# Download Dell EMC D-PE-OE-23 Exam Dumps Free

**Shared by Hutchinson on 17-06-2026**

**For More Free Questions and Preparation Resources**

Check the Links on Last Page

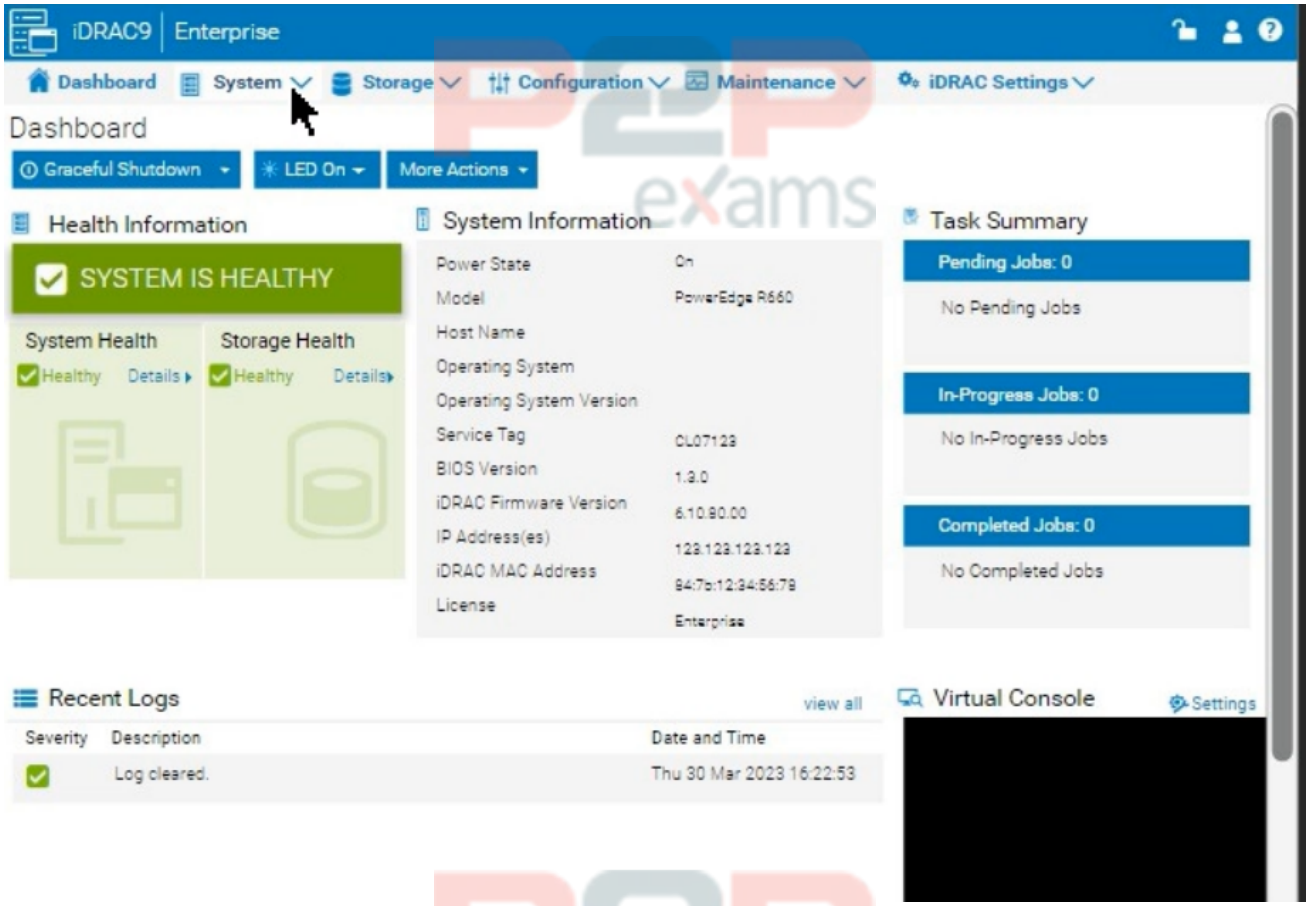
# Question 1

Question Type: MultipleChoice

Click the Launch Simulator button.

