) architectural framework. The System Level CUPS Index provides a normalized, high-level composite metric that models real-time utilization across the core bottlenecks:
processing units, system memory bandwidth, and internal I/O bus tracking structures. By analyzing this consolidated telemetry index, system architects can instantly determine whether a database performance bottleneck stems from platform-level resource saturation or specialized software configuration limits. Because CUPS operates entirely out-of-band within the management chip, it gathers precise hardware metrics directly from the chipset without consuming host processor cycles, ensuring reliable data delivery during extreme performance degradation events.
Study Guide References: Server Monitoring; Compute Usage Per Second (CUPS); Performance Telemetry.

NO.6 An administrator wants to ensure continuous visibility into the hardware health of a Dell PowerEdge server and be notified immediately if a component begins to fail. Using iDRAC, what action should be taken to meet these requirements?

A. Monitor hardware health only through the operating system tools

B. Log in to iDRAC only after the operating system reports a failure

C. Configure iDRAC hardware health monitoring with automated alerting

D. Disable system alerts to reduce unnecessary notifications

Answer: C

Explanation:
To maintain continuous, proactive visibility into the underlying physical health of a Dell PowerEdge node and ensure instantaneous warning when sub-components exhibit early signs of failure, relying on reactive policies or host OS frameworks is insufficient. Operating system tools can become blind if a kernel failure occurs, and manually logging into management panels post-incident shifts the paradigm from preventive maintenance to disaster recovery. The correct methodology is to configure the integrated Dell Remote Access Controller (iDRAC) hardware health monitoring framework paired with automated alerting routines. Operating completely out-of-band, the iDRAC continuously

processes status checks across critical components- including storage backplanes, memory channels, cooling infrastructure, and power supply circuitry. When an metric falls outside normal thresholds, the internal evaluation engine references the active notification matrix and dispatches immediate warnings via industry-standard mechanisms such as SMTP emails, SNMP traps, or Syslog streams. This autonomous approach eliminates reliance on human inspection intervals and host stability, guaranteeing that operations teams receive real-time actionable telemetry to remedy minor degradation problems before they result in unexpected system downtime.
Study Guide References: Server Monitoring; Proactive Hardware Alerting; iDRAC Telemetry and Notification Profiles.

NO.7 You are managing a PowerEdge R570 and iDRAC is not reachable on the Network. You need to collect iDRAC details on the server. Which two tools will allow you to get the iDRAC details?

A. Use RACADM to capture inventory and log

B. Use iSM to capture inventory and log

C. Use Lifecycle Controller to capture inventory and log

D. Use OME to capture inventory and log

Answer: A C

Explanation:
When network connection faults block remote access to the Integrated Dell Remote Access Controller (iDRAC) on a Dell PowerEdge R570 server, administrators must switch to local or alternate firmware interfaces to perform inventory extraction and log collection. The first tool capable of harvesting this data in an isolated scenario is the RACADM (Remote Access Controller Admin) command-line utility. If the host operating system is functional, a local in-band RACADM instance communicates with the management processor directly through internal system interface drivers, letting the technician run diagnostic commands and capture inventory blocks directly to the OS command prompt without network routing. The second tool is the pre-boot Lifecycle Controller (LCC) interface. By rebooting the server and pressing F10 during POST, the engineer accesses a local, firmware-driven UI that reads device inventories and logs from the persistent flash storage container. Conversely, centralized management systems like OpenManage Enterprise (OME) are completely ineffective because they depend entirely on the disrupted out-of-band network links to pull device states.
Study Guide References: Troubleshooting; Local RACADM Command Architectures; Lifecycle Controller Maintenance Utilities.

NO.8 A company operates a Dell PowerEdge server configured with a RAID 10 virtual disk that hosts critical databases services. Monitoring tools indicate that the virtual disk usage has reached 95% of total capacity.
The server provides 24/7 mission-critical services, so downtime must be minimized or completely avoided.
Currently, the server has only one empty drive bay remaining. What should the operations team consider first to safely plan the expansion of the RAID 10 virtual disk?

A. Check the RAID controller's capabilities, available drive bays, and whether expansion is supported.

B. Replace the RAID controller with the latest model to guarantee maximum performance, then add the new disk.

C. Add the new disk, trigger a rebuild of the RAID, and wait until the rebuild is complete before using

the expanded capacity.

D. Add the new disk and immediately perform Online Capacity Expansion through iDRAC.

Answer: A

Explanation:

Planning a storage capacity expansion on a live enterprise production server hosting mission-critical databases necessitates verifying the architectural boundaries of the underlying PowerEdge storage subsystem. A RAID 10 virtual disk layout functions by striping data across multiple mirrored drive pairs (spans), meaning any structural expansion via Online Capacity Expansion (OCE) typically demands the simultaneous addition of an entire new mirror set, which requires a minimum of two physical disks. Because the physical chassis currently possesses only one unpopulated drive bay, executing a standard online expansion by dropping a single drive into the matrix is structurally impossible. Therefore, the operations team must first evaluate the PowerEdge RAID Controller (PERC) capabilities, confirm the exact physical drive slot constraints, and determine if alternative modification methods-such as sequentially swapping existing drives with higher-capacity units- are supported by the firmware. Attempting an immediate online capacity modification without inspecting controller constraints can lead to unexpected failures, and replacing the physical controller on a live production machine introduces severe operational downtime that violates the continuous availability mandate.

Study Guide References: Server Maintenance; PowerEdge RAID Controller (PERC) Operations; Online Capacity Expansion Constraints.

NO.9 A PowerEdge R760 powers on with no video output. You decide to perform a Minimum-to-POST test. Which configuration correctly represents a valid Minimum-to-POST?

