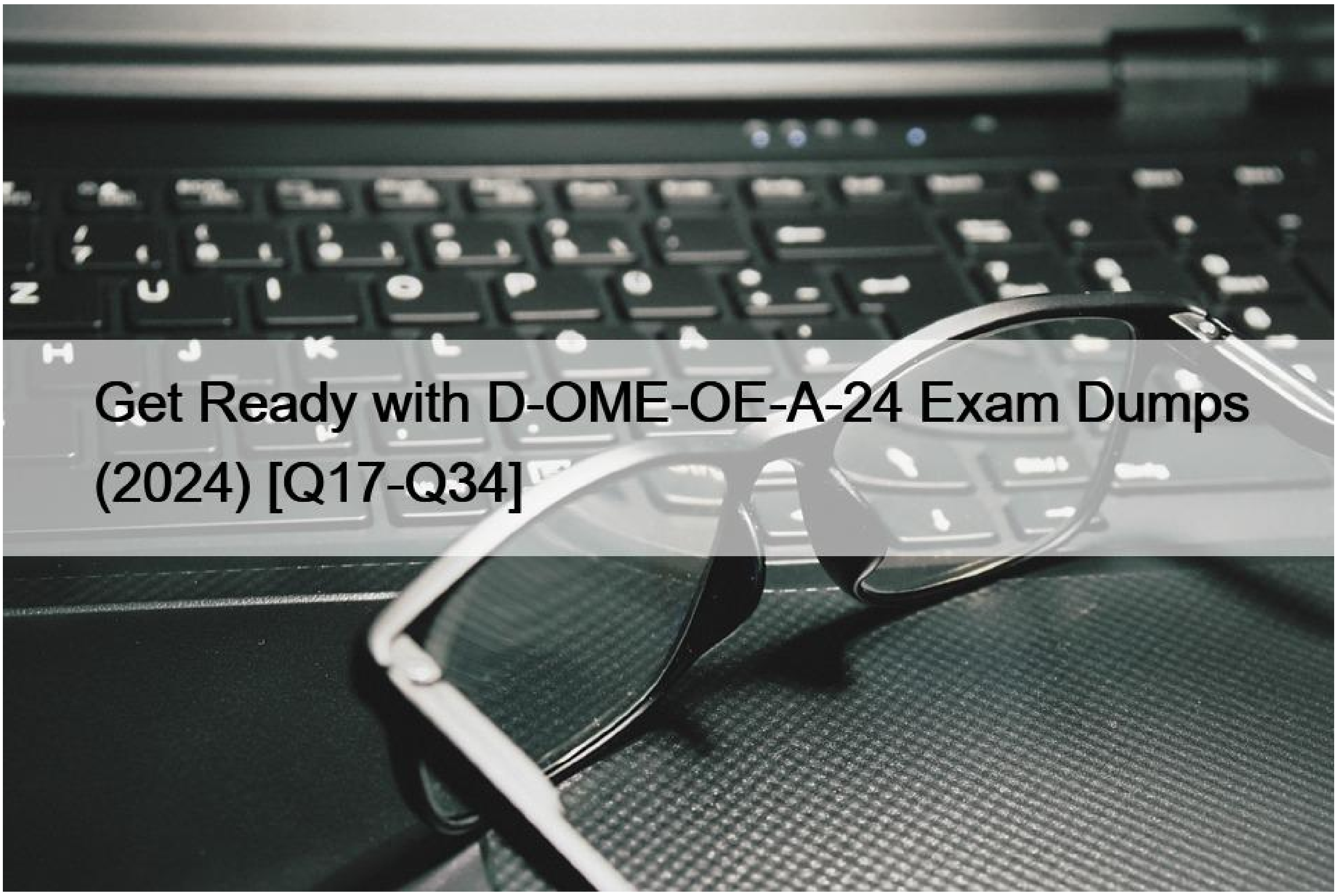
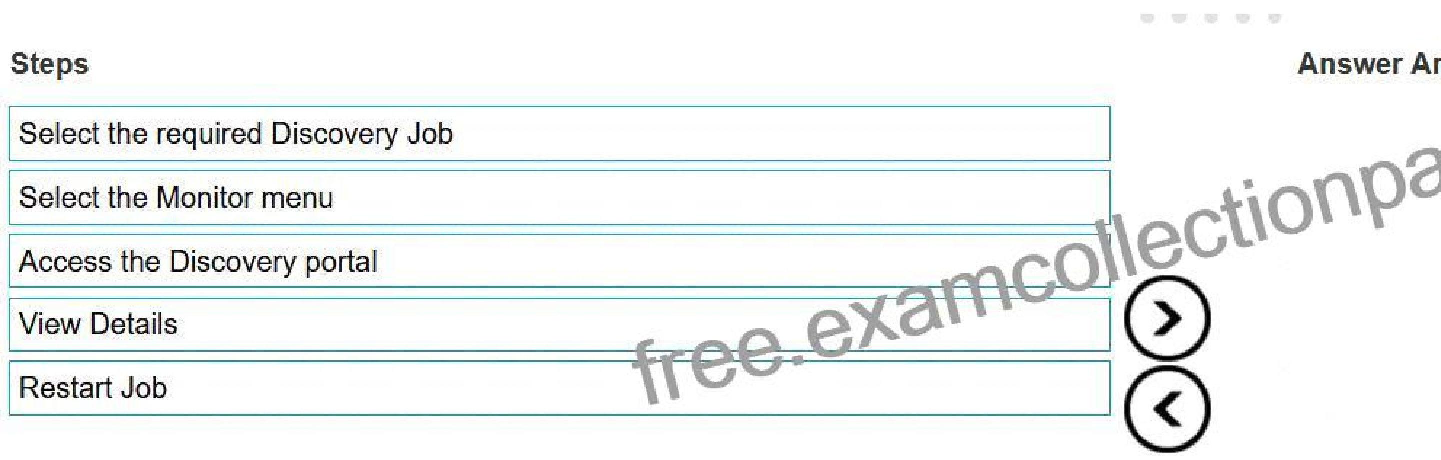
Get Ready with D-OME-OE-A-24 Exam Dumps (2024) [Q17-Q34