Using the iDRAC UI, what is listed as the Cache Memory Size for the H965i storage controller?

Note: It is necessary to close (x) the simulator window before you can select a response to this question.




## Options:

A- 965 MB
B- 8361 MB
C- 1064 MB
D- 8 GB

## Answer:

D

## Explanation:

Launch the Simulator:

Open the PowerEdge iDRAC simulator to access the user interface and perform the required task.

Navigate to System Information:

In the top menu bar, select the 'Configuration' tab.

From the options that appear, choose 'Storage'. This section will display details and configurations for the storage controllers installed on the server.

Check the H965i Storage Controller:

Locate the H965i storage controller in the list. Selecting it should bring up a summary page with various specifications for the controller.

Look for the field labeled 'Cache Memory Size'. This will provide the cache memory size value for the controller.

# Question 2

Question Type: MultipleChoice

An administrator is in a non-secure location with a high latency connection. What option should be used to recover a PowerEdge server using an existing server profile?

## Options:

A- iDRAC
B- Redfish
C- IPMI
D- RACADM

## Answer:

D

## Explanation:

Selecting the Appropriate Recovery Tool

Server Management and Configuration Tools (14%)

Explain the management interface options - LCC, racadm, OMSA, iSM, OME

Scenario Analysis

Constraints:

Non-secure location: Security of the connection is a concern.

High latency connection: Requires a tool that operates efficiently over slow networks.

Objective: Recover a PowerEdge server using an existing server profile.

Option Evaluations

Option A: iDRAC

Analysis: While iDRAC provides remote management, accessing it via a web interface may be slow and less secure in high latency and non-secure environments.

Option B: Redfish

Analysis: Redfish uses HTTPS, which is secure but may not perform well over high latency connections and requires more overhead.

Option C: IPMI

Analysis: IPMI lacks robust security features and is not recommended in non-secure locations.

Option D: RACADM

Correct Answer

Advantages:

Secure: Can use SSH for secure command-line access.

Efficient: Command-line interface minimizes bandwidth usage, suitable for high latency.

Powerful: Allows full management of the server, including applying existing server profiles.

Scriptable: Enables automation and faster recovery processes.

Understanding RACADM

RACADM (Remote Access Controller Admin):

A command-line utility for managing Dell servers via iDRAC.

Supports both local and remote management.

Ideal for automated scripts and low-bandwidth situations.

Dell Operate Reference

Server Management and Configuration Tools (14%)

Emphasizes understanding different management tools and their appropriate use cases.

System Administration (18%)

Covers configuring and managing servers in various environments.

Conclusion

Given the need for a secure and efficient tool in a high latency and non-secure location, RACADM is the optimal choice for recovering the PowerEdge server using an existing server profile.



# Question 3

Question Type: MultipleChoice

Which statement is true about Software RAID?

## Options:

A- Runs only in write-through mode.
B- Runs on embedded CPU and memory.
C- Runs on the NVRAM.
D- Runs on a PERC H965.



## Answer:

B

## Explanation:

Understanding Software RAID

Server Components (26%)

Define storage options, Drives, PERC, IDSDM, and BOSS

What is Software RAID?

Software RAID utilizes the system's main CPU and memory to manage RAID operations, without the need for dedicated hardware RAID controllers.

Functionality:

RAID levels (such as RAID 0, 1, 5) are implemented via software drivers.

Offers flexibility and cost savings by eliminating additional hardware.

Dependent on the operating system and system resources.

Explanation of Options

Option A: Runs only in write-through mode.

Software RAID can support both write-through and write-back modes, depending on the configuration and operating system capabilities.

Conclusion: Incorrect.

Option B: Runs on embedded CPU and memory.

Software RAID relies on the server's main CPU and system memory to perform RAID calculations and manage data redundancy.

Conclusion: Correct Answer.

Option C: Runs on the NVRAM.

NVRAM (Non-Volatile RAM) is used in hardware RAID controllers to store RAID configuration and cache data. Software RAID does not utilize NVRAM.

Conclusion: Incorrect.

Option D: Runs on a PERC H965.

The PERC H965 is a Dell hardware RAID controller. Software RAID, by definition, does not run on hardware RAID controllers.

Conclusion: Incorrect.