A. One CPU with all associated DIMM, one PSU, no PCIe card

B. One CPU, one DIMM in the primary channel, one PSU, no PCIe card

C. Two CPUs installed with all DIMMs populated, one PCIe card

D. One CPU with all associated DIMM, one PSU, one PCIe card

Answer: B

Explanation:

Isolating a severe execution failure such as a No-Video or No-POST state on a Dell PowerEdge R760 server requires executing a systematic component isolation strategy known as a Minimum-to-POST test configuration. This diagnostic process establishes the absolute minimum selection of core electrical and compute components required for the platform's Unified Extensible Firmware Interface (UEFI) and baseboard management controller to initialize, clear power-on diagnostics, and complete core system initialization. For a standard PowerEdge 16G dual-socket chassis, a valid Minimum-to-POST configuration consists strictly of one central processing unit (CPU 1), a single memory module (DIMM) installed in the designated primary memory channel slot associated with CPU 1, one functional power supply unit (PSU), and the complete removal of all auxiliary components, including expansion riser cards, non-essential storage backplanes, and PCIe accelerators. Excluding unneeded components removes potential electrical shorts, device negotiation lockups, and bus initialization faults from the communication path, allowing technicians to definitively confirm if the foundational motherboard assembly, processor, or primary memory block is the root cause of the system failure.

Study Guide References: Troubleshooting; Minimum-to-POST Diagnostic Subsystems; Hardware Isolation Fault Recovery.

NO.10 A customer reports four physical GPUs installed but only three are detected by the OS on a

PowerEdge XE with NVIDIA cards. Which command should be used to identify the missing GPU?

A. rocm-smi

B. nvidia-smi -L

C. dcgmi diag -r 4

Answer: B

Explanation:

Dell PowerEdge XE acceleration platforms hosting multiple high-performance enterprise accelerators rely on specific driver subsystems to communicate with the host operating system. When a hardware discrepancy occurs-such as only three out of four physical NVIDIA GPUs initializing successfully-the administrator must utilize the specialized NVIDIA System Management Interface utility (nvidia-smi) to interrogate the driver layer. Executing the command nvidia-smi -L lists all recognized graphics processing units currently attached to the system along with their operational indexes, model names, and specific Universally Unique Identifiers (UUIDs). If a physical card is completely missing from this command output, it implies the operating system driver has failed to discover or bind to the device during the boot sequence. This standard isolation step allows an engineer to quickly cross-reference the recognized hardware against the system's physical topology to pinpoint the exact slot location requiring physical intervention. Study Guide References:

Troubleshooting; GPU Acceleration Management; NVIDIA System Management Interface Subsystems.

NO.11 You are installing an OS remotely using Virtual Media In IDRAC. When you to launch the Virtual Media client, the message: "Virtual media is currently unavailable" appears. What is the cause of this error?

A. USB is unreachable

B. A remote file share session is active

C. The server is powered off

D. The ISO file is corrupted

Answer: B

Explanation:

The Integrated Dell Remote Access Controller (iDRAC) Virtual Media feature allows an administrative workstation to map local or network-attached disk images directly to the host server as virtual USB storage components. However, when the console client reports that "Virtual media is currently unavailable," it indicates an active session contention policy enforcement within the out-of-band controller subsystem. This state typically occurs when a remote network file share session-such as a concurrent ISO mount via an explicit CIFS, NFS, or HTTP/HTTPS configuration path-is already bound to the virtualization engine. The underlying architecture restricts simultaneous file mapping sources to prevent data stream collision and drive mapping conflicts at the boot manager layer. To restore client-side interactive Virtual Media functionality, any pre-existing background server-side network mount mappings must be explicitly unmounted or disconnected. Once the background storage pipeline is cleared, the controller frees the virtual device manager lock, allowing the administrator to successfully establish a new client-based media redirect session.

Study Guide References: Troubleshooting; Virtual Media Subsystems; iDRAC Remote Management Session Policies.

NO.12 A technician receives a new server with five drives. They need to configure the drives based

on the following requirements received from the administrator:
* Drive 0 as a single disk with no RAID
* Drives 1-3 as a RAID 5 with drive 4 as a hot spare just for this newly created RAID 5 The administrator plans to add more disks as separate RAID arrays at a later date but only wants drive 4 to be available for this first RAID 5 set.
How should the technician configure the drives?

A. Set drive 0 to Non-Raid; set drives 1-3 as RAID 5; set drive 4 as a Dedicated Hot Spare

B. Set drive 0 to Ready; set drives 1-3 as RAID 5; set drive 4 as a Global Hot Spare

C. Set drive 0 to Ready; set drives 1-3 as RAID 5; set drive 4 as a Dedicated Hot Spare

D. Set drive 0 to Non-Raid; set drives 1-3 as RAID 5; set drive 4 as a Global Hot Spare

Answer: A
Explanation:
In Dell PowerEdge storage architectures managed by PowerEdge RAID Controllers (PERC), configuring individual physical drives to fulfill precise array and operational boundary conditions requires proper manipulation of disk states. For Drive 0, which must function independently as a standalone disk completely outside of any RAID layer, the technician must explicitly toggle its operational state to 'Non-RAID'. Leaving a drive in the 'Ready' state means it remains unconfigured and unmapped, preventing direct pass-through operating system initialization. For Drive 4, the requirement specifies that it must act as a protective failover drive restricted exclusively to the newly provisioned RAID 5 volume composed of Drives 1-3. To achieve this structural isolation, Drive 4 must be configured as a 'Dedicated Hot Spare' bound strictly to that specific virtual disk group. If configured as a 'Global Hot Spare', the disk controller would automatically deploy Drive
4 to assist any compatible degraded array across the entire backplane, violating the administrator's constraint to preserve it solely for the first RAID 5 set when future storage pools are introduced later. Therefore, Option A represents the only structurally valid layout configuration.
Study Guide References: Server Deployment; PowerEdge RAID Controller (PERC) Configurations; Drive States and Hot Spare Assignment Policies.

