Free Questions for D-OME-OE-A-24 by dumpshq

Shared by Chavez on 09-08-2024

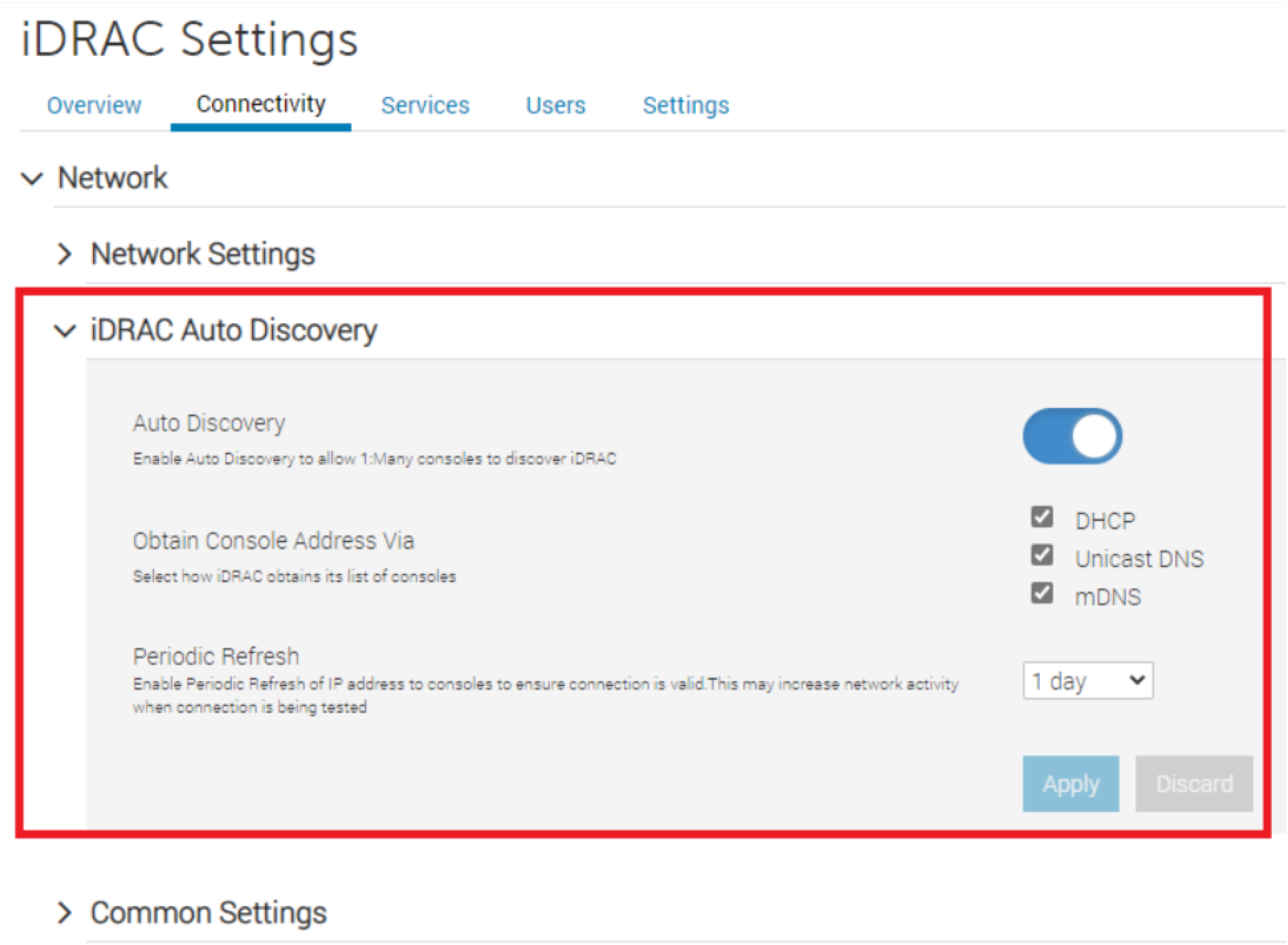
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

Refer to Exhibit:



iDRAC Settings

Network

Network Settings

iDRAC Auto Discovery

Auto Discovery

Enable Auto Discovery to allow 1:Many consoles to discover iDRAC

Obtain Console Address Via

Select how iDRAC obtains its list of consoles

☑ DHCP
☑ Unicast DNS
☑ mDNS

Periodic Refresh

Enable Periodic Refresh of IP address to consoles to ensure connection is valid.This may increase network activity when connection is being tested

1 day

Common Settings

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

Options:

A- Redfish

B- Automatic Discovery Jobs

C- Server Initiated Discovery

D- Global Exclude

Answer:

C

Explanation:

The iDRAC (Integrated Dell Remote Access Controller) setting displayed in the exhibit is associated with the Server Initiated Discovery feature in OpenManage Enterprise. This feature allows servers to initiate their discovery into OpenManage Enterprise using the iDRAC Auto Discovery settings.

