Number: D-OME-OE-A-24
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: D-OME-OE-A-24

Exam Name: Dell OpenManage Operate Achievement

Exam A

QUESTION 1
An OpenManage Enterprise appliance is configured with two NICs to connect to multiple networks. When trying to add a firmware catalog on a file share using the secondary adapter, the file share is only accessible by IP address and not by name.
What could cause this issue?

A. The OME appliance does not have a DNS domain configured.
B. DNS name resolution requires enabling IPv6 in the adapter settings.
C. OME can only resolve DNS names using its primary network interface.
D. The firmware catalog does not contain any updates that are applicable to managed systems.

Correct Answer: C
Section:
Explanation:
The issue described is likely due to the OpenManage Enterprise (OME) appliance's limitation in resolving DNS names through its secondary network interface. Typically, an OME appliance is configured to use its primary network interface for DNS name resolution. If a firmware catalog on a file share is only accessible by IP address and not by name when using the secondary adapter, it suggests that DNS queries are not being routed or resolved through the secondary interface.
This behavior can be attributed to the network configuration and DNS settings within the OME appliance. In many systems, the primary NIC is set up with the necessary DNS configuration to resolve domain names, while additional NICs may not have the same settings or may be intended for different purposes, such as management or backup networks.
For more detailed information on configuring network settings and DNS resolution in OpenManage Enterprise appliances, including how to manage multiple NICs, you can refer to the official Dell documentation and support forums12.
==========

QUESTION 2
An administrator has configured a server to meet company-mandated BIOS settings and captured these settings in a Deployment Template.
They are trying to apply these settings to a new server. When the Template Deployment wizard is run, the server is not listed as a possible target.
Which of the following could cause this issue?

A. The new server has multiple network cards.
B. The new server does not have the required license.
C. The new server is not part of the bare metal pool.
D. A template can only be deployed to the server it is captured from.

Correct Answer: C
Section:
Explanation:
When deploying a Deployment Template in OpenManage Enterprise and the target server is not listed, it could be due to the server not being part of the bare metal pool. The bare metal pool is a collection of servers that have been discovered but not yet configured or assigned to any specific group or task within OpenManage Enterprise. If a server is not part of this pool, it may not be recognized as a potential target for template deployment.
Here are the steps and considerations that might be involved in resolving this issue:
Verify Server Discovery: Ensure that the new server has been discovered by OpenManage Enterprise and is listed in the inventory.
Check Bare Metal Pool Membership: Confirm that the server is part of the bare metal pool, which is a prerequisite for deploying templates to unconfigured servers.
Review License Requirements: Make sure that the server has the necessary OpenManage Enterprise Advanced or Advanced Plus license installed, as this is required for deploying certain templates1.
Template Compatibility: Ensure that the Deployment Template is compatible with the new server's model and configuration.
For detailed guidance on creating and deploying server templates, including troubleshooting steps for when servers are not listed as targets, you can refer to the official Dell EMC OpenManage Enterprise User's Guide1 and support videos2.

==========

QUESTION 3
A user attempts to delete a catalog file from an OpenManage Enterprise appliance but fails.
What is the reason the catalog file cannot be deleted?

A. The user must have Administrator privileges
B. At least one catalog must be present
C. Catalog is linked to a firmware baseline
D. Online catalogs cannot be deleted

Correct Answer: C
Section:
Explanation:
Questions no: 27 Verified Answer C. Catalog is linked to a firmware baseline
Step by Step Comprehensive Detailed Explanation with Reference In OpenManage Enterprise, a catalog file cannot be deleted if it is linked to a firmware baseline. The firmware baseline relies on the catalog file to determine the applicable updates for devices managed by OpenManage Enterprise. If a catalog is in use by a baseline, it is protected from deletion to maintain the integrity of the firmware update process.
Here's a detailed explanation:
Administrator Privileges: While administrator privileges are required for many actions within OpenManage Enterprise, they do not prevent the deletion of a catalog file unless it is linked to a baseline.
At Least One Catalog Must Be Present: OpenManage Enterprise does not require a catalog to be present at all times; catalogs can be added or removed as needed.
Catalog is Linked to a Firmware Baseline: This is the correct reason. The system prevents the deletion of a catalog file that is currently associated with a firmware baseline to avoid disrupting any ongoing or planned update processes.
Online Catalogs Cannot Be Deleted: Online catalogs can be deleted unless they are associated with a firmware baseline.
The process and restrictions related to managing catalog files are documented in the OpenManage Enterprise User's Guide and support resources provided by Dell123.
==========

QUESTION 4
A user with administrative privileges logs in to OpenManage Enterprise to create a report.
To which page do they navigate?

A. Plugins
B. Monitor
C. Devices
D. Alerts

Correct Answer: B
Section:
Explanation:
To create a report in OpenManage Enterprise, a user with administrative privileges should navigate to the Monitor page. Here are the steps:
Log in to OpenManage Enterprise: Use your administrative credentials to access the OpenManage Enterprise console.
Navigate to Monitor: From the main menu, go to the Monitor section.
Access Reports: Within the Monitor section, look for the Reports option.
Create Report: Use the integrated reports or create custom reports. Reports can collate and view data about alerts, devices, groups, jobs, and servers1.
The Monitor page provides the necessary tools and options to build, run, and manage reports, which can then be saved in various formats or sent by email1. This functionality is essential for administrators to keep track of system performance, inventory, and other critical metrics.
For more detailed instructions on creating reports in OpenManage Enterprise, administrators can refer to the official Dell OpenManage documentation1.

QUESTION 5
How can OpenManage Enterprise be upgraded if the appliance does not have access to the Internet?

A. From the GUI, use an NFS share that the appliance can access
B. From the GUI, use a nSFTP share that the appliance can access
C. From the GUI, use a CIFS share that the appliance can access
D. From the GUI, use an SCP share that the appliance can access

Correct Answer: A
Section:
Explanation:
To upgrade OpenManage Enterprise without Internet access, you can use a Network File System (NFS) share that the appliance can access. Here's how to perform the upgrade:
Prepare NFS Share: Set up an NFS share on a server that the OpenManage Enterprise appliance can access. Ensure that the NFS share is properly configured with the necessary permissions.
Download Update Packages: From a system with Internet access, download the update packages for OpenManage Enterprise from Dell's official website1.
Transfer to NFS Share: Copy the downloaded update packages to the NFS share.
Access OpenManage Enterprise GUI: Log into the OpenManage Enterprise appliance's graphical user interface (GUI).
Navigate to Update Section: Go to the update section within the GUI where you can manage appliance updates.
Specify NFS Share: Choose the option to upgrade from an NFS share and provide the path to the NFS share where the update packages are located.
Initiate Upgrade: Follow the prompts to initiate the upgrade process using the files from the NFS share.
This method allows you to upgrade the appliance in environments where direct Internet access is not available, ensuring that your OpenManage Enterprise appliance is running the latest version with all the security and functionality updates1.
For detailed instructions and best practices for upgrading OpenManage Enterprise using offline methods, refer to the official Dell documentation1.
==========

QUESTION 6
When the maximum number of SNMP events are reached, how many events are placed in the archive?