NO.13 A PowerEdge server is running critical production workloads and has passed all validation and compliance checks. The security team requires that no unauthorized or accidental changes be made to the system configuration during the production phase. Later, the administrator attempts to update the BIOS remotely using iDRAC but the operation fails without applying any changes. Which is the most likely reason for this behavior?

A. TPM is blocking the firmware operation

B. System Lockdown Mode is enabled

C. Secure Boot is preventing the BIOS update

D. The RAID controller is in a degraded state

Answer: B
Explanation:
Dell PowerEdge cyber-resilient security features include an integrated System Lockdown Mode designed to block unauthorized configuration changes across production environments. When an administrator activates System Lockdown Mode via iDRAC, the management subsystem applies a global execution block on all configuration settings and firmware modification vectors. This security policy explicitly blocks any firmware updates targeting the BIOS, iDRAC, Lifecycle Controller, power supply units, or storage controllers, regardless of whether the request originates from a valid

administrator account or an external orchestration tool. Any attempt to stage a Dell Update Package (DUP) or initiate a remote firmware modification results in an immediate execution failure to protect the system's baseline status. To successfully apply a critical BIOS update or modify a managed variable, the administrator must explicitly disable System Lockdown Mode, perform the required infrastructure maintenance, and then re-enable the lockdown wrapper to restore full system protection.
Study Guide References: System Administration; Cyber Resilient Security; System Lockdown Mode Management.

NO.14 You are managing PowerEdge Servers in different locations across the globe. Your security team instructed you to apply specific settings and firmware on the BIOS to comply with Company policies. You must ensure these applied settings and firmware do not change or have anomalies overtime. How could you achieve this?

A. Use DC-HPM

B. Use Enterprise Key Management

C. Use BIOS Live Scanning

D. Use DC-MHS

E. Use iDRAC Credential Vault

Answer: C

Explanation:
Dell PowerEdge servers feature advanced cyber-resilient architectures designed to enforce configuration baseline integrity and eliminate configuration drift across enterprise deployments. When security policies require that globally deployed BIOS configuration options and cryptographic firmware structures remain absolutely locked against unauthorized alteration or external corruption, administrators must leverage the BIOS Live Scanning feature. Available under the iDRAC Datacenter tier license, BIOS Live Scanning enables continuous out-of-band validation of the primary ROM image without requiring host operating system intervention or incurring system downtime. This background security daemon executes cryptographically signed checksum comparisons on critical immutable boot blocks either on-demand or automatically via a scheduled frequency. If any structural modification, unauthorized firmware flash attempt, or memory bit anomaly is detected during runtime operations, iDRAC instantly records the tamper event within the Lifecycle Controller Logs and System Event Logs. This feature ensures total transparency and compliance verification across distributed multi-region infrastructures without degrading production computing performance.
Study Guide References: System Administration; Cyber Resilient Security; iDRAC Datacenter Telemetry Subsystems.

NO.15 A system administrator is tasked with upgrading the environment to VMware vSphere 8 and manage the latest Dell PowerEdge servers. The company wants to simplify operations, reduce costs, and avoid using multiple tools for physical and virtual infrastructure management. Which integration should the administrator implement to meet these requirements?

A. Use standalone OpenManage Server Administrator

B. Continue using OMIW for VMware integration

C. Deploy OpenManage Enterprise with VMware vCenter

D. Implement manual firmware updates and health checks

Answer: C

Explanation:
In enterprise virtualization environments leveraging VMware vSphere 8, traditional hardware management paradigms using siloed toolsets add operational complexity and increase administrative costs. To address this, Dell provides the OpenManage Enterprise (OME) integration with VMware vCenter. Deploying OpenManage Enterprise combined with VMware vCenter plugins enables administrators to consolidate bare-metal infrastructure management directly within the native vSphere Client. This unified interface gives systems administrators single-pane-of-glass operational visibility, allowing them to monitor physical hardware health, perform automated baseline configuration compliance reviews, and execute cluster-aware firmware updates across groups of PowerEdge nodes simultaneously. This integration avoids the need for standalone utilities like OpenManage Server Administrator (OMSA) or legacy standalone OpenManage Integration for VMware vCenter (OMIW) virtual appliances, significantly reducing management overhead. By automating routine component orchestration workflows and synchronizing hypervisor hosts with physical host profiles, data centers can achieve strict lifecycle compliance baselines with minimal operational risk and complete optimization of physical resources.
Study Guide References: System Administration; Dell OpenManage Enterprise Integrations; VMware vCenter Lifecycle Orchestration.

NO.16 A Dell PowerEdge R750 shows a sudden reduction in usable capacity on a RAID 6 virtual disk after replacing a failed drive with a larger one. The OS and iDRAC both report the VD as "Ready'" and "Optimal" but usable capacity remains unchanged. What is the cause of this behavior?