Here's how it works:

iDRAC Auto Discovery: This setting, when enabled on the server's iDRAC, allows the server to present itself to OpenManage Enterprise for discovery and management.

Server Initiated Discovery: In OpenManage Enterprise, this feature is used to automatically discover servers that have iDRAC Auto Discovery enabled. It simplifies the process of adding new servers to the management console.

Network Configuration: The network settings in iDRAC, such as obtaining an IP address via DHCP, mDNS, or Unicast DNS, are configured to ensure that the server can communicate with OpenManage Enterprise.

Periodic Refresh: The periodic refresh setting ensures that the server's presence is consistently updated in OpenManage Enterprise, maintaining accurate and current device management.

By using Server Initiated Discovery, administrators can automate the process of integrating servers with OpenManage Enterprise, reducing the need for manual discovery jobs and streamlining the management of server infrastructure.

For more detailed information on Server Initiated Discovery and its configuration, administrators can refer to the official Dell OpenManage documentation and support resources.

Question 2

Question Type: MultipleChoice

An OpenManage Enterprise administrator has been tasked to enforce server configuration policies on 2,000 servers using six different configuration profiles.

What is a valid method to create a compliance template?

Options:

A- Export the deployment template

B- Import the template from dell.com

C- Clone an existing template

D- Export the template from a file

Answer:

C

Explanation:

To enforce server configuration policies on multiple servers using different configuration profiles, one valid method is to clone an existing template. Cloning allows administrators to take a pre-existing template that closely matches the desired configuration and make necessary adjustments to create a new compliance template. Here's how it can be done:

Access OpenManage Enterprise: Log into the OpenManage Enterprise console with administrative privileges.

Navigate to Templates: Go to the section where server templates are managed.

Select a Template: Choose an existing template that is closest to the desired configuration for the compliance policy.

Clone the Template: Use the option to clone the selected template. This will create a new template with the same configuration settings.

Modify the Template: Make any necessary changes to the cloned template to meet the specific requirements of the compliance policy.

Save the New Template: Save the newly created compliance template.

Apply the Template: Deploy the compliance template to the servers to enforce the configuration policies.

Cloning an existing template is a time-saving approach that leverages the work already done on previous configurations. It ensures consistency across server configurations and simplifies the management of multiple servers1.

For more detailed instructions on creating and managing server templates in OpenManage Enterprise, administrators can refer to the official Dell OpenManage documentation2.

Question 3

Question Type: MultipleChoice

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

Options:

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

Answer:

A

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 4

Question Type: MultipleChoice

A user with administrative privileges logs in to OpenManage Enterprise to create a report.

To which page do they navigate?

Options:

A- Plugins

B- Monitor

C- Devices

D- Alerts

Answer:

B

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

Question Type: MultipleChoice

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

Options:

A- Application settings

B- Identity pools

C- OME database

D- Audit logs

Answer:

C

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.

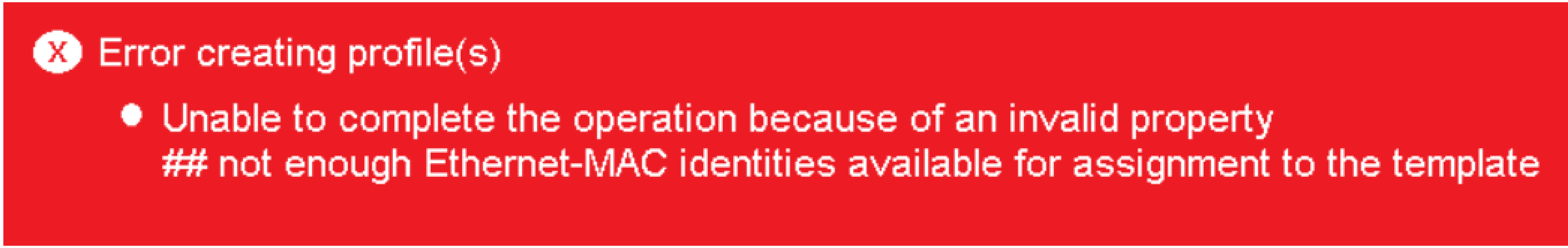
For more information on the discovery process and data storage in OpenManage Enterprise, administrators can refer to the official Dell OpenManage documentation and support resources1.

========================

Question 6

Question Type: MultipleChoice

Refer to the exhibit



Error creating profile(s)

- Unable to complete the operation because of an invalid property ## not enough Ethernet-MAC identities available for assignment to the template

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?

Options:

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

Answer:

D

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.