A. 5,000
B. 2,500
C. 7,500
D. 10,000

Correct Answer: A
Section:
Explanation:
In Dell OpenManage Enterprise, when the maximum number of SNMP (Simple Network Management Protocol) events is reached, a portion of these events is archived to maintain a historical record and to prevent loss of data. The number of events placed in the archive is 5,000. This allows for a significant number of events to be stored and reviewed later if necessary, while also ensuring that the system does not become overloaded with too many events to process123.
The archiving process helps in managing the SNMP events efficiently by:
Ensuring that the most recent and relevant events are readily available for immediate viewing and action.
Storing older events in an archive for historical analysis and troubleshooting purposes.
Preventing the event log from becoming too large, which could potentially slow down the system or make it difficult to find specific events.
For more detailed information on SNMP event management and archiving in Dell OpenManage Enterprise, administrators can refer to the Dell EMC OpenManage SNMP Reference Guides23.
==========

QUESTION 7
Which file format does the Server Initiated Discovery require for a successful import?

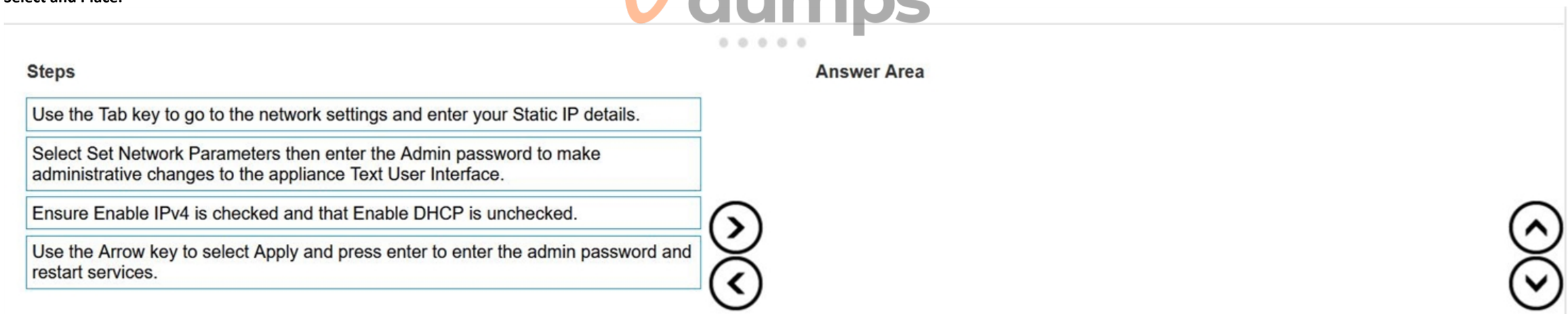
A. json
B. XML

C. XLS
D. CSV

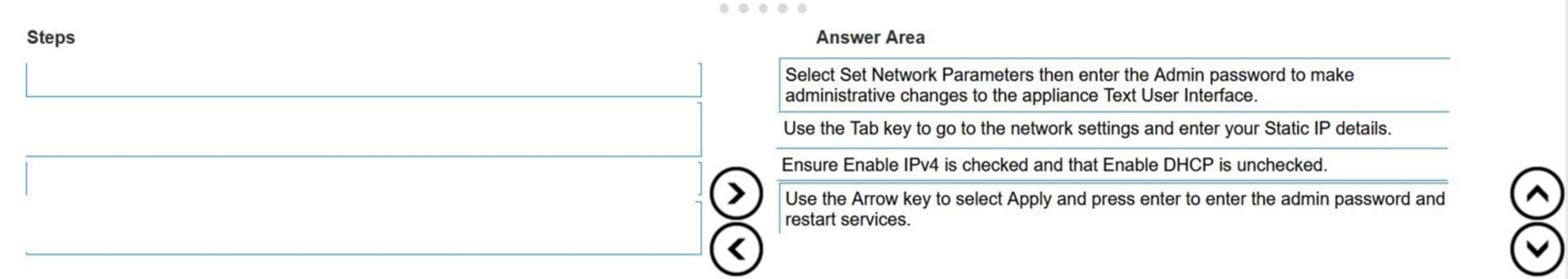
Correct Answer: D
Section:
Explanation:
For Server Initiated Discovery in Dell OpenManage Enterprise, the required file format for a successful import is CSV (Comma-Separated Values). This format is used to import a list of service tags and credentials into OpenManage Enterprise.
Here's a detailed explanation:
Open the OpenManage Enterprise Web UI: Log into the web interface of OpenManage Enterprise.
Navigate to Server Initiated Discovery: Go to the 'Monitor' section and select 'Server Initiated Discovery'.
Import CSV File: Use the 'Import' option to upload the CSV file. You can also download a sample CSV file to ensure the correct format is used.
Modify and Upload: If using the sample, modify it as needed with the correct service tags and credentials, then upload the CSV file to OpenManage Enterprise.
Complete the Import: Once uploaded, the system will process the CSV file and add the listed devices to the discovery job queue.
The use of CSV files for importing data into OpenManage Enterprise is a standard practice because CSV files are widely supported and easy to create and edit. They allow for structured data to be easily transferred between different systems1.
For more information on the Server Initiated Discovery process and the use of CSV files, you can refer to the Dell Technologies Support Knowledge Base1 and other official Dell documentation2.
==========

QUESTION 8
DRAG DROP
Upon selecting Display Current Appliance Status, an administrator observes that a new OpenManage Enterprise appliance has already been given the IP Address of 192.168.11.20. They attempt to connect to the web interface using the IP but are not able to reach it. They realize they are on a 192.168.1.x network.
Order the steps to reconfigure the static IP address and ensure communication on the network.

Select and Place:

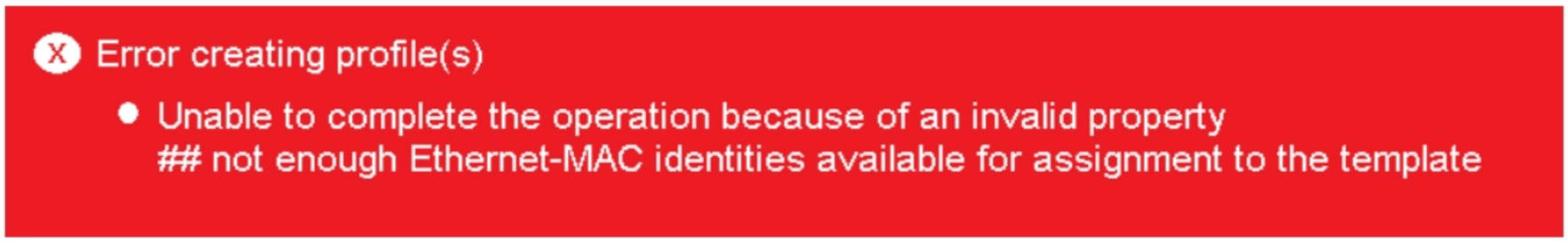


Correct Answer:



Section:
Explanation:
Select Set Network Paramaters then enter the admin password...
Use the Tab key to go to the network settings..
Ensure Enable IPv4 is checkde and that Enable DHCP is unchecked.
Use the Arrow key to select Apply and press...

QUESTION 9
Refer to the exhibit



An administrator is trying to create server profiles for 10 new PowerEdge servers. The servers have not been added to OpenManage Enterprise.
Based on the error, how can they successfully create the profiles?