A. The drive was added as a dedicated hot spare instead of a member disk

B. The virtual disk remains limited by the smallest disk

C. The rebuild failed and the virtual disk is using reduced capacity mode

D. The virtual disk automatically expanded but the OS has not refreshed

Answer: B

Explanation:
When an administrator replaces a degraded physical drive within an existing RAID 6 array with a drive of a larger capacity, the usable storage space of the virtual disk layout remains bound to its original values. In hardware storage configurations managed by a PowerEdge RAID Controller (PERC), the maximum storage contribution of any individual member disk within a specific array group is strictly governed by the footprint of the smallest operational drive initialized during the array's creation. Consequently, even though the new disk successfully initializes, passes validation, and registers an 'Optimal' or 'Ready' status via the iDRAC management engine, the excess capacity residing on that larger drive remains unallocated and unusable within the current parity volume configuration. To exploit the additional raw capacity, every single participant drive in that specific RAID group must be sequentially upgraded to matching larger sizes, allowing the controller to successfully execute a virtual disk extension or Online Capacity Expansion (OCE) process across the expanded array boundaries.
Study Guide References: Server Maintenance; PowerEdge RAID Controller (PERC) Layouts; Storage Array Rebuild Mechanics.

NO.17 After adding a GPU to a Dell PowerEdge server:
* The operating system does not detect the GPU.
* Lifecycle Controller (LCC) Diagnostics reports a POST failure.
* IDRAC System Event Log shows a GPU power-related error.

What action should be performed first for practical troubleshooting?

A. Reset the iDRAC network configuration.

B. Modify the BIOS Thermal Profile.

C. Reinstall the GPU driver.

D. Reseat the GPU in its PCIe slot.

Answer: D

Explanation:

When a high-performance graphic processing unit (GPU) accelerator is integrated into a Dell PowerEdge server and produces a POST failure alongside power-related errors, the initial remediation vector must address structural physical alignment. A PowerEdge server uses complex PCIe riser topologies designed with tight mechanical and electrical tolerances to distribute auxiliary power and high-speed data lines. If a GPU is not fully home or correctly seated within its designated PCIe lane assignment, the pins responsible for negotiating power consumption thresholds and sideband device signaling will exhibit high resistance or open circuits. This physical deviation induces localized voltage drops and causes the iDRAC telemetry agent to log a power delivery failure. Because the operating system driver cannot establish communication with an uninitialized or unmapped PCIe device, software modifications such as driver reinstallation or network modifications will fail to influence the condition. Physically isolating the component, inspecting the slot contacts for debris, and firmly reseating the accelerator into its respective slot establishes the necessary hardware baseline required to pass early UEFI initialization tests.

Study Guide References: Troubleshooting; GPU Acceleration Management; Expansion Riser and Bus Interconnect Diagnostics.

NO.18 A customer wants to deploy security compliance at hardware level using TPM hashing algorithm. Which hashing algorithm meets the requirements of the customer?

A. SHA-256

B. MD5

C. SHA-1

D. AES-256

Answer: A

Explanation:

Trusted Platform Module (TPM) 2.0 implementations on Dell PowerEdge servers provide hardware-level cryptographic assurance to verify boot integrity and satisfy strict corporate security compliance policies.

When selecting a cryptographic hashing algorithm for key derivation, platform configuration register (PCR) measurements, and system configuration sealing, modern enterprise standards demand robust collision resistance. The SHA-256 (Secure Hash Algorithm, 256-bit) algorithm serves as the default secure baseline for TPM 2.0 architectures, entirely replacing legacy hashing structures like SHA-1 which are mathematically vulnerable to signature collision exploits. MD5 is completely deprecated due to structural encryption weaknesses, and AES-256 is an advanced symmetric encryption cipher rather than a one-way cryptographic hashing function. By configuring the TPM platform configuration matrix to utilize SHA-256 hashing, the PowerEdge firmware generates dense, fixed-length cryptographic digests for every individual firmware component, option ROM, and operating system bootloader layer initialized during the early system startup sequence. This establishes a robust hardware root of trust that ensures total protection against sub-OS rootkits and pre-boot data

tampering compliance audits. Study Guide References: System Administration; Cryptographic Root of Trust; TPM 2.0 Security Compliance and Hashing Algorithms.

NO.19 You are installing a PowerEdge R7725 into a Bank Data Center. One of the requirements Is to ensure only trusted devices can be used to boot. What BIOS settings can be used to meet this requirement?

A. Boot Settings > BIOS Boot Settings > Boot Sequence

B. Boot Settings > Set Boot Mode to BIOS

C. Network Settings > Set all UEFI PXE Settings to Disabled

D. System Security > Set Secure Boot to Enable

Answer: D

Explanation:

Securing enterprise compute infrastructure within highly regulated environments like a bank data center requires enforcing rigid platform boot-path authorization controls. To satisfy the operational requirement of ensuring that only trusted, cryptographically validated operating system binaries, Option ROMs, and driver devices are permitted to initialize the hardware platform, deployment engineers must implement the Unified Extensible Firmware Interface (UEFI) Secure Boot architecture. Navigating within the System Setup BIOS utility to the 'System Security' page and configuring 'Secure Boot' to 'Enable' activates a cryptographic validation layer. This forces the platform's initialization engine to inspect the digital signatures of all EFI drivers and OS bootloader files against certified keys stored securely within the motherboard's non-volatile RAM. If any unauthorized boot device, malicious pre-boot software, or compromised operating system file lacks a valid signature matching the enrolled certificate authority databases, the server blocks execution completely and halts the boot path. This mechanism effectively neutralizes rootkit vulnerabilities and unauthorized boot-media modifications, verifying complete platform integrity. Study Guide References:
System Administration; UEFI Secure Boot Configuration; System Security Infrastructure Baselines.

NO.20 A technician In Portland, Oregon has been asked to update the firmware on a server in Omaha, Nebraska.
They will use an NFS server also located in Nebraska for serving patches that have been vetted by their security teams. What two pieces of information does the technician need in order to access the NFS patch server from the Lifecycle Controller or iDRAC?