Get Ready with D-OME-OE-A-24 Exam Dumps (2024) Realistic D-OME-OE-A-24 Dumps are Available for Instant Access QUESTION 17

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



Steps

Select the required Discovery Job

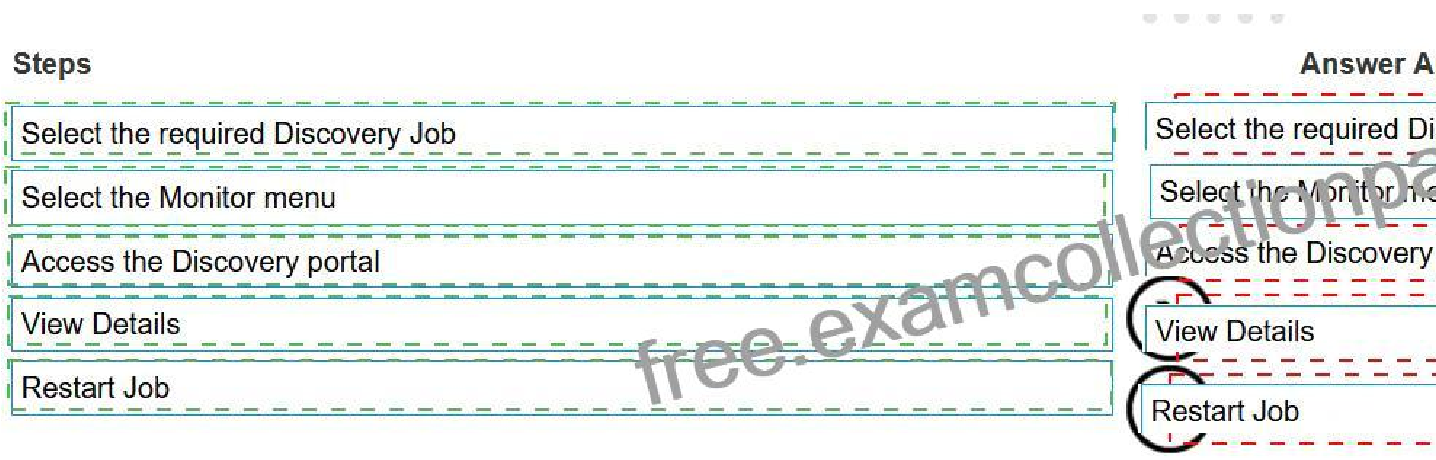
Select the Monitor menu

Access the Discovery portal

View Details

Restart Job

Answer Ar



Steps

Select the required Discovery Job

Select the Monitor menu

Access the Discovery portal

View Details

Restart Job

Answer A

Select the required Di

Select the Monitor me

Access the Discovery

View Details

Restart Job

Explanation:

The steps required to restart a previously stopped Discovery Job in OpenManage Enterprise are:

* 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.