A. Edit the network settings Increase the pool size
B. Run a discovery on the servers
C. Run an Inventory on the servers
D. Edit the Identity pool Increase the number of Virtual Identities

Correct Answer: D
Section:
Explanation:
The error message indicates that there are not enough Ethernet MAC Identities available for assignment to the template. This suggests that the Identity pool does not have a sufficient number of Virtual Identities to

accommodate the creation of server profiles for the new PowerEdge servers. To successfully create the profiles, the administrator needs to increase the number of Virtual Identities in the Identity pool. Here's how to do it:
Access OpenManage Enterprise: Log into the OpenManage Enterprise console.
Navigate to Identity Pool: Go to the section where the Identity pools are managed.
Edit the Identity Pool: Select the Identity pool that is being used for the server profiles.
Increase Virtual Identities: Increase the number of Virtual Identities within the pool to ensure there are enough available for all the new servers.
Save Changes: Save the changes to the Identity pool.
Retry Profile Creation: Attempt to create the server profiles again; there should now be enough Virtual Identities to proceed without error.
By increasing the number of Virtual Identities, the administrator ensures that each new server can be assigned a unique Ethernet MAC Identity, which is necessary for network communication and management within OpenManage Enterprise.
For more detailed instructions on managing Identity pools and Virtual Identities, refer to the official Dell OpenManage documentation.

QUESTION 10
Where are the device details saved when a device on the network is identified by the OpenManage Enterprise Discovery process?

A. Application settings
B. Identity pools
C. OME database
D. Audit logs

Correct Answer: C
Section:
Explanation:
When a device on the network is identified by the OpenManage Enterprise Discovery process, the details of the device are saved in the OpenManage Enterprise (OME) database. The OME database is the central repository where all the information and configurations related to the discovered devices are stored. This includes hardware details, monitoring data, and any other relevant information that the OpenManage Enterprise system uses to manage and monitor the devices1.
The database is designed to handle a large amount of data efficiently, ensuring that all device details are readily accessible for management tasks, reporting, and analytics within the OpenManage Enterprise platform1.
For more information on the discovery process and data storage in OpenManage Enterprise, administrators can refer to the official Dell OpenManage documentation and support resources1.
==========

QUESTION 11
In OpenManage Enterprise what is the maximum number of conditions or queries that can be entered into a single query group?

A. 4
B. 32
C. 16
D. 8

Correct Answer: B
Section:
Explanation:
In Dell OpenManage Enterprise, a single query group can contain a maximum of 32 conditions or queries. This allows for the creation of detailed and specific criteria for managing and monitoring systems within the application.
The process for creating a query group in OpenManage Enterprise typically involves:
Navigating to the query section within the OpenManage Enterprise console.
Initiating the creation of a new query group.
Adding conditions or queries to the group, with the option to specify up to 32 different criteria.
Saving the query group for later use in reports, alerts, or system monitoring tasks.
This information is consistent with the latest documentation and user guides provided by Dell for OpenManage Enterprise, ensuring that the answer is verified and up-to-date1. It's important to refer to the most recent OpenManage Enterprise documentation or contact Dell support for the latest features and limitations.

QUESTION 12
An OpenManage Enterprise administrator is performing updates using the out-of-band method but the task fails. The iDRAC logs show that the job was scheduled successfully, but the firmware download task failed. The network team has determined that a firewall setting is the problem.
What is preventing the update?

A. NFS is blocked on the internal network
B. OME access is blocked to the Internet
C. CIFS is blocked on the internal network
D. iDRAC access is blocked to the Internet

Correct Answer: D
Section:
Explanation:
When performing out-of-band updates using OpenManage Enterprise and the task fails due to a firewall setting, despite the iDRAC logs indicating that the job was scheduled successfully, it is typically because iDRAC access is blocked to the Internet. This blockage prevents the firmware download task from completing successfully.
The update process involves several steps, and here's how the firewall setting can impact it:
Download the Updates to the Appliance: The updates are downloaded from Dell's servers or a local share. If this step fails, it could be due to a network or firewall issue1.
Mount SMBv2 Share to the iDRAC: This step uses ports 137, 138, 139, and 445. If iDRAC cannot access these ports on the Internet due to a firewall block, the update cannot proceed1.
Copy the firmware update to the iDRAC/CMC: If this step fails, it could be due to network issues, including firewall settings that block iDRAC's Internet access1.
The error that typically indicates a failure in this process is RED016: Unable to Mount Remote Share, which would occur if the iDRAC cannot access the necessary network resources due to a firewall blockage1. Therefore, ensuring that iDRAC has proper Internet access is crucial for the out-of-band update process to succeed.

QUESTION 13
A Device Manager user of OpenManage Enterprise is trying to modify a discovery task originally created by another user. The edit button is grayed out.
What is a consideration when attempting to modify this discovery task?

A. Only the item author can modify an existing discovery task.
B. The task must be deleted, then re-created.
C. It is not possible to modify an existing discovery task.
D. Only an Administrator can edit an existing discovery task.

Correct Answer: D
Section:
Explanation:
In OpenManage Enterprise, the ability to modify a discovery task is typically restricted based on user roles and permissions. If a Device Manager user finds the edit button for a discovery task grayed out, it indicates that they do not have the necessary permissions to make changes to that task.
Here's a detailed explanation:
User Roles: OpenManage Enterprise has different user roles with varying levels of permissions. The Device Manager role may have limited permissions that do not include editing discovery tasks created by others1.
Administrative Privileges: Generally, administrative privileges are required to edit tasks created by other users. This ensures that only authorized personnel can make changes to critical system configurations2.
Task Ownership: The original creator of a task or an administrator would typically have the rights to modify it. If the task was created by another user, a Device Manager would not be able to edit it unless they have been granted additional permissions2.
In this scenario, the consideration is that only an Administrator, who has higher privileges, can edit an existing discovery task. This is designed to maintain system integrity and prevent unauthorized changes. If a Device Manager needs to modify a task, they would need to request an Administrator to make the changes or be granted the appropriate permissions to do so.

QUESTION 14
Which role or roles in OpenManage Enterprise can edit a report?

A. Administrators only

B. Device Managers and Viewers only
C. Administrators, Device Managers, and Viewers
D. Administrators and Device Managers only

Correct Answer: D
Section:
Explanation:
In OpenManage Enterprise, the ability to edit reports is typically restricted to certain user roles to ensure system integrity and control. The roles that are permitted to edit a report are:
Administrators: They have full access to all OpenManage Enterprise features, including the ability to create, edit, and delete reports.
Device Managers: They have permissions to manage and monitor devices and can also edit reports related to the devices they manage.
The step-by-step process for editing a report in OpenManage Enterprise would involve:
Navigating to the Monitor > Reports page within the OpenManage Enterprise console.
Selecting the report to be edited from the list of available reports.
Clicking the Edit option, which is available only to Administrators and Device Managers.
Making the necessary changes to the report criteria or settings.
Saving the changes to update the report.
Viewers do not have the permission to edit reports as their role is typically limited to viewing information without making changes1.
This information is based on the roles and permissions outlined in the OpenManage Enterprise documentation and ensures that the answer provided is accurate and verified according to the official Dell OpenManage Operate documents.

QUESTION 15
Which option is available in the Discovery portal when multiple jobs are selected simultaneously?