A. Client IP address

B. CHAP authentication credentials

C. Share name

D. Username and password

Answer: A C

Explanation:

In Dell PowerEdge Lifecycle Controller and iDRAC firmware update workflows, mounting a remote network repository via Network File System (NFS) requires specific parameters. Unlike authenticated protocols such as CIFS/SMB or HTTPS, standard NFS relies on IP-based or hostname-based access control lists configured on the hosting server. Therefore, no username or password credentials or Challenge-Handshake Authentication Protocol (CHAP) parameters are required or evaluated during the connection initialization. To establish a communication session from the client endpoint, the network administrator must define two primary network parameters inside the firmware update

interface: the absolute IP address or fully qualified domain name (FQDN) of the remote server and the exact exported Share Name (or directory path) where the Dell Update Packages (DUPs) reside. The iDRAC utilizes these metrics to issue an explicit mount command.
Note that the label 'Client IP address' in some interface legacy fields represents the network path context of the target endpoint server repository connection. Verifying that the target server path is properly exported to allow access ensures a successful firmware execution lifecycle.
Study Guide References: Server Deployment; Remote Firmware Repository Management; Network File System Protocols.

NO.21 A technician In a data center must update the firmware on a server that has no network connectivity. Which two tools must the technician use together to update the BIOS, iDRAC, and lifecycle Controller firmware?

A. USB key with Dell Update Package

B. Virtual console

C. SMB share

D. OpenManage Server administrator

Answer: A D

Explanation:
Performing critical firmware maintenance on an isolated Dell PowerEdge server operating inside a secure, dark-site data center environment with no network connectivity removes remote repository or remote share update methods. In this scenario, the technician must transition to an in-band local maintenance methodology.
This requires using a physical USB key loaded with the appropriate local system Dell Update Packages (DUPs) compiled for the server's specific operating system environment. To execute these payload packages directly inside the host environment, the technician relies on OpenManage Server Administrator (OMSA).
OMSA establishes a localized communication loop with the underlying Lifecycle Controller and iDRAC subsystems via native operating system drivers. Because network subsystems are unavailable, remote out-of- band delivery tools such as the iDRAC Virtual Console or network-attached Server Message Block (SMB) shares will fail to initialize or route patches to the target system. Utilizing the local OMSA deployment interface alongside a physically attached USB storage drive ensures a secure, controlled update process across the BIOS, iDRAC, and controller planes.
Study Guide References: Server Maintenance; In-Band Firmware Deployment; OpenManage Server Administrator Utilities.

NO.22 A disk fails in a RAID 5 array on a PowerEdge R760. You replace it, but the rebuild process takes longer than expected. What is a possible cause of this behavior?

A. The OS needs updates

B. The rebuild process slows down the array

C. The replacement disk is the wrong size

D. The RAID cache card is disabled

Answer: D

Explanation:
A prolonged physical drive reconstruction cycle inside a RAID 5 array on a Dell PowerEdge R760 server points to performance-limiting configurations or structural bottlenecks within the internal

storage subsystem architecture. When the physical RAID cache card is disabled or enters a forced 'Write-Through' operational state-often caused by a depleted, uncharged, or faulty battery backup unit (BBU)-the controller switches off its high-speed volatile write-caching pipelines. Without a functioning write cache, all read-modify-write parity computations required to rebuild data blocks onto the new replacement drive must be committed directly to the persistent disk media, incurring substantial rotational or flash write latencies. This technical shift drops random and sequential storage I/O throughput by orders of magnitude, causing the drive synchronization progress to run significantly slower than normal. While active production workloads running concurrently on the host array can also stretch completion windows, a disabled cache architecture represents the principal hardware-level degradation mechanism causing unexpectedly long rebuild cycles during maintenance operations.
Study Guide References: Troubleshooting; Storage Cache Operational Modes; PERC Battery Backup Units and Rebuild Priorities.

NO.23 A Dell PowerEdge server becomes unresponsive at the operating system level, but an administrator still needs to check hardware health, review system event logs, and diagnose potential component failures remotely.
Which two tools can be used to perform these tasks independently of the operating system?
A. LCC
B. iSM
C. OMSA
D. iDRAC
Answer: A D
Explanation:
When a Dell PowerEdge server encounters a severe fault that leaves the host operating system completely locked or unresponsive, conventional in-band systems management utilities lose operational visibility. To inspect underlying hardware components and perform error extraction under these conditions, administrators must rely on tools operating entirely separate from the host OS kernel plane. The Integrated Dell Remote Access Controller (iDRAC) serves as the primary out-of-band management plane, functioning on an independent system-on-chip with separate power delivery. It enables continuous hardware monitoring, health status evaluations, and comprehensive System Event Log (SEL) retrieval via remote web, SSH, or API endpoints, regardless of host stability. Concurrently, the Lifecycle Controller (LCC) provides an embedded pre-boot deployment and diagnostic framework directly integrated within the platform firmware. If a cold reboot is executed, an engineer can enter the LCC environment to run exhaustive hardware diagnostics on processors, memory, and storage sub-assemblies. Conversely, tools like OpenManage Server Administrator (OMSA) and the iDRAC Service Module (iSM) are in-band agents requiring a functional operating system to run.
Study Guide References: Troubleshooting; Out-of-Band Management Infrastructure; Lifecycle Controller Pre- boot Diagnostics.

