

Dell OpenManage Operate Achievement

EMC D-OME-OE-A-24

Version Demo

Total Demo Questions: 7

Total Premium Questions: 74

Buy Premium PDF

<https://passqueen.com>

support@passqueen.com

QUESTION NO: 1

In the OpenManage Enterprise web console where can VLAN settings be managed?

- A. Devices > Select Device > IOA > Hardware > Networking
- B. Network Devices > IOA Device Settings
- C. Configuration > Network Devices
- D. Devices > Select Device > View Details > Hardware > Networking

ANSWER: D

Explanation:

Devices > Select Device > View Details > Hardware > Networking is the correct navigation path because VLAN configuration is exposed in the managed device's hardware networking inventory and configuration area. OpenManage Enterprise first requires an administrator to select the relevant discovered device, then open its detailed view. The Hardware section presents component-level information and supported configuration capabilities; Networking is where network adapters and their associated settings, including VLAN-related settings when supported by the managed hardware and its management interface, are accessed. This device-focused workflow ensures that any VLAN settings are viewed and managed in the context of the specific server or chassis whose network interfaces are being configured. Available controls can depend on the device model, installed adapter or controller, firmware level, discovery method, and user permissions. Dell's OpenManage Enterprise documentation provides the product user guides and current feature documentation through its support portal, including device inventory and hardware-management workflows. See the [Dell OpenManage Enterprise documentation page](#) and the [Dell OpenManage Enterprise knowledge-base overview](#) for current documentation and release-specific guidance.

QUESTION NO: 2

On which virtualization platforms, other than VMware vSphere, can OpenManage Enterprise be deployed?

- A. Microsoft Hyper-V and Proxmox VE
- B. Microsoft Hyper-V and Red Hat KVM
- C. Red Hat KVM and Proxmox VE
- D. Citrix Xen and Red Hat KVM

ANSWER: B

Explanation:

Microsoft Hyper-V and Red Hat KVM is correct. Dell OpenManage Enterprise is delivered as a virtual appliance, and Dell supports deploying that appliance on supported Microsoft Hyper-V and KVM environments in addition to VMware vSphere. This gives organizations flexibility to operate OpenManage Enterprise within an established Windows-based virtualization infrastructure or within a Linux-based KVM virtualization environment, while retaining the appliance's core capabilities for discovering, monitoring, updating, and managing Dell infrastructure. The deployment workflow differs by hypervisor—for example, importing and configuring the virtual appliance image in the target platform—but the OpenManage Enterprise appliance remains the centralized management application after deployment. Administrators should always consult the installation guide that corresponds to their OpenManage Enterprise release because supported hypervisor versions, virtual hardware requirements, and deployment procedures can change between releases. Dell's OpenManage Enterprise documentation portal provides the applicable installation guides and release notes, while the product support page provides current documentation and downloads. See the [Dell OpenManage Enterprise documentation page](#) and [Dell OpenManage Enterprise support resources](#).

QUESTION NO: 3

Refer to Exhibit:

What is the corresponding OpenManage Enterprise feature used with this iDRAC setting?

- A. Redfish
- B. Automatic Discovery Jobs
- C. Server Initiated Discovery
- D. Global Exclude

ANSWER: C

Explanation:

Server Initiated Discovery is the OpenManage Enterprise feature that corresponds to the iDRAC Auto Discovery setting shown in the exhibit. When Auto Discovery is enabled and configured in iDRAC, the server can advertise itself to OpenManage Enterprise rather than waiting for an administrator to create and run a conventional discovery job. This supports faster onboarding of newly deployed servers and helps reduce manual inventory-management work.

OpenManage Enterprise listens for these server-initiated discovery communications and presents eligible devices for management. The iDRAC configuration supplies the information needed for the controller to locate and communicate with the OpenManage Enterprise appliance, including the applicable network-discovery method and periodic refresh behavior. After the appliance receives the notification, an administrator can discover and manage the server through OpenManage Enterprise according to the configured discovery and credential policies.