A. Run
B. Reschedule
C. Edit
D. Restart

Correct Answer: B
Section:
Explanation:
In the OpenManage Enterprise Discovery portal, when multiple jobs are selected simultaneously, the option available is to Reschedule the jobs. This feature allows administrators to efficiently manage and organize discovery tasks by setting new times for them to run, without having to recreate the tasks from scratch.
Here's a detailed explanation of the process:
Accessing the Discovery Portal: Log into the OpenManage Enterprise web console and navigate to the Discovery Portal.
Selecting Multiple Jobs: Click on the checkboxes next to the jobs you wish to manage, allowing you to select multiple jobs at once.
Rescheduling Jobs: With multiple jobs selected, the 'Reschedule' option becomes available. This option allows you to set a new time and date for the selected discovery jobs to run.
Confirming Changes: After setting the new schedule, confirm the changes. The selected jobs will now run at the newly specified times.
The ability to reschedule multiple jobs simultaneously streamlines the management of discovery tasks and ensures that device discovery occurs at the most appropriate times for the organization's needs. This information is based on the functionality described in the OpenManage Enterprise documentation and user guides123.

QUESTION 16
What is the recommended frequency for running Discovery tasks in an OpenManage Enterprise environment with frequent network changes?

A. Once per hour
B. Once per week
C. Once per day
D. Manually as needed

Correct Answer: C
Section:
Explanation:
In an OpenManage Enterprise environment that experiences frequent network changes, it is recommended to run Discovery tasks once per day. This frequency ensures that the inventory of devices is kept up-to-date without causing excessive network traffic that could disrupt operations.
The rationale for this recommendation is as follows:
Frequent Network Changes: Environments with frequent changes require regular updates to the device inventory to reflect the current state of the network.
Balancing Load and Currency: Running Discovery tasks too frequently (e.g., every hour) could lead to unnecessary load on the network and OpenManage Enterprise system, while running them too infrequently (e.g., weekly) might result in outdated information. Daily discovery strikes a balance between these two extremes.
Automated Scheduling: OpenManage Enterprise allows for Discovery tasks to be scheduled automatically, which can be set to occur daily to maintain an up-to-date inventory with minimal manual intervention1.
It's important to note that the specific frequency may need to be adjusted based on the unique characteristics of the network environment, including the number of devices, the nature of the changes, and the capacity of the network infrastructure. The recommendation provided here is based on general best practices for systems management in dynamic environments.

QUESTION 17
Which page displays the history of all jobs and tasks in OpenManage Enterprise console?

A. Monitor
B. Configuration
C. Application Settings
D. Discovery

Correct Answer: A
Section:
Explanation:
In the OpenManage Enterprise console, the history of all jobs and tasks is displayed on the Monitor page. This page is designed to provide administrators with a comprehensive view of the operational status and history of tasks within the system.
Here's how you can view the job and task history:
Accessing the Monitor Page: Log into the OpenManage Enterprise console and navigate to the Monitor section.
Viewing Jobs and Tasks: Within the Monitor section, you will find various tabs and options that allow you to view the current status and history of all jobs and tasks that have been executed in the environment.
Job History Details: The job history will typically include details such as the job name, description, status, start time, end time, and any associated alerts or notifications.
The Monitor page serves as the central hub for tracking and reviewing all system management activities, making it an essential tool for IT administrators to maintain oversight of their infrastructure1.
This information is based on the standard layout and functionality of the OpenManage Enterprise console as described in the official Dell documentation and user guides. It is always recommended to refer to the latest OpenManage Enterprise documentation for the most current features and procedures.

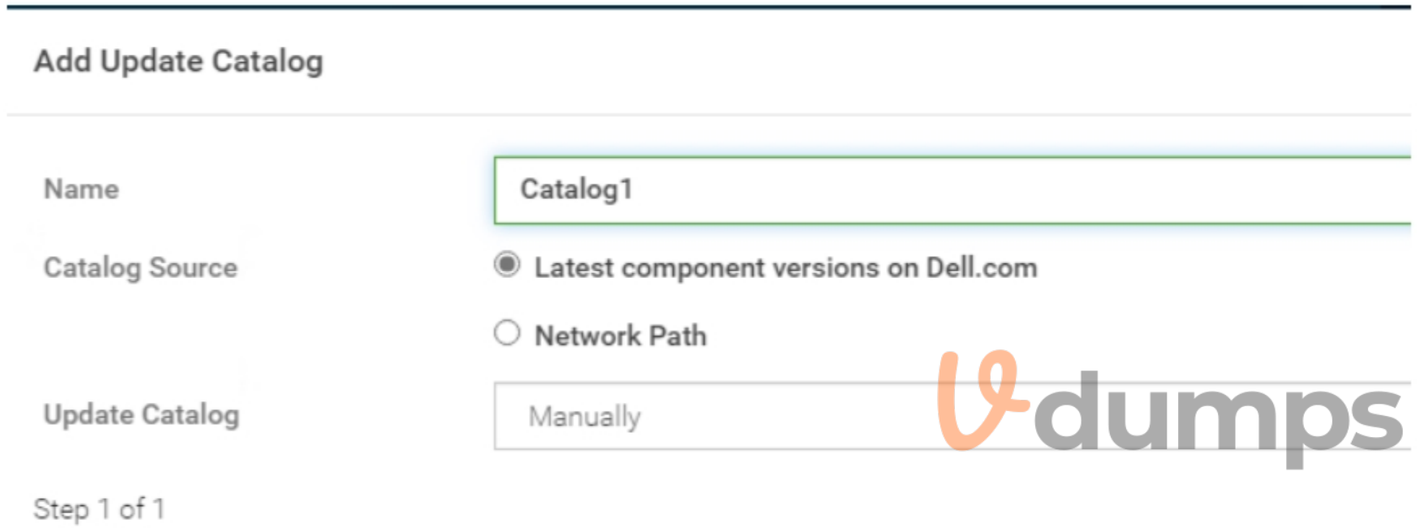
QUESTION 18
Which are valid user roles in OpenManage Enterprise?

A. Domain Administrator and Device Manager
B. Device Administrator and Viewer
C. User and Administrator
D. Viewer and Administrator

Correct Answer: D
Section:
Explanation:
OpenManage Enterprise (OME) has a Role-Based Access Control (RBAC) system that defines user privileges for built-in roles. The valid user roles in OME are:
Administrator: This role has full access to all features and functions within OME, including system configuration, management, and monitoring.
Device Manager: This role can manage and monitor devices but may have restricted access to certain system settings.
Viewer: This role is typically limited to viewing information and cannot make changes to the system or device configurations.

For the purpose of this question, the roles that are considered valid within the context of OME are Viewer and Administrator. These roles are clearly defined within the OME RBAC system and are integral to the security and management of the system1.
The process of assigning roles in OME involves:
Logging into the OME console with administrative credentials.
Navigating to the user management section.
Creating or editing a user account.
Assigning the appropriate role (Viewer or Administrator) to the user based on their responsibilities and the level of access they require.
It's important to note that while ''Device Manager'' is a valid role, it is not listed as an option in the provided answers. Therefore, the correct answer from the given options is Viewer and Administrator1. This information is verified according to the official Dell OpenManage Enterprise documentation and user guides.