Dell Operate Reference

Server Components (26%):

Define storage options, Drives, PERC, IDSDM, and BOSS: Understanding the differences between software RAID and hardware RAID solutions like PERC controllers.

Storage Options: Knowledge of how storage configurations are managed within servers.

Conclusion

Software RAID runs on the server's embedded CPU and memory, utilizing system resources to manage RAID functions without additional hardware.

# Question 4

Question Type: MultipleChoice

A customer acquired six R750 servers. They must add these servers to their existing R760 iDRAC Group but are encountering errors.

What is the reason for the errors?

## Options:

A- R750 iDRACs firmware is out of date.
B- R750 iDRACs are not running the same version of firmware.
C- 15G and 16G servers cannot be in the same group.
D- The feature requires iDRAC Enterprise.

## Answer:

C

## Explanation:

Understanding iDRAC Group Management and Compatibility

Server Management and Configuration Tools (14%)

Define the function of the iDRAC, login procedures, licensing, and connection methods

Explain the management interface options - LCC, racadm, OMSA, iSM, OME

System Administration (18%)

Configure BIOS, Storage, virtual media, networking, user access, lockdown mode, and group management

Scenario Analysis

The customer has acquired six Dell PowerEdge R750 servers and wants to add them to an existing iDRAC Group that currently contains R760 servers. However, they are encountering errors during this process.

Understanding Dell Server Generations

PowerEdge R750: Part of the 15th Generation (15G) servers.

PowerEdge R760: Part of the 16th Generation (16G) servers.

iDRAC Group Manager Limitations

iDRAC Group Manager allows administrators to manage multiple servers from a single interface.

Important Limitation: Servers of different generations cannot be grouped together in iDRAC Group Manager.

This is due to differences in firmware, hardware capabilities, and iDRAC features between server generations.

Impact: Attempting to add 15G servers (R750) to a group containing 16G servers (R760) will result in errors.

Evaluation of Options

Option A: R750 iDRACs firmware is out of date

Analysis: While outdated firmware can cause issues, it is not the primary reason here. Firmware updates would not resolve the incompatibility between different server generations.

Option B: R750 iDRACs are not running the same version of firmware

Analysis: Similar to Option A, firmware version mismatches can cause problems but not errors related to grouping different generations.

Option C: 15G and 16G servers cannot be in the same group

Correct Answe r: This is the primary reason for the errors encountered.

Option D: The feature requires iDRAC Enterprise

Analysis: Since the customer already has an existing iDRAC group with R760 servers, they likely have the necessary licensing.

Dell Operate Reference

Server Management and Configuration Tools (14%)

Emphasizes understanding iDRAC functionalities and limitations.

System Administration (18%)

Highlights the importance of group management and its constraints.