This workflow is particularly useful in environments that provision PowerEdge servers at scale, because it connects iDRAC-side auto-discovery configuration directly to automated enrollment in the central management console. Dell documents OpenManage Enterprise resources and guides on its [OpenManage Enterprise documentation page](#); broader OpenManage platform information is available from [Dell OpenManage systems-management resources](#).

QUESTION NO: 4 - (SIMULATION)

What is the correct order of steps to manually onboard a device?

ANSWER: Check the explanation for the answer

Explanation:

Correct order:

1. Go to the **IP Addresses** page.
2. Select **Discovery**.
3. Enter the administrator credentials.
4. Select the target device from the discovered devices.
5. Select **Onboarding** to add the device for management.

This sequence first starts discovery for the selected IP address, authenticates to the device, then selects and onboards the discovered target.

QUESTION NO: 5

A PowerEdge server was discovered successfully by OpenManage Enterprise using an iDRAC account with limited privileges. Health and inventory information are visible, but a configuration template deployment cannot be started for the server.

What should the administrator do to enable template deployment?

- A. Onboard the server by using an iDRAC account with administrative privileges
- B. Run a new discovery job against the server IP address
- C. Add the server to a custom group before deploying the template
- D. Create a new deployment template for the server model

ANSWER: A

Explanation:

The server must be onboarded by using iDRAC credentials with administrative privileges. Credentials with insufficient privileges allow OpenManage Enterprise to monitor the server and collect inventory, but they do not provide the authority required for configuration deployment and other management operations.

Running another discovery job does not increase the privileges of the configured account. Adding the device to a custom group or creating a new template also does not change the server from monitored to managed.

QUESTION NO: 6

An OpenManage Enterprise Administrator has been tasked to place servers in device groups depending on the data center location. The Administrator wants to ensure that all future servers are

included in these device groups.

How can this be accomplished?

- A. Create static groups based on a data center-specific attribute.
- B. Create dynamic groups based on a data center-specific attribute.
- C. Create query groups based on a data center-specific attribute.
- D. Create plug-in groups based on a data center-specific attribute.

ANSWER: C

Explanation:

Create query groups based on a data center-specific attribute. In OpenManage Enterprise, a query group is a dynamically maintained device group whose membership is determined by administrator-defined filter criteria. The administrator can build a query using inventory attributes that identify the relevant data-center location, such as device name, service tag, model, operating system, or other discovered properties available in the group query criteria. Once the query group is saved, OpenManage Enterprise evaluates discovered devices against that query. Servers that meet the location-specific criteria are included automatically, including newly discovered future servers as their inventory is collected and matches the query.

This approach provides persistent, policy-based grouping rather than requiring an administrator to manually add each server after discovery. It is particularly useful when separate operational tasks, monitoring views, configuration baselines, or alert policies need to target all servers belonging to a specific site. The location-identifying attribute must be applied consistently to discovered systems so that the query accurately represents the intended data center. Dell documents query groups as device groups created by using filter criteria and maintained according to matching device inventory information. See the [Dell OpenManage Enterprise documentation](#) and Dell's [OpenManage Enterprise support resources](#).

QUESTION NO: 7

An administrator is preparing to deploy a configuration template to a production server that already contains its operating system on a virtual disk. The server must retain its existing operating system and data.

Which template area requires the most careful review before deployment?

- A. The RAID configuration section
- B. The operating system IP address section
- C. The virtual identity section
- D. The discovery credential section

ANSWER: A

Explanation:

The RAID configuration section is correct. A deployment template can include storage and RAID attributes. Applying those settings can alter, replace, create, delete, or initialize virtual disks. If the template includes settings that affect the existing operating-system virtual disk, the system may no longer boot or its data may become unavailable.

Network and virtual-identity settings can affect connectivity, but they do not normally modify the operating-system disk layout. The administrator should remove or exclude unintended RAID configuration before deploying the template to an in-use server.