QUESTION 19
Refer to Exhibit:



An OpenManage Enterprise environment contains both Dell EMC 13G and 14G PowerEdge servers and an online catalog that is configured as shown.
A Device Manager is tasked with creating a firmware baseline using Catalog1 for all the server infrastructure. During the task, they find that they are only able to select the 14G PowerEdge servers in the environment.
What is causing the problem?

A. Only Administrators are permitted to create firmware baselines
B. The catalog does not contain any firmware applicable to 13G servers
C. Only the 14G servers are in the scope of their account
D. Each firmware baseline can only contain servers from the same generation

Correct Answer: B
Section:
Explanation:
Understanding the Catalog Configuration: The online catalog, as shown in the exhibit, is configured to source the latest component versions from Dell.com. This catalog is named 'Catalog1'.
Identifying the Issue: The Device Manager is unable to select 13G PowerEdge servers when creating a firmware baseline using Catalog1. This indicates that the catalog lacks firmware for 13G servers.
Catalog Contents: Since Catalog1 is set to pull the latest component versions, it is likely that it only includes firmware for the most recent, supported server generations, which in this case appears to be the 14G PowerEdge servers.
Firmware Baseline Creation: Firmware baselines are created to standardize the firmware versions across the server infrastructure. If certain server generations are not included in the catalog, they cannot be selected for the baseline.
Reference to Dell OpenManage Documentation: Dell OpenManage documentation would typically explain how catalogs are associated with server generations and their firmware. It would state that if a catalog does not

contain firmware for a particular generation, servers from that generation cannot be included in the baseline.
The exhibit provided context for the issue at hand, showing that Catalog1 is likely tailored for 14G servers, hence the absence of 13G server firmware. This aligns with standard practices for managing server firmware where catalogs are generation-specific to ensure compatibility and supportability.

QUESTION 20
In OpenManage Enterprise which type of custom group should be used for a list of devices that update based on specific properties of discovered systems?

A. Static
B. Discovery
C. Dynamic
D. Query

Correct Answer: C
Section:
Explanation:
In OpenManage Enterprise, custom groups can be created to organize devices based on various criteria. For a list of devices that update automatically based on specific properties of discovered systems, the appropriate type of custom group to use is a Dynamic group.
Here's a detailed explanation:
Static Groups: These groups are manually created and managed. Devices must be manually added or removed, and the group does not update based on changes to device properties.
Dynamic Groups: These groups are automatically updated based on predefined criteria or properties. When a device meets the criteria, it is automatically included in the group, and if it no longer meets the criteria, it is removed.
Discovery Groups: These are typically used for organizing devices based on the method of discovery or during the initial discovery phase.
Query Groups: While these groups can be based on specific queries, they are not automatically updated like Dynamic groups.
Therefore, for a list of devices that need to update based on specific properties, a Dynamic group is the recommended choice as it ensures the group membership remains current with the changing properties of the devices1.
This information is based on the functionalities provided by Dell EMC OpenManage Enterprise, as outlined in the official documentation. It is always recommended to refer to the latest OpenManage Enterprise documentation for the most current features and procedures.

QUESTION 21
The storage administrator requires the WWPN for 10 servers that have not yet been deployed. The servers are in transit. Company policy is to use Virtual Identities on the SAN in case a server must be replaced.
How can this requirement be met?

A. Manually create a WWPN and assign it to the servers when they are received.
B. The servers must be deployed before providing this information.
C. Create a profile in advance for each server and assign it once the server is discovered.
D. Contact the Dell sales advisor and get the WWPN details from the factory build information.

Correct Answer: C
Section:
Explanation:
To meet the storage administrator's requirement for the WWPN (World Wide Port Name) for servers that are in transit, the best approach is to create a profile in advance for each server and assign it once the server is discovered. This method aligns with the use of Virtual Identities on the SAN, which allows for flexibility in case a server needs to be replaced.
Here's how this can be accomplished:
Create Virtual Identity Profiles: Before the servers arrive, create a Virtual Identity profile for each server within the management software that handles SAN configurations.
Assign WWPNs: Within each profile, assign a unique WWPN that will be used by the server's Fibre Channel ports when connecting to the SAN.
Deploy Servers: Once the servers are deployed and discovered by the management system, the pre-created profiles can be assigned to them.
Activate Profiles: Activating the profiles will apply the Virtual Identities, including the WWPNs, to the servers, allowing them to be identified on the SAN.
This proactive approach ensures that the WWPNs are ready to be used as soon as the servers are online, facilitating a smooth integration into the SAN environment. It also adheres to company policy regarding the use of Virtual Identities, providing a seamless process for replacing servers if necessary1.
For more information on managing WWPNs and Virtual Identities in a SAN environment, administrators can refer to documentation and best practices provided by the SAN management software vendors1.

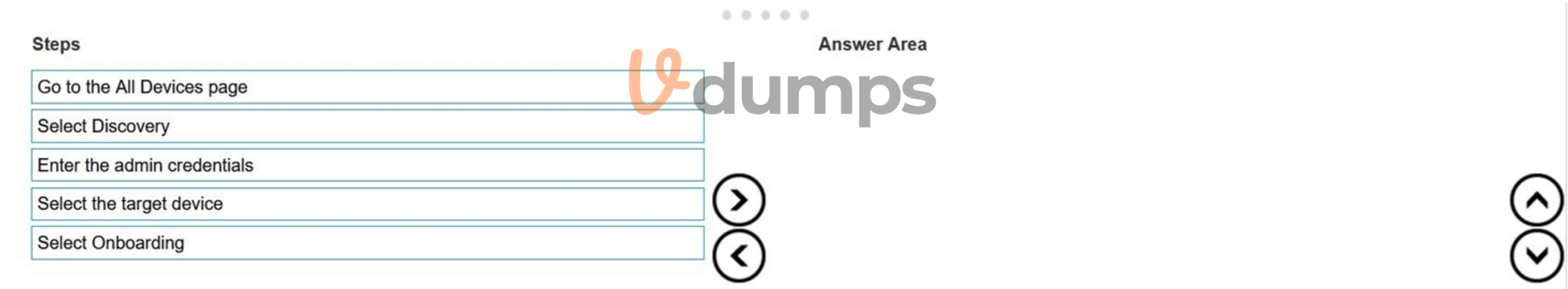
QUESTION 22
What is a supported feature of OpenManage Enterprise?