Conclusion

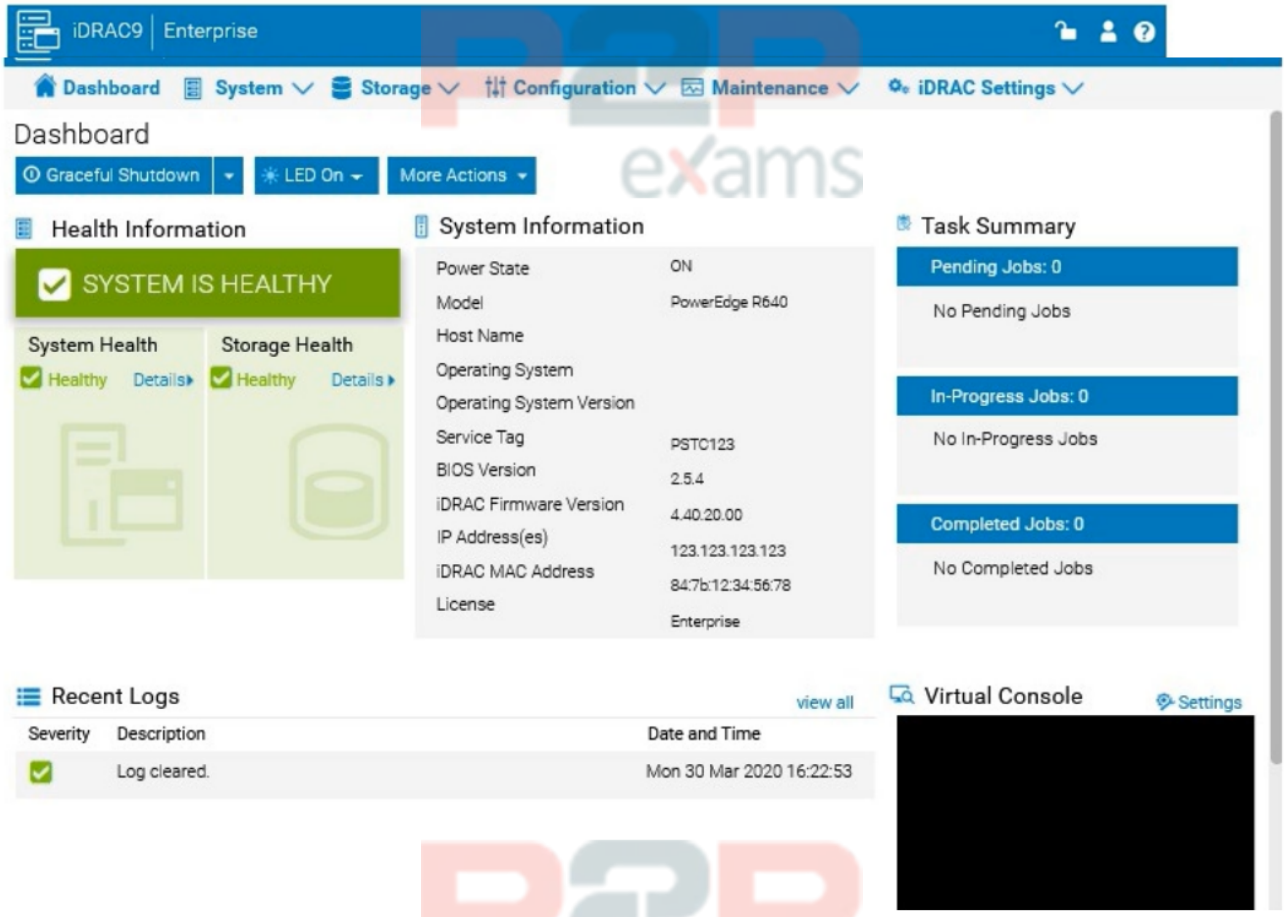
The errors occur because iDRAC Group Manager does not support grouping servers from different generations. The customer cannot add 15G servers (R750) to a group that contains 16G servers (R760).

# Question 5

Question Type: MultipleChoice

SIMULATION

Due to recent security breaches and to avoid accidental changes made by the junior IT staff, an administrator would like to prevent unwanted configuration changes in the iDRAC UI.




## Options:

A- See the Explanation for Step by Step solution

## Answer:

A

## Explanation:

To prevent unwanted configuration changes in the iDRAC UI, you can adjust user roles, permissions, or enable specific security settings to restrict access for junior IT staff. Here are the steps to secure the iDRAC configuration:

Step-by-Step Guide:

Access User Settings:

In the iDRAC interface, navigate to iDRAC Settings from the main menu.

Choose User Authentication or Users to manage user accounts and permissions.

Adjust User Roles and Permissions:

Identify the accounts associated with junior IT staff.

For each user account, adjust the role to Read-Only if you want them to have view-only access without making configuration changes.

Alternatively, set their permissions to exclude configuration changes. This may involve assigning a custom role with limited access based on your needs.

Enable Configuration Lock (if available):

Some versions of iDRAC offer a Configuration Lock feature, which prevents any configuration changes until the lock is removed by an administrator.

Navigate to Configuration > System Security or User Authentication, depending on the version, and enable the Configuration Lock option.

Set Up Two-Factor Authentication (Optional):

For added security, enable Two-Factor Authentication under iDRAC Settings > Network or Security settings. This step ensures only authorized users can access and make changes to the iDRAC UI.

Save and Apply Security Changes:

After setting up the desired restrictions and permissions, save the settings to apply the changes.

Verify that junior IT staff accounts now have restricted access and cannot make configuration changes.

Log Out and Test the Changes:

Log out of the administrator account and log in with a junior IT staff account to confirm that the permissions are set correctly.