NO.24 You are assisting an administrator, who Is working on a PowerEdge R670. They are trying to connect to iDRAC using iDRAC Direct but cannot make a connection. The LED status indicators are: the wrench
/spanner LED on the front right is off, the system ID LED on the front right is blinking blue, and the power LED on the front right is amber. What action should be taken to establish connectivity?

A. Press the power button once
B. Press and hold the system ID button for 5-10 seconds
C. Press the system ID button once
D. Press and hold the power button for 5-10 seconds
Answer: B
Explanation:
On modern Dell PowerEdge servers like the R670, the physical System ID button on the front chassis bezel handles multiple management modes. When a technician finds the system ID LED blinking blue, it indicates that location identification mode is active, which can cause connection conflicts on the shared iDRAC Direct USB subsystem if the underlying controller has entered a locked state. Additionally, an amber power light indicates the system is in a standby or faulted state where standard background tasks might be asleep. To force the baseboard management microchip to reset its local configuration and wake up the iDRAC Direct USB communication interface, the administrator must press and hold the System ID button for 5 to 10 seconds. This long-press action initiates a hard restart of the iDRAC subsystem without disrupting host server computing operations. Once restarted, the controller initializes the front panel USB connection, clears the identification state, and allows the direct network link to connect correctly.
Study Guide References: Troubleshooting; iDRAC Direct Subsystem Faults; Chassis Status Indicators and Hardware Control Nodes.

NO.25 An engineer needs to install an OS that is not supported by the Lifecycle Controller on a Dell PowerEdge server. Since the OS Deployment menu cannot be used, the engineer plans to proceed with a manual installation. Which two factors should be considered in this situation?
A. Appropriate drivers based on storage configuration must be applied.
B. Required drivers are manually managed during installation.
C. Hardware compatibility with the OS must be verified before installation.
D. Firmware and driver version compatibility is checked after installation.
Answer: B C
Explanation:
Deploying an operating system that lacks native entry listings within the Dell Lifecycle Controller embedded OS deployment framework mandates transitioning to a completely unassisted manual installation model.
Under this architecture, the automated injection of optimized Dell driver bundles is bypassed, altering the responsibilities placed upon the systems deployment engineer. The first primary factor requiring validation is verifying hardware compatibility with the OS prior to starting the installation sequence. Deploying an unvalidated or end-of-life operating system platform on modern PowerEdge architectures can lead to immediate initialization faults or kernel panics if the kernel cannot map modern x86 instructions or advanced chipsets. The second primary factor is that required device drivers must be manually managed throughout the OS installation lifecycle. Because the deployment wizard cannot automate disk controller or network interface initialization, the engineer must manually supply appropriate storage drivers-such as PERC or BOSS-N1 drivers-via secondary media to ensure the installation targets are exposed and accessible.
Study Guide References: Server Deployment; Manual OS Installation Methodologies; Operating System Matrix Verification.

NO.26 After updating BIOS and NIC firmware using Lifecycle Controller, a PowerEdge server boots into Lifecycle Controller instead of the OS, although the OS disks are intact. What is the most likely root cause?

A. Boot mode was changed

B. RAID metadata corruption

C. Secure Boot certificates expired

D. iDRAC lost network connectivity

Answer: A

Explanation:

When a PowerEdge server bypasses its standard operating system boot sequence and automatically defaults into the pre-boot Lifecycle Controller interface following a firmware flash event, it signifies a disruption within the NVRAM boot variable mapping. A frequent consequence of major BIOS or platform firmware updates is the reset or modification of the global Boot Mode setting back to factory defaults or an alternate state. For instance, if the operating system was originally deployed under a modern Unified Extensible Firmware Interface (UEFI) profile, and the firmware update script forces the system back to legacy BIOS mode, the platform initialization layer will be unable to discover or interpret the UEFI bootloader block.

Because the system cannot find a valid boot target matching its current boot mode configuration, it defaults to the embedded management partition. Reviewing the Boot Settings menu inside the System Setup utility to verify and align the boot mode with the operating system layout resolves this boot loop without data loss.

Study Guide References: Troubleshooting; UEFI Boot Order Synchronization; System Setup Configuration Verification.

NO.27 You are deploying an OS on a new Dell PowerEdge R760 at a dark-site data center. There is no management network for iDRAC, and you need to configure IDRAC using virtual media. What must you do in order to access the web interface to use the virtual media?

A. Connect using OpenManage Mobile

B. Enable PXE boot in BIOS

C. Connect using iDRAC direct

D. Update the iDRAC firmware using Lifecycle Controller

Answer: C

Explanation:

In a secure, dark-site data center environment completely lacking local management network infrastructure, traditional remote out-of-band access to the Integrated Dell Remote Access Controller (iDRAC) web user interface is unavailable. To circumvent this constraint and establish a localized, direct management session for operating system deployment, engineers utilize the integrated iDRAC Direct feature. By physically connecting a client workstation via a standard USB cable to the designated iDRAC Direct port located on the front panel of the PowerEdge R760, the management subsystem automatically provisions an isolated, point-to- point virtual network link. This connection automatically maps a link-local IP address configuration to the host controller, enabling the technician to launch a local web browser and securely log into the graphical user interface. From this session, the administrator gains access to the full suite of infrastructure deployment utilities, including the Virtual Media framework. This allows a remote operating system installation ISO image to be mapped directly to the server as a bootable virtual device, enabling successful bare-metal OS

initialization without requiring external switches or routers.
Study Guide References: Server Deployment; iDRAC Direct Connectivity; Virtual Media Provisioning.