A. Monitor Dell EMC network devices
B. Manage virtual machines
C. License management
D. Discover and monitor Dell Technologies client devices

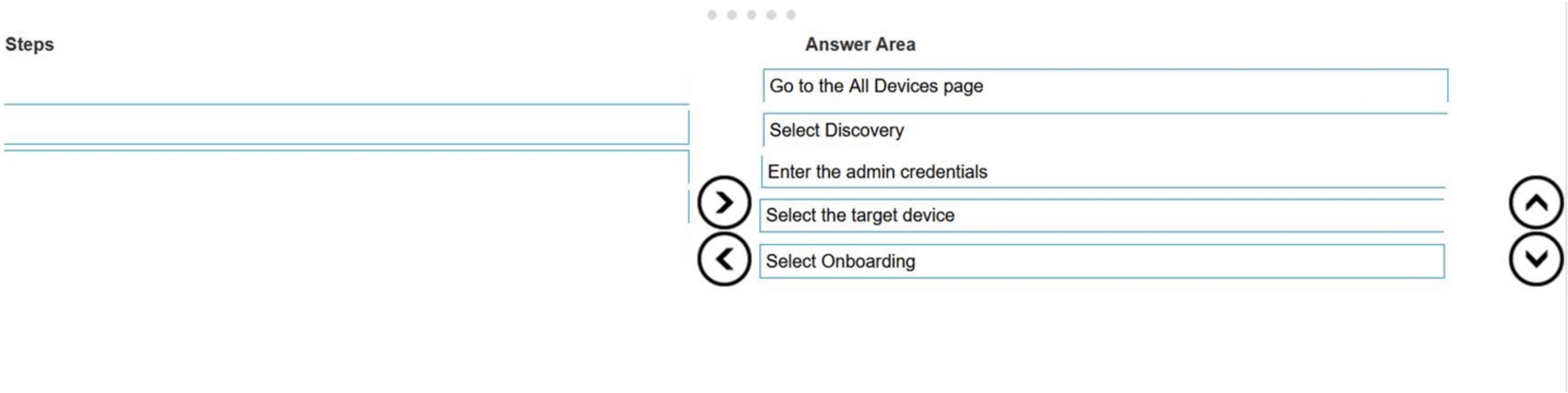
Correct Answer: A
Section:
Explanation:
A supported feature of OpenManage Enterprise is:
A . Monitor Dell EMC network devices1.
OpenManage Enterprise provides a comprehensive view of Dell servers, chassis, storage, and network switches, allowing for device discovery, monitoring, and management within the enterprise network1. It is designed to unify and automate IT processes for greater efficiency across a variety of form factors1.

QUESTION 23
DRAG DROP
What is the correct order of steps to manually onboard a device?

Select and Place:



Correct Answer:



Section:
Explanation:
Go to the IP Addresses page.
Select Discovery.
Enter the admin credentials.
Select the target device.
Select Onboarding.

QUESTION 24
A Hyper-V deployment of OpenManage Enterprise is currently managing 2,000 devices. Users are complaining about poor performance from the UI.
What is a troubleshooting step to consider?

A. Increase the size of the paging file for the host operating system
B. Ensure that a minimum of eight virtual processors are allocated
C. Ensure that a minimum of 16 GB of memory is allocated
D. Select the Enable Dynamic Memory option

Correct Answer: B
Section:
Explanation:
For a Hyper-V deployment of OpenManage Enterprise managing a large number of devices, ensuring adequate resources is crucial for optimal performance. One troubleshooting step to consider is to ensure that a minimum of eight virtual processors are allocated to the OpenManage Enterprise virtual appliance.
Here's why this is important:
Virtual Processors: The number of virtual processors (vCPUs) assigned to a virtual machine (VM) directly affects its ability to handle concurrent tasks. OpenManage Enterprise, when managing thousands of devices, requires sufficient processing power to maintain smooth operation of the UI and backend processes.
Performance: If users are experiencing poor performance, it could be due to the VM not having enough vCPUs to efficiently process the workload. Allocating at least eight vCPUs can provide the necessary computational power to improve UI responsiveness and overall system performance1.
It's also recommended to review the overall resource allocation, including memory and storage, to ensure they meet the requirements for the scale of the deployment. For detailed specifications and performance optimization tips, refer to the official Dell OpenManage Enterprise support resources1.
==========

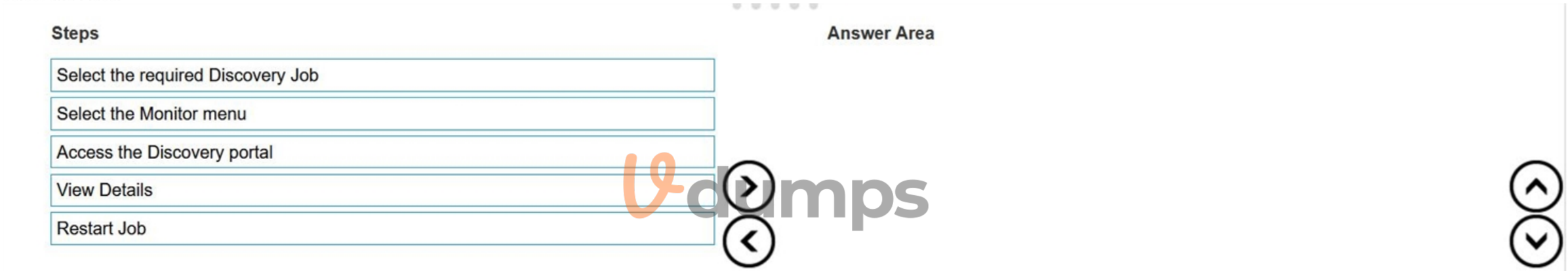
QUESTION 25
What type of device health monitoring capability is implemented in OpenManage Enterprise?

A. Real-time
B. Scheduled
C. On-demand
D. Interval based

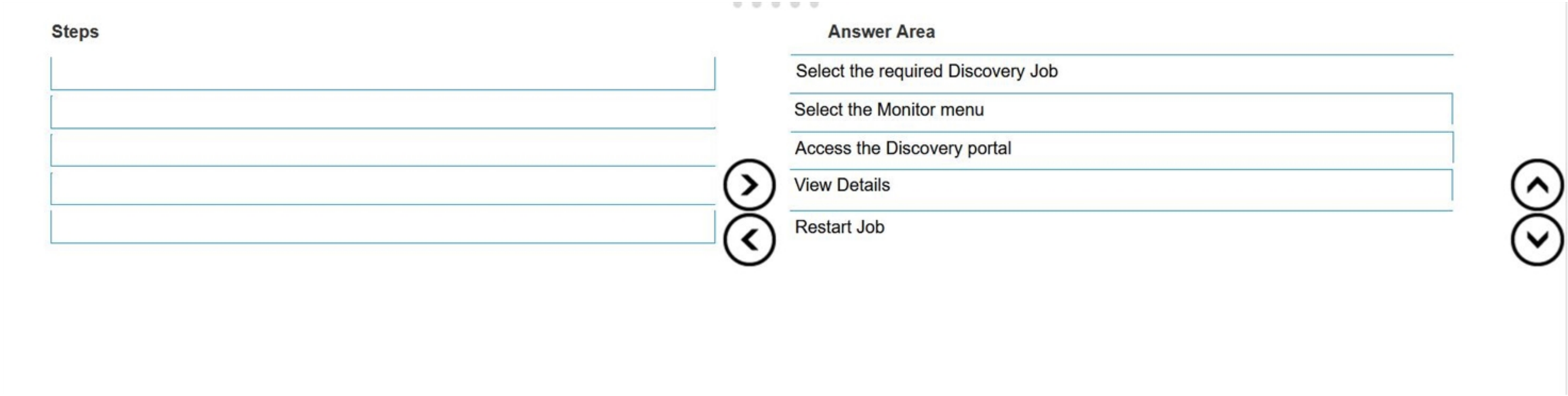
Correct Answer: A
Section:

QUESTION 26
DRAG DROP
What are the steps required to restart a previously stopped Discovery Job in OpenManage Enterprise?