Ensure that configuration changes are disabled and that the user can only view the iDRAC interface as per the restrictions.

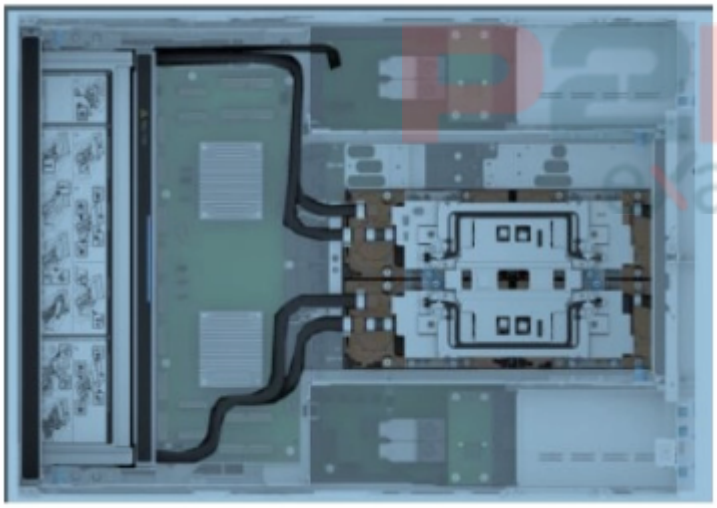
By following these steps, you can restrict junior IT staff from making any configuration changes

within the iDRAC interface, thus preventing accidental or unauthorized modifications.

# Question 6

Question Type: MultipleChoice

Exhibit.



Which two components are displayed in the image?

(Select 2)

## Options:

A- Power cables
B- Paddle card
C- Cold plates
D- Leak sensor

## Answer:

B, C

## Explanation:

Identifying Components in the Exhibit

Server Components (26%)

Identify power options and redundancy features, thermal features, and liquid cooling

Analyzing the Image

From the image, the following two components are displayed:

Cold Plates

Cold plates are a key component of liquid cooling systems used in modern servers to dissipate heat from high-performance components like CPUs and GPUs.

The image shows two prominent cooling structures, which are indicative of cold plates mounted over processors for efficient heat transfer.

Conclusion: Correct Answer.

Paddle Card

Paddle cards are connectors or adapters used to interface between various server components or facilitate cable management.

In this image, the paddle card can be seen as part of the interconnect between the cooling system or main components.

Conclusion: Correct Answer.

Explanation of Other Options

Option A: Power cables

Analysis: There are no visible power cables in the image. The black tubes seen in the image are more likely part of the liquid cooling system, not power cables.

Conclusion: Incorrect.

Option D: Leak sensor

Analysis: Leak sensors are used in liquid cooling systems to detect leaks, but there are no visible sensors or specific indicators of leak detection in the image.

Conclusion: Incorrect.

Dell Operate Reference

Server Components (26%)

Define power and thermal options: Recognizing cooling components like cold plates is essential for understanding server cooling solutions.

Explain expansion cards and their functions: Understanding the purpose of paddle cards helps in identifying how components connect and function in the server.