NO.28 During a physical Inspection, the System Status LED Is blinking blue. What does this indicate?
A. Hardware fault detected
B. PSU redundancy lost
C. Thermal threshold exceeded
D. System is being identified
Answer: D
Explanation:
The physical front chassis panel of a Dell PowerEdge server features an integrated health and identification indicator framework, including the System Status LED. When this specific LED emits a continuous or intermittent blinking blue pattern, it indicates that the system identification mode has been activated by an infrastructure administrator. This behavioral status is not an indicator of a hardware fault, thermal threshold breach, or network connectivity disruption. Instead, it serves as a structural locating mechanism designed to assist data center technicians in accurately identifying a specific physical chassis within a high-density equipment rack during maintenance routines. This beacon state can be toggled manually by pressing the physical System ID button on the front or rear panels, or remotely via the iDRAC web interface, RACADM CLI utilities, or OpenManage Enterprise orchestration tools. Once the technician completes the scheduled field intervention, pressing the button again deactivates the blinking sequence, returning the LED to a solid blue pattern signifying a normal operational status.
Study Guide References: Server Monitoring; Front Panel Diagnostic Indicators; Chassis Topology Mapping.

NO.29 After adding DIMMs on a PowerEdge R760, the server powers on, fans spin, but the system does not reach POST. The LCD shows no error. What two things should be done to resolve this Issue?
A. Reseat memory
B. Replace the system board
C. Verify DIMM population
D. Update the BIOS
E. Clear SEL logs
Answer: A C
Explanation:
When a modern Dell PowerEdge R760 server experiences a No-POST condition immediately following a memory capacity expansion, the root cause is almost exclusively tied to a physical installation error or an unvalidated configuration layout. Modern Intel Xeon Scalable processor architectures implement complex, multi-channel memory controllers that operate under rigid DIMM population matrices and balanced routing rules. If newly added modules are inserted into incorrect slots or violate the strict symmetrical configuration criteria mandated by the system architecture, the memory controller will fail to pass early hardware training phases, preventing the server from completing POST. To remediate this specific behavior, the technician must verify the exact DIMM population rules outlined in the technical documentation to ensure proper channel alignment. Following validation, a physical reseating of the memory modules must be completed to rule out minor electrical contact resistance or structural alignment faults inside the slots. Study Guide

References:
Troubleshooting; Memory Subsystem Architecture; POST Failure Isolation and Memory Population Rules.

NO.30 A PSU is blinking green on a PowerEdge R750 while there no issue reported in the iDRAC. What is the most likely cause?

A. The firmware of the PSU is being updated

B. This indicates a PSU mismatch

C. A valid power source is connected to the PSU

D. indicates an issue with the PSU

Answer: A

Explanation:
In Dell PowerEdge server hardware troubleshooting frameworks, interpreting the precise visual telemetry provided by the physical components is necessary to isolate transient automated maintenance operations from genuine hardware faults. On a PowerEdge R750 server, an individual Power Supply Unit (PSU) status LED exhibiting an isolated blinking green pattern typically signifies that the unit's embedded microcontroller is currently undergoing a live firmware update flash sequence orchestrated by the Lifecycle Controller. During this specific update lifecycle window, the out-of-band management plane intentionally suppresses standard redundancy alerts or warning generation within the Integrated Dell Remote Access Controller (iDRAC) web interface. This suppression prevents transient power fluctuations or momentary redundancy loss indicators from triggering false positive critical system infrastructure events. A steady, solid green LED pattern indicates stable normal operational input voltage detection, while a true physical mismatch or hardware component circuit failure would cause the LED to transition to a flashing or solid amber alert pattern. Thus, the absence of an active iDRAC fault entry coupled with the flashing green LED validates a running background patch deployment. Study Guide References: Troubleshooting; Power Supply Subsystem Diagnostics; Hardware Firmware Updates and LED Diagnostics.

NO.31 A Dell PowerEdge server is experiencing intermittent hardware alerts, and the operating system is occasionally unresponsive. An administrator needs to diagnose and troubleshoot the hardware issue efficiently. Which three tools can be used to troubleshoot hardware issues on a Dell PowerEdge server?

A. Operating system application logs

B. LiveOptics

C. OME

D. iDRAC

E. Lifecycle Controller diagnostics

Answer: C D E

Explanation:
Isolating hardware faults on Dell PowerEdge servers requires leveraging specialized infrastructure tools designed to collect and parse low-level component telemetry. The Integrated Dell Remote Access Controller (iDRAC) provides an independent, out-of-band management plane that monitors component health status continuously and records historical errors within the localized System Event Log (SEL). For hardware-level diagnostics executed outside the operating system workspace, the Lifecycle Controller (LCC) diagnostics offer embedded, pre-boot UEFI test suites capable of

performing exhaustive stress tests on the processor, physical memory blocks, and storage backplanes. At an infrastructure-wide level, OpenManage Enterprise (OME) acts as a centralized console that aggregates hardware alerts, evaluates firmware compliance baselines, and monitors structural events across multiple server nodes simultaneously. Together, these three solutions provide the dedicated out-of-band monitoring and localized diagnostics necessary to resolve intermittent hardware anomalies. Study Guide References: Troubleshooting; Dell OpenManage Systems Management Portfolio; Pre-boot Diagnostics and iDRAC Telemetry.

NO.32 A Dell PowerEdge server has Temperature Alert Configuration set up in iDRAC. A Test Event was executed, and email alerts appeared to be delivered successfully. However, a few days later, the server unexpectedly rebooted. Upon inspection, CPU temperatures had exceeded the configured threshold. What is a possible reason IDRAC failed to alert the administrator about the high temperature?

