**Vendor:** Dell-EMC

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

**Exam Name:** Dell PowerEdge Operate v2

**Version:** DEMO

**QUESTION 1**
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.

**QUESTION 2**
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.

**QUESTION 3**
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.

**QUESTION 4**
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.

**QUESTION 5**
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:** AC
**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.

**QUESTION 6**
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.

**QUESTION 7**
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.

**QUESTION 8**
A company with a 17G PowerEdge Server model requires these features: Essential System Management Features; Core Features, Automation, Virtual and Security Enhancements; Enterprise Features with added telemetry, thermal management, support for accelerators (GPU and DPU), and advanced Air and Liquid Cooling. Which iDRAC license is the minimum required to meet these requirements?

A. Datacenter
B. Core
C. Enterprise
D. Express

**Answer:** A
**Explanation:**
Meeting the infrastructure demands of modern, high-density Dell PowerEdge servers requires matching capabilities with the correct operational license tier. While lower license tiers--such as Express and Enterprise--provide basic server lifecycle automation, user directory integrations, and general monitoring functions, they lack the advanced telemetry pipelines needed for complex deployments. The Datacenter license tier is specifically engineered to manage large-scale data centers running complex workloads. It provides comprehensive telemetry streaming features alongside specialized thermal optimization hooks, which are required to support advanced computing accelerators like GPUs and DPUs. Furthermore, managing modern advanced cooling architectures--including automated air cooling adjustment algorithms and direct-contact liquid cooling loops--is restricted to the Datacenter functional framework. Therefore, to unlock these advanced instrumentation metrics, performance profiles, and thermal capabilities, the Datacenter tier license must be applied as the minimum operational baseline.

**QUESTION 9**
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.

**QUESTION 10**
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.

**QUESTION 11**
A PowerEdge server unexpectedly rebooted, and the SEL did not provide enough information to determine the cause. Upon investigation, the engineer noticed that the Last Crash Screen feature was disabled and recommended enabling it. Which primary gap does enabling the Last Crash Screen address?

A. The system may lose the final crash state before logs are written.
B. OS-level crash dump data may be incomplete when writes fail.
C. Crash during POST may cause firmware messages to be lost.
D. Sensor activity may not be captured when a crash occurs suddenly.

**Answer:** A
**Explanation:**
When a Dell PowerEdge server experiences an unexpected kernel panic, blue screen, or spontaneous operating system crash, the local System Event Log (SEL) may fail to preserve sufficient descriptive parameters. This diagnostic visibility gap occurs if the host operating system crashes or loses processing capacity before it can successfully write crash logs across the system bus. Enabling the 'Last Crash Screen' feature inside the iDRAC management architecture directly addresses this limitation by autonomously capturing a precise frame buffer image of the host video output at the exact millisecond a fatal system exception or execution fault is detected. This out-of-band capture logs operating system blue screen (BSOD) parameters, Linux kernel panic dumps, or hypervisor registers directly to non-volatile iDRAC memory. Without this feature active, if a severe exception triggers an immediate automated hardware watchdog reset, the host system transitions through a cold reboot cycle so rapidly that the system completely loses the final crash state before logs are written to disk. Activating this option preserves the high-fidelity data required to troubleshoot non- reproducible boundary faults.

**QUESTION 12**
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.

# Thank You for Trying Our Product

## Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

**10% Discount Coupon Code:** **ASTR14**