

Dell PowerEdge Operate v2 Exam

DELL EMC D-PE-OE-01

Version Demo

Total Demo Questions: 6

Total Premium Questions: 64

Buy Premium PDF

<https://passqueen.com>

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, PowerEdge Server Components	2
Topic 2, PowerEdge Server Configuration	16
Topic 3, PowerEdge Server Management	19
Topic 4, PowerEdge Server Maintenance	8
Topic 5, PowerEdge Server Troubleshooting	19
Total	64

QUESTION NO: 1

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:

USB key with Dell Update Package and **OpenManage Server administrator** support an in-band, local firmware-maintenance workflow when the target PowerEdge server cannot reach a network repository or share. The technician can obtain the Dell Update Packages (DUPs) matching the server model and installed operating system, copy them to removable USB media, and attach that media directly to the server. A DUP is Dell's executable firmware payload format and can include applicable updates for platform components such as the BIOS, iDRAC, and Lifecycle Controller.

OpenManage Server Administrator provides the local server-management environment used from the host operating system to inventory components, assess applicable updates, and invoke the locally available update packages. This approach keeps both the update source and the execution path on the isolated server, rather than depending on external connectivity. Firmware updates may require staged application and a reboot so that the platform controller can complete the update safely. Dell's firmware-update guidance and OpenManage documentation describe the use of Dell-provided update packages and local OpenManage management capabilities for PowerEdge maintenance: [Dell PowerEdge firmware update guidance](#) and [OpenManage Server Administrator User's Guide](#).

QUESTION NO: 2

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:

iDRAC is Dell PowerEdge's dedicated out-of-band management controller and remains available independently of the server's operating system. Because it operates on separate embedded management hardware and has its own network-management capability, an administrator can remotely view overall system health, hardware inventory and sensor readings, alerts, and the System Event Log (SEL) even when the host OS is hung. iDRAC also provides remote console and virtual-media capabilities, allowing recovery actions and access to pre-boot environments without relying on an in-band management agent.

LCC is embedded firmware that runs outside the installed operating system. It provides a pre-OS environment for platform configuration, updates, inventory collection, and hardware diagnostics. Following a reboot, an administrator can reach the Lifecycle Controller through the server console, including an iDRAC virtual console session, and run diagnostics against server components such as memory, processors, storage, and other supported hardware. This makes iDRAC and LCC appropriate management paths when the OS cannot provide monitoring or diagnostic access. Dell documents iDRAC's out-of-band monitoring and logging functions in the [iDRAC User's Guide](#) and describes Lifecycle Controller capabilities in the [Dell Lifecycle Controller overview](#).

QUESTION NO: 3

A system administrator must update the virtual console security settings on their PowerEdge server to comply with company standards. The company requires strong encryption and secure access policies. Which setting meets these requirements?

- A. Use a strong password
- B. Disable SSL encryption for faster performance
- C. Configure an acceptable timeout value
- D. Set SSL encryption to 256-bit or higher

ANSWER: D

Explanation:

Set SSL encryption to 256-bit or higher meets the stated requirement because it applies strong cryptographic protection to the remote virtual-console session. A virtual console carries sensitive interactive traffic between the administrator's client and the PowerEdge server, including displayed server video and remotely entered keyboard and mouse input. Configuring the highest available SSL/TLS encryption level ensures that this management traffic is protected in transit with a high-strength encryption policy, reducing the risk of interception or unauthorized observation over the network.

This setting directly addresses the requirement for strong encryption while supporting secure remote access administration. It should be used as part of the organization's broader iDRAC security baseline, alongside trusted certificates, current TLS protocol and cipher-suite settings, authenticated user accounts, and appropriate session controls. Dell's iDRAC security guidance emphasizes securing management interfaces and encrypted remote-management communications. See Dell's [iDRAC9 Security Configuration Guide](#) and the [iDRAC9 and Lifecycle Controller documentation](#) for configuration and security guidance.

QUESTION NO: 4

A PowerEdge server reports intermittent correctable memory errors in iDRAC, but the operating system remains available and production workloads must not be interrupted. Dell Support requests diagnostic information before any DIMMs are reseated or replaced. What action should the administrator take first?

- A. Clear the System Event Log before the entries become stale
- B. Reseat all installed DIMMs immediately
- C. Generate a SupportAssist Collection from iDRAC
- D. Restart iDRAC to refresh the memory inventory

ANSWER: C

Explanation:

Generate a SupportAssist Collection from iDRAC is the appropriate first action. The collection preserves diagnostic information needed for analysis, including hardware inventory, iDRAC logs, Lifecycle Controller logs, System Event Log entries, and relevant health data. It can be generated out-of-band while the operating system and workloads remain active.

Reseating or replacing DIMMs before collecting the evidence can remove useful fault history and may interrupt production workloads. Clearing the SEL would discard relevant event data, while restarting iDRAC is not the first action when iDRAC is available and reporting the memory condition.

QUESTION NO: 5

A technician is installing additional GPUs in a PowerEdge server. The server must operate the accelerators under sustained production workloads without thermal or power faults. Which three installation requirements should be verified? Select three.

- A. Install each GPU in any available PCIe slot
- B. Verify that the GPU is installed in a supported PCIe slot and riser
- C. Verify that all required auxiliary GPU power cables are connected
- D. Disable iDRAC fan control to reduce acoustic output
- E. Verify the supported PSU capacity and server cooling configuration

ANSWER: B C E

Explanation:

Using a supported PCIe slot and riser, connecting required auxiliary GPU power cables, and verifying the supported PSU and cooling configuration are required checks. GPU support is platform-specific, and the server must provide the required PCIe topology, power delivery, and airflow provisions for the installed accelerator configuration.

Installing the GPU in any available PCIe slot can violate supported slot and riser requirements. Disabling fan control can prevent the platform from responding correctly to thermal demand. Installing an operating-system driver alone cannot resolve a GPU that lacks correct physical power, cooling, or PCIe support.

QUESTION NO: 6

A Dell PowerEdge server reports intermittent hardware alerts and occasional system instability. An administrator needs to identify and resolve the underlying hardware issue with minimal disruption to services. Which action should the administrator take first to troubleshoot the hardware problem?

- A. Use iDRAC to review hardware health status and the SEL
- B. Disable monitoring alerts to prevent false warnings
- C. Reinstall the operating system to eliminate software-related causes
- D. Replace multiple hardware components simultaneously

ANSWER: A

Explanation:

Use iDRAC to review hardware health status and the SEL is the appropriate first action because it provides a non-disruptive, out-of-band view of the server's monitored components and recorded fault history. iDRAC remains available independently of the host operating system, allowing the administrator to investigate a potentially unstable server without restarting it, taking it offline, or making unverified physical changes. The hardware-health pages consolidate the current condition of key components, including processors, memory, storage, power supplies, fans, temperatures, and voltage sensors. The System Event Log provides timestamped events that can reveal intermittent patterns, such as recurring correctable memory errors, thermal excursions, power anomalies, fan warnings, or storage-controller alerts. Correlating those events with the reported instability gives the administrator evidence to identify the affected component and plan targeted remediation. This approach also supports Dell's lifecycle-management workflow, in which administrators use iDRAC monitoring, logs, and diagnostics to assess hardware health before performing corrective service. Dell's iDRAC documentation and PowerEdge support resources describe iDRAC as the platform for remote monitoring and event-log review: [Dell iDRAC9 and Lifecycle Controller documentation](#) and [Dell iDRAC9 User's Guide](#).