A. iDRAC only sends alerts for Critical events or higher.

B. Although the Temperature Alert was configured, it was not fully activated.

C. Test Events verify alert delivery but do not trigger actual hardware alerts.

D. The reboot may have bypassed iDRAC alert mechanisms.

Answer: B

Explanation:

In the Integrated Dell Remote Access Controller (iDRAC) architecture, configuring a destination and executing a successful Test Event merely validates the underlying notification network pathway and the SMTP handshake with the mail server. It does not mean that automated notifications are active for operational system events. To achieve full activation, an administrator must explicitly enable the desired alert actions within the iDRAC Alerts Configuration Matrix. If a specific metric category-such as a thermal or temperature threshold breach-has not been explicitly checked and mapped to an email action inside this matrix, the iDRAC will log the hardware event internally to the System Event Log but will fail to transmit an external message. Consequently, when the CPU temperature surpassed the critical operational threshold, the server executed an automatic protective shutdown without dispatching an alert to the administrator. To prevent this, the alert state must be toggled from configured to fully active across the respective category rows. Study Guide References: Server Monitoring; iDRAC Alert Configuration Matrix; Thermal Management Policies.

NO.33 On a Dell PowerEdge server equipped with NVIDIA GPUs, one of the installed GPUs shows a continuous Increase in ECC Correctable Errors whenever the system is under load. Running dcgmi diag -r 3 returns PASS for all diagnostic tests, and a full GPU memory BIST detects no memory cell faults. The IDRAC System Event Log repeatedly reports: ' Correctable Memory Warning increased" for the same GPU. The system appears healthy, and no PCIe or XID fatal errors are recorded. What action should be taken first?

A. Reduce the GPU memory clock to mitigate temperature-dependent memory errors.

B. Reseat the GPU to eliminate any potential connector or contact issues.

C. Update the PCIe switch firmware to prevent bus-related memory parity errors.

D. Inspect the airflow and thermal conditions for the PCIe slot where the GPU is installed.

Answer: D

Explanation:

When a high-performance NVIDIA GPU accelerator inside a Dell PowerEdge server registers a

continuous increase in single-bit Error-Correcting Code (ECC) correctable errors exclusively under operational compute load, but consistently clears standalone diagnostic validation layers (such as advanced DCGM Level 3 diagnostics and full hardware-level memory Built-In Self-Tests), the issue points to a thermal-dependent signaling issue rather than a permanent physical silicon cell failure. Under intensive processing workloads, localized heat retention within the GPU's dense High Bandwidth Memory (HBM) layout can induce marginal timing variations that force internal ECC engines to work continuously to preserve data accuracy, generating frequent correctable alerts within the iDRAC System Event Log. Because permanent hardware memory cell defects are ruled out by the comprehensive BIST pass execution rating, the first practical troubleshooting step requires inspecting the internal airflow path, cooling fan profiles, and specific thermal conditions surrounding the designated PCIe slot. Ensuring proper air baffling, clearing cable blockages, and validating slot-specific cooling optimization allows the accelerator to remain within nominal operating temperature ranges, completely stabilizing signal integrity under stress. Study Guide References: Troubleshooting; GPU Accelerator Thermal Profiling; Hardware Telemetry and ECC Error Isolation.

NO.34 You are performing a GPU firmware update using IDRAC. IDRAC Direct was used during the update. The update stalls and the GPU appear unresponsive. What is the most likely cause of the issue?

A. The server needs a BIOS downgrade

B. The USB management port interaction

C. The iDRAC license expired during the update

D. The GPU is incompatible with the server OS

Answer: B

Explanation:

The iDRAC Direct feature allows administrators to perform management tasks and firmware updates locally by connecting a client device directly to the designated USB port on the front panel of a Dell PowerEdge server. This connection establishes a localized virtual network link mapping directly to the out-of-band management controller. When a high-performance component firmware update-such as a complex GPU subsystem flash-stalls or causes the device to become unresponsive, the root cause is frequently related to data stream interruptions across this interface. Physical movement of the cable, signal degradation over unshielded connections, or host-side USB controller power-management policies can disrupt the communication handshake between the iDRAC and the target device during execution. Because the firmware payload transmission relies on continuous micro-packet validation through the physical port, any communication breakdown halts the deployment state machine mid-execution. This results in an incomplete firmware block state that requires a hard reset of the management controller to clear.

Study Guide References: Troubleshooting; iDRAC Direct Connectivity; USB Management Port Interconnects.

NO.35 You have replaced a failed drive in slot three for the second time but it's not detected by the PERC. A diagnostic test using the PERCCLI utility indicates that other drives are working properly. What is a possible issue?

A. iDRAC licensing

B. PERC controller is faulty

C. PERC firmware level

D. Backplane or slot connection fault

Answer: D

Explanation:

When a replacement hard drive or solid-state drive fails to be recognized or initialize after multiple swap attempts in the exact same physical slot, the issue typically stems from a localized physical layout failure rather than a global controller fault. The PowerEdge RAID Controller (PERC) utilizes a command-line interface tool called PERCCLI to query storage topology and interact with attached physical disk objects.

Because the PERCCLI diagnostics verify that all other member drives across the remaining slots are functioning normally and communicating flawlessly with the controller, the core integrity of the PERC assembly itself is validated. This isolates the failure to a point-of-failure unique to that specific node coordinate. The root cause is almost exclusively a hardware defect within the physical storage backplane, a damaged or bent pin inside the slot 3 SAS/SATA connector receptacle, or a loose internal signal/power cable linkage connecting that specific backplane segment. Mechanical wear from inserting drives can degrade the slot interface, preventing proper electrical contact. Study Guide References: Troubleshooting; Storage Subsystem Diagnostics; PERCCLI Command Operations and Backplane Isolation.