Conclusion

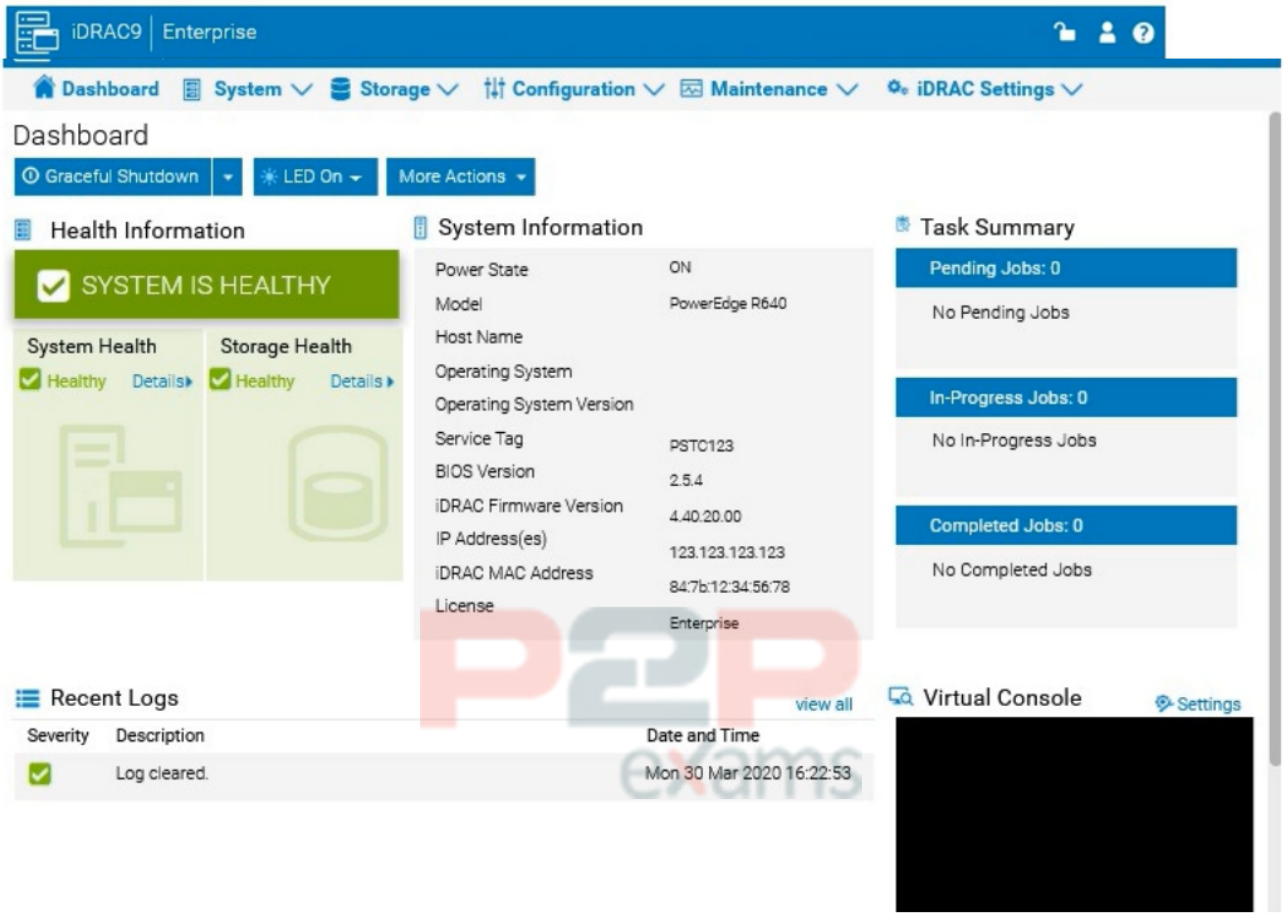
The components visible in the image are Cold Plates and Paddle Cards. These are essential parts of the server's cooling and connectivity systems.

# Question 7

Question Type: MultipleChoice

SIMULATION

Using the iDRAC UI, generate and save locally a SupportAssist collection with system information and debug logs only.




## Options:

A- See the Explanation for Step by Step solution

## Answer:

A

## Explanation:

To generate and save a SupportAssist collection with system information and debug logs only in the iDRAC UI, follow these steps:

Step-by-Step Guide:

Access SupportAssist in iDRAC:

In the iDRAC interface, navigate to the Maintenance tab in the top menu.

From the dropdown, select SupportAssist. This will bring up the SupportAssist options.

Initiate a Collection:

In the SupportAssist section, look for the option to Create a New Collection or Start a Collection.

Choose Collect System Data or Generate a Collection, depending on the version of iDRAC.

Select Collection Components:

When prompted to select components for the collection, check the boxes for System Information and Debug Logs only.

Ensure no other components are selected to limit the collection to just the required data.

Start the Collection:

Confirm your selection, then click Start or Generate. This will initiate the process to gather the specified data from the system.

Save the Collection Locally:

Once the collection is complete, you should see an option to Download or Save the file.

Click the download link and save the collection file locally on your computer.

Verify the Collection File:

Check the downloaded file to ensure it contains only the system information and debug logs. It should be in a format such as ZIP or TAR, depending on the system configuration.

By following these steps, you can successfully generate a SupportAssist collection with just the system information and debug logs and save it to your local system for further review or support purposes.