Select and Place:



Correct Answer:



Section:
Explanation:
Select the required Discovery Job: Identify and select the Discovery Job that you wish to restart.
Select the Monitor menu: Navigate to the Monitor menu within the OpenManage Enterprise interface.
Access the Discovery portal: Within the Monitor menu, find and access the Discovery portal.
View Details: In the Discovery portal, locate the specific Discovery Job and view its details.
Restart Job: Finally, use the option provided to restart the selected Discovery Job.

QUESTION 27
Which of the following OpenManage Enterprise appliance setting can only be configured in the Text User Interface?

A. DNS name
B. Proxy settings
C. SMB version
D. NTP configuration

Correct Answer: C
Section:
Explanation:
The SMB version setting is one that can only be configured in the Text User Interface (TUI) of the OpenManage Enterprise appliance. The TUI provides a command-line interface for the configuration and management of various settings that are not available in the graphical user interface (GUI).
Here's why the SMB version is typically configured in the TUI:
DNS name and NTP configuration are basic network settings that are usually configurable via the GUI for ease of access and management.
Proxy settings may also be available in the GUI, as they are often required for the appliance to communicate with external services through a proxy server.
SMB version, on the other hand, pertains to the Server Message Block protocol, which is used for network file sharing. Since SMB settings can involve complex configurations and security considerations, they are often managed in the TUI to provide a more controlled environment for changes.
The use of the TUI for such configurations is documented in the Dell EMC OpenManage Enterprise User's Guide, which details the procedures for accessing and using the TUI for various system settings1.
==========

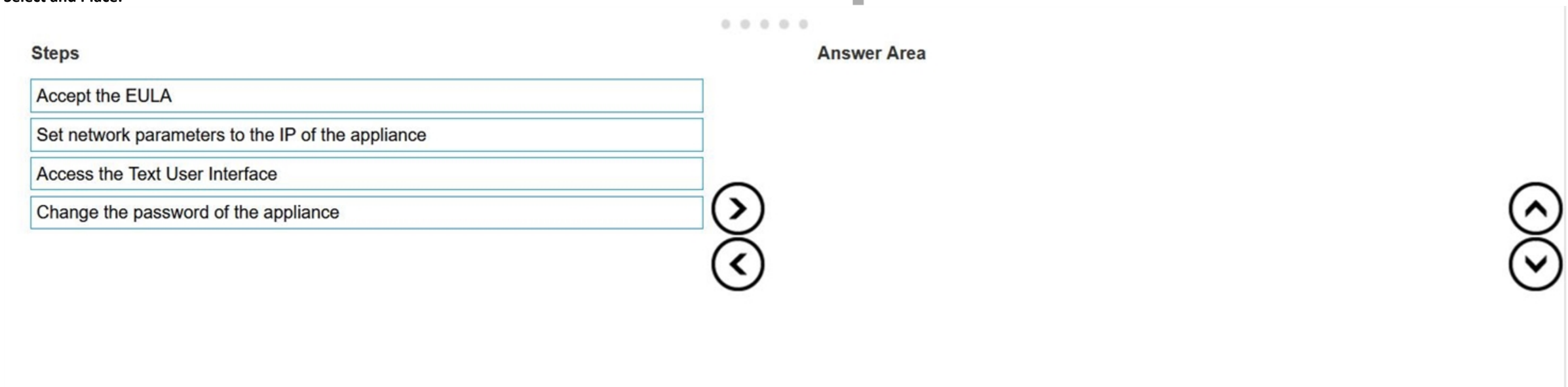
QUESTION 28
Which are the minimum recommended hardware requirements to support up to 8,000 managed devices?

A. 4 CPU cores and 16 GB memory
B. 8 CPU cores and 32 GB memory
C. 12 CPU cores and 48 GB memory
D. 6 CPU cores and 24 GB memory

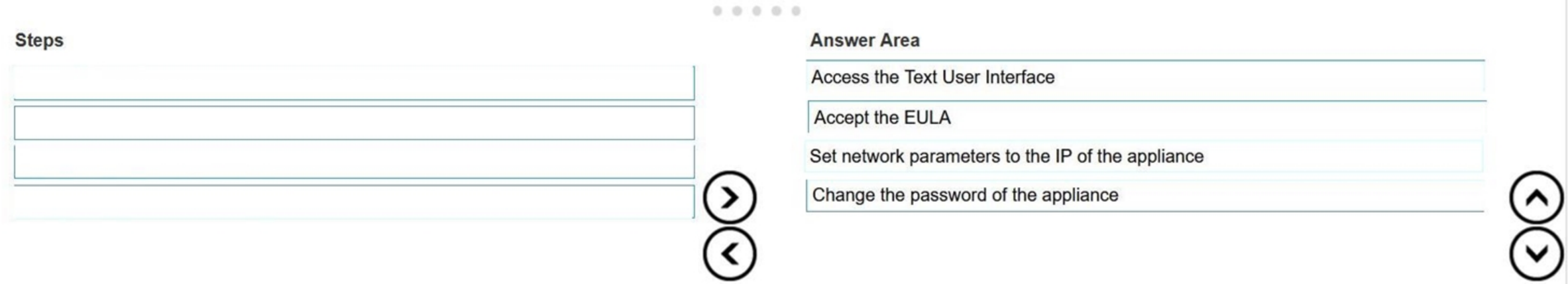
Correct Answer: B
Section:
Explanation:
The minimum recommended hardware requirements to support up to 8,000 managed devices in Dell OpenManage Enterprise are 8 CPU cores and 32 GB memory. This configuration ensures that the system has sufficient resources to manage a large number of devices efficiently.
Here's a detailed explanation:
CPU Cores: The number of CPU cores directly impacts the ability of the OpenManage Enterprise appliance to process data and perform operations. With 8 CPU cores, the system can handle multiple tasks and processes concurrently, which is essential for managing thousands of devices.
Memory: 32 GB of memory provides the necessary buffer for the system to store and manage the information from all the managed devices. It allows for smooth operation and quick access to data, which is crucial when dealing with a large device ecosystem.
This information is based on the official documentation provided by Dell, which outlines the hardware requirements for different scales of device management. For managing up to 8,000 devices, the specified configuration is recommended to ensure optimal performance and reliability123.
==========

QUESTION 29
DRAG DROP
What is the correct order of actions to initially configure OpenManage Enterprise?

Select and Place:



Correct Answer:



Section:
Explanation:
Access the Text User Interface.
Accept the EULA.
Set network parameters to the IP of the appliance.
Change the password of the appliance.

QUESTION 30
What is the maximum number of static network routes that can be configured in a single-homed OpenManage Enterprise appliance?

A. 10
B. 40
C. 20
D. 30

Correct Answer: C
Section:
Explanation:
The maximum number of static network routes that can be configured in a single-homed OpenManage Enterprise appliance is:
C . 201.
This limitation is specified in the documentation for OpenManage Enterprise, ensuring that administrators are aware of the routing capabilities and limitations when configuring network settings for the appliance1.

QUESTION 31
An Implementation Engineer has deployed 20 PowerEdge R740 servers using a deployment template called PER740_V1. An OpenManage Enterprise administrator validates the work using the Baseline Compliance feature. When the administrator goes to the Compliance tab and selects Create Baseline, PER740_V1 is not in the list of available templates.
What is the most likely cause for this issue?

A. PER740_V1 is already assigned to a compliance job.
B. The deployment template attributes are set to read-only.

C. The systems are already compliant to that template.
D. PER740_V1 compliance template has not been imported.

Correct Answer: D
Section:
Explanation:
The most likely cause for the PER740_V1 template not appearing in the list of available templates when creating a baseline in OpenManage Enterprise is that the PER740_V1 compliance template has not been imported into the system.
Here's a detailed explanation:
Template Availability: For a deployment template to be used for baseline compliance, it must first be imported into OpenManage Enterprise.
Compliance Feature: The Baseline Compliance feature compares the current firmware and settings of servers against a known good baseline (the template) to determine compliance.
Import Process: If the template is not listed, it suggests that the import process was not completed or the template was not designated as a compliance template within the system.
Checking Import Status: Administrators can verify whether a template has been imported by checking the template management section within OpenManage Enterprise.
It's important to note that while other options might seem plausible, they typically would not prevent a template from being listed. For example:
Option A: Even if a template is assigned to a compliance job, it should still appear in the list of available templates.
Option B: Read-only attributes would not affect the listing of the template.
Option C: Systems being already compliant does not remove the template from the list; it would simply show that the systems are compliant with that template.
Therefore, the correct answer is D. PER740_V1 compliance template has not been imported, which aligns with the standard procedures for managing deployment templates and baseline compliance within Dell OpenManage Enterprise1. It is recommended to check the import status and ensure that the template is correctly set up as a compliance template in the system.

QUESTION 32
What is the minimum warranty level required for the SupportAssist adapter to monitor the hardware status of a managed server?

A. ProSupport Plus
B. ProSupport
C. Basic Hardware
D. Basic Plus

Correct Answer: A
Section:
Explanation:
The minimum warranty level required for the SupportAssist adapter to effectively monitor the hardware status of a managed server is ProSupport Plus. This level of service provides the most comprehensive support features, including proactive and predictive support capabilities that are essential for hardware monitoring.
Here's the rationale for this answer:
ProSupport Plus: This is the highest level of service offered by Dell, providing 24x7 priority access to ProSupport engineers, repairs for accidental damages, and proactive monitoring with SupportAssist technology1.
SupportAssist Technology: SupportAssist is a proactive monitoring tool that automatically detects hardware and software issues. It requires an active ProSupport or ProSupport Plus warranty to utilize all its features2.
Hardware Monitoring: With ProSupport Plus, SupportAssist can perform detailed hardware monitoring, send alerts, and even initiate automatic case creation for issues3.
While SupportAssist can still function with other warranty levels, ProSupport Plus ensures the full utilization of its capabilities, especially for critical hardware status monitoring and automated support case generation. It's important to have the appropriate level of warranty to ensure that servers are monitored effectively and support is provided promptly when issues are detected.

QUESTION 33
DRAG DROP
Match the device to be discovered with the correct discovery protocol.

Select and Place:

Ethernet Switch

Windows Server

PowerEdge MX7000 chassis

PowerEdge chassis (CMC)

PowerVault ME

Options

WS-Man

SNMP

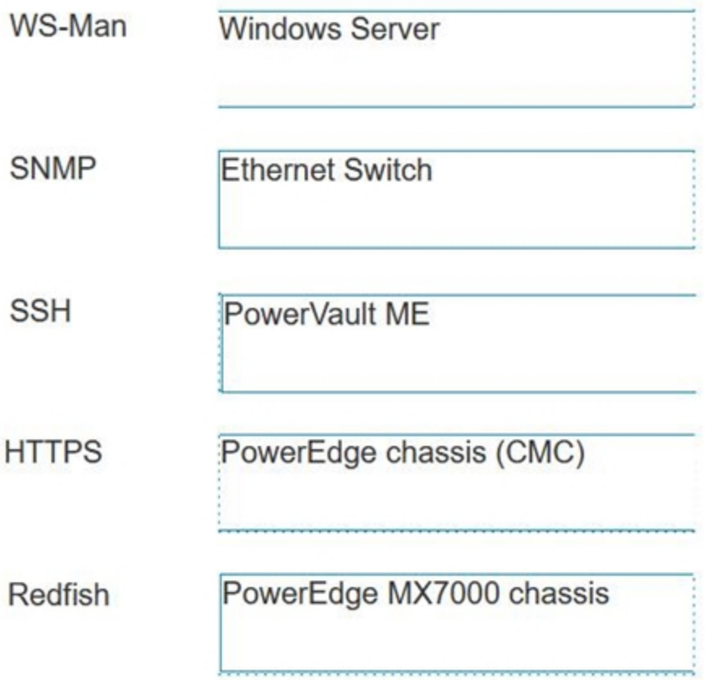
SSH

HTTPS

Redfish

Correct Answer:

Options



Section:
Explanation:

QUESTION 34
What advantage does the IPMI discovery protocol have over SNMP?

A. There is an added encryption layer with IPMI
B. Discovery timeouts increase for SNMP
C. IPMI allows for subsystem sensor monitoring
D. No credentials are required when using IPMI

Correct Answer: C
Section:
Explanation:
IPMI (Intelligent Platform Management Interface) is a set of computer interface specifications for an autonomous computer subsystem that provides management and monitoring capabilities independently of the host system's CPU, firmware, and operating system. One of the key advantages of IPMI over SNMP (Simple Network Management Protocol) is its ability to monitor and manage various subsystem sensors within the hardware. While SNMP is widely used for network management and can gather data from various devices on the network, it is not as specialized in sensor data collection as IPMI. IPMI provides more detailed monitoring of system health and environment by allowing access to a broader range of sensor types and data. This includes temperatures, voltages, fans, power supplies, and more123.
Moreover, IPMI operates independently of the operating system, which means it can function even if the server's OS fails or is unresponsive. This level of monitoring is crucial for maintaining system stability and preventing downtime due to hardware issues.
Dell EMC OpenManage SNMP Reference Guide1
Server Fault community discussions on Dell OpenManage and IPMI2

Spiceworks Community insights on Dell OpenManage monitoring3
==========

QUESTION 35
After onboarding a device, what are the recommended actions to apply a VLAN template with OpenManage Enterprise?

A. Create IOA template Configure VLAN settings Deploy Template on IOA
B. Create VLAN template Configure VLAN settings Deploy Template on Modular Server
C. Create server template Configure VLAN settings Deploy Template on Modular Server
D. Create server template Configure VLAN settings Deploy Template on IOA

Correct Answer: B
Section:
Explanation:
Create VLAN Template: The first step is to create a VLAN template within OpenManage Enterprise. This involves defining the VLAN ID and any associated settings such as name, description, and VLAN type.
Configure VLAN Settings: Once the template is created, you need to configure the VLAN settings according to your network design. This may include setting up access or trunk modes, allowed VLANs on trunks, and other relevant settings.
Deploy Template on Modular Server: The final step is to deploy the VLAN template on the modular server. This action applies the VLAN configuration to the server interfaces, ensuring that the server can communicate on the specified VLANs.
The process of applying a VLAN template is documented in the OpenManage Enterprise Modular API guide1, which provides detailed instructions on how to apply VLANs to a template. Additionally, Dell's support videos and documentation offer guidance on creating and deploying server templates in OpenManage Enterprise2.
==========