The process to restart a Discovery Job typically involves navigating through the OpenManage Enterprise interface to locate the specific job and initiating a restart. The steps are based on standard procedures for managing Discovery Jobs within the OpenManage Enterprise system. For detailed instructions and best practices, refer to the official Dell OpenManage Enterprise User Guide, which provides comprehensive guidance on managing Discovery Jobs, including starting, stopping, and restarting jobs as needed.

QUESTION 18

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

To meet the storage administrator&#8217;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&#8217;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&#8217;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 19

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

To which page do they navigate?
* Plugins

- Monitor
- Devices
- Alerts

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 20

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

- Application settings
- Identity pools
- OME database
- Audit logs

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 21

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

- 5,000
- 2,500
- 7,500
- 10,000

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 22

Shortly after deploying a template you notice that you are no longer able to log in to the server Operating System.

What is the most likely cause?
* The Operating System IP address was changed
* The template deployment failed
* The deployment template included RAID configuration
* The Operating System Password was changed
The most likely cause of being unable to log in to the server Operating System shortly after deploying a template is that the Operating System Password was changed. When deploying a template in Dell OpenManage Enterprise, if the template includes user credentials or password settings, it may overwrite the existing credentials on the target server.

Here&#8217;s why this is the most likely cause:

* The Operating System IP address was changed: While changing the IP address can affect remote connectivity, it would not prevent login once access to the server is established.

* The template deployment failed: If the deployment had failed, the server would likely revert to its previous settings, including the original password.

* The deployment template included RAID configuration: Configuring RAID would not typically affect the Operating System&#8217;s ability to log in unless it resulted in data loss or corruption.

* The Operating System Password was changed: This directly affects the ability to log in, as the credentials used previously would no longer be valid.

It&#8217;s important to review the contents of the deployment template before applying it to ensure that any changes to user credentials are intentional and documented. For more information on the effects of template deployment on server settings, you can refer to the Dell OpenManage Enterprise documentation and community discussions1.

QUESTION 23

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?
* Only the item author can modify an existing discovery task.
* The task must be deleted, then re-created.
* It is not possible to modify an existing discovery task.
* Only an Administrator can edit an existing discovery task.
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&#8217;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 24

What is the maximum number of static network routes that can be configured in a single-homed OpenManage Enterprise appliance?
* 10
* 40
* 20
* 30
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 25

Which option is available in the Discovery portal when multiple jobs are selected simultaneously?
* Run
* Reschedule
* Edit
* Restart
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&#8217;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 &#8216;Reschedule&#8217; 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&#8217;s needs. This information is based on the functionality described in the OpenManage Enterprise documentation and user guides123.

QUESTION 26

Where is the Server Initiated Discovery feature enabled?
* The Configure Server Initiated Discovery option from the Text User Interface
* The Set Networking Parameters option from the Text User Interface
* Application Settings > Console Preferences from the GUI
* Monitor > Server Initiated Discovery from the GUI
The Server Initiated Discovery feature is enabled through the Text User Interface (TUI) of the OpenManage Enterprise appliance. Here are the steps to enable this feature:

* Log in to the OpenManage Enterprise TUI: Access the TUI through the VM Guest Console.

* Select Configure Server Initiated Discovery: Navigate to this option and press Enter.

* Enable Server Initiated Discovery: Select the option to enable Server Initiated Discovery and confirm by selecting the Apply option.

* Enter Administrator Password: Provide the administrator password for OpenManage Enterprise to confirm the changes.

* Close the Confirmation Dialog: After enabling the feature, close the dialog to complete the process.

These steps are outlined in the Dell Technologies OpenManage Enterprise documentation, which provides detailed instructions for enabling and configuring the Server Initiated Discovery feature1. It&#8217;s important to ensure that the corresponding DNS entries are added for OpenManage Enterprise in the DNS server to support this feature.

QUESTION 27

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?
* Static
* Discovery
* Dynamic
* Query
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&#8217;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.

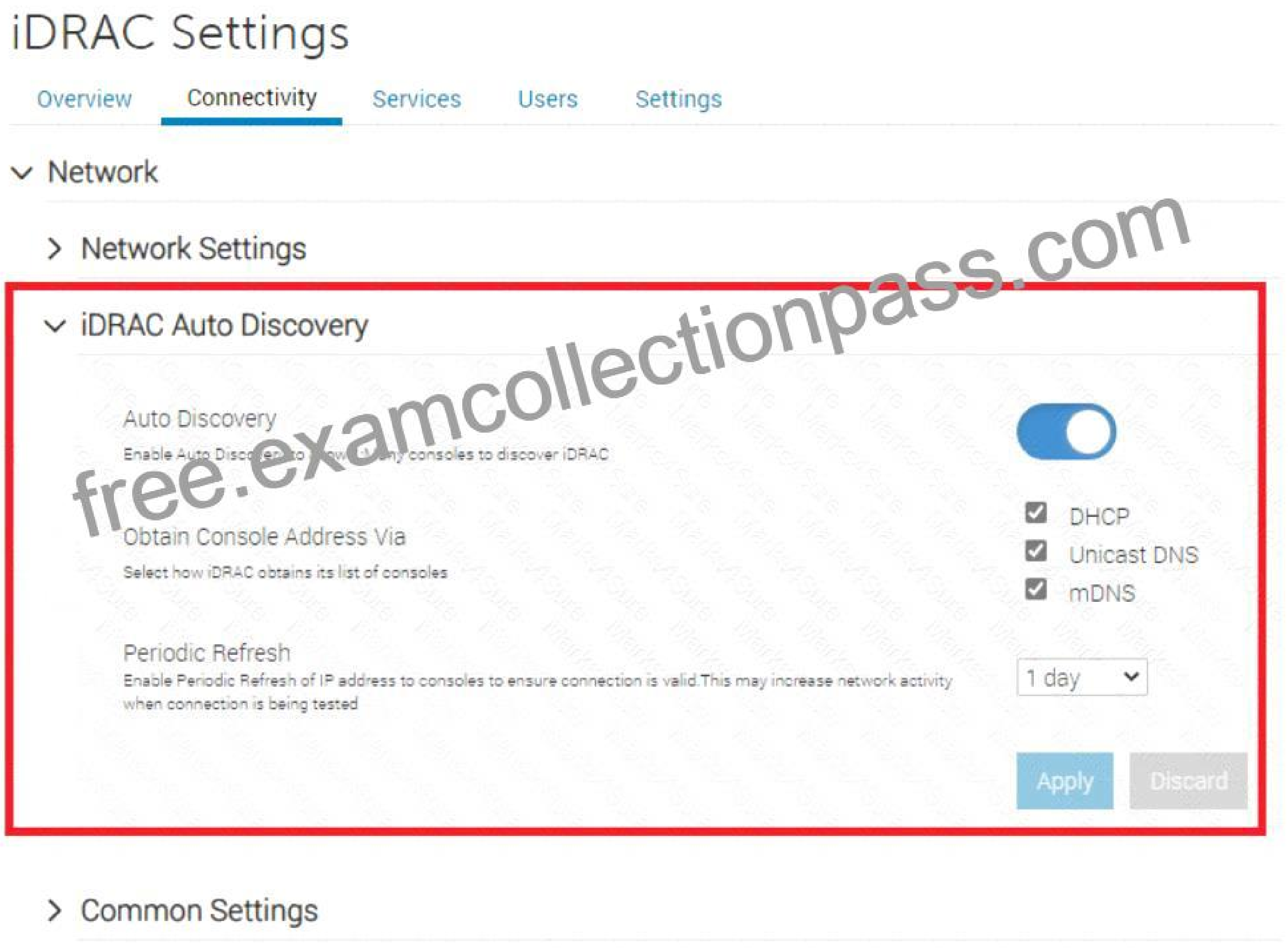
* Query Groups: While these groups