# Question 8

Question Type: MultipleChoice

The customer implemented ten Dell PowerEdge R660 servers in their data center. The environment also has two MX7000 chassis. The system administrator requires a management application that can help holistically manage and monitor the storage, server, and network environment.

What would be the recommended solution?

## Options:

A- iSM
B- OME
C- Group Manager
D- OMSA

## Answer:

B

## Explanation:

Selecting a Management Application for Holistic Management of Dell PowerEdge Servers and MX7000 Chassis

Server Management and Configuration Tools (14%)

Explain the management interface options - LCC, racadm, OMSA, iSM, OME

System Administration (18%)

Configure BIOS, Storage, virtual media, networking, user access, lockdown mode, and group management

Understanding Customer Requirements

Environment:

Ten Dell PowerEdge R660 servers (rack servers).

Two MX7000 chassis (modular servers).

Requirement:

A management application that can holistically manage and monitor storage, servers, and network environment.

Evaluation of Options

Option A: iSM (Integrated Dell Remote Access Controller Service Module)

iSM is a software module that enhances iDRAC functionality by providing OS-level monitoring and management.

It is installed on individual servers to facilitate communication between the OS and iDRAC.

Limitation:

Not a centralized management application.

Does not provide holistic management across multiple servers and chassis.

Conclusion: Not suitable.

Option B: OME (OpenManage Enterprise)

Dell OpenManage Enterprise is a web-based, one-to-many systems management application.

Features:

Provides comprehensive management of Dell EMC servers, storage, and networking devices.

Supports both rack servers (R660) and modular chassis (MX7000).

Offers monitoring, configuration, deployment, and update capabilities.

User-friendly dashboard for holistic infrastructure management.

Conclusion: Correct Answer.

Option C: Group Manager

Group Manager is an iDRAC feature that allows basic grouping of servers for simplified management.

Limitations:

Limited to servers of the same generation and similar configurations.

Does not support the full range of management functions required.

Not suitable for managing storage and network environments.

Conclusion: Not sufficient.

Option D: OMSA (OpenManage Server Administrator)

OMSA is a software agent that provides a comprehensive, one-to-one systems management solution.

Installed on individual servers to manage and monitor hardware components.

Limitations:

Does not provide a centralized, holistic view.

Lacks the ability to manage multiple servers and chassis collectively.

Conclusion: Not appropriate.

Dell Operate Reference

Server Management and Configuration Tools (14%)

Explain the management interface options - LCC, racadm, OMSA, iSM, OME: Understanding the capabilities and limitations of various management tools is essential for selecting the appropriate solution.

System Administration (18%)

Group management: OpenManage Enterprise facilitates group management of diverse hardware.

Conclusion

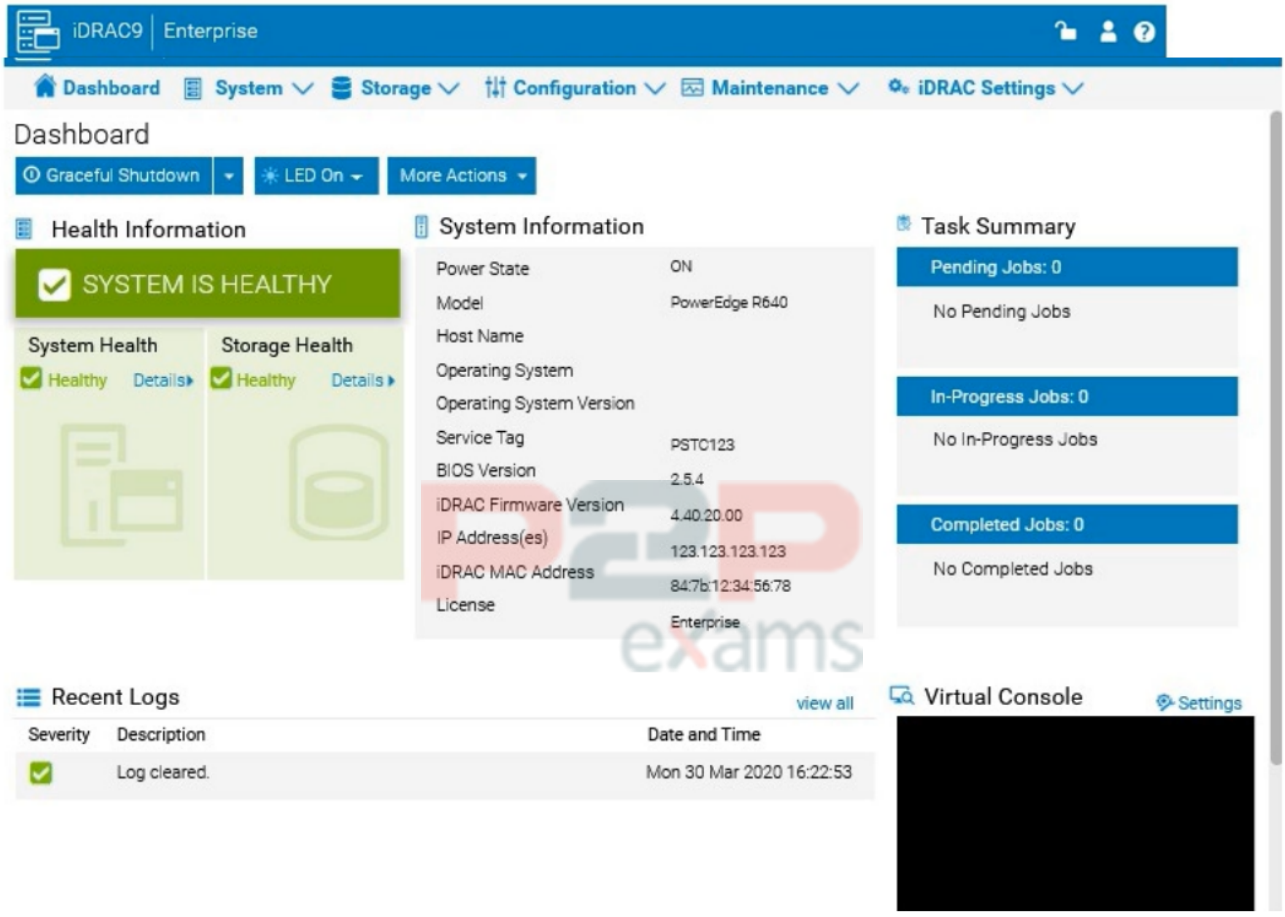
OpenManage Enterprise (OME) is the recommended solution. It provides a unified management console capable of holistically managing and monitoring the customer's storage, server, and network environment, including both rack servers and modular chassis.

# Question 9

Question Type: MultipleChoice

SIMULATION

A customer wants to change the PSU configuration to a 2+0 with PSU2 as the primary. Use the simulator to complete this task in the iDRAC UI.




## Options:

A- See the Explanation for Step by Step solution

## Answer:

A

## Explanation:

To change the Power Supply Unit (PSU) configuration to a 2+0 setup with PSU2 as the primary in the iDRAC interface, follow these steps:

Step-by-Step Guide:

Navigate to Power Management Settings:

In the iDRAC interface, go to the Configuration tab at the top.

Select Power Management from the dropdown options.

Locate the Power Configuration Section:

Within the Power Management settings, look for a section labeled Power Configuration or Power Supply Configuration.

Select the Redundancy Policy:

Change the Redundancy Policy to 2+0. In this configuration, there will be no redundancy, and both power supplies will be active but configured as independent power sources without failover.

Set PSU2 as the Primary PSU:

Locate the option to designate the Primary PSU. Select PSU2 as the primary power source.

This setting ensures that PSU2 will handle the primary power load under normal conditions.

Apply and Save Changes:

Once you have made these changes, click Apply or Save to confirm the new configuration.

The interface may prompt for confirmation, after which the settings will be saved, and PSU2 will become the primary power supply under a 2+0 configuration.

Verify Configuration:

Review the updated settings to confirm that PSU2 is now set as primary and that the redundancy policy is 2+0, meaning only PSU2 is actively providing power without a secondary backup.

By following these steps in the iDRAC simulator, you will set up PSU2 as the primary power source with no redundancy, ensuring a 2+0 configuration. This setup will leverage PSU2 exclusively without automatic failover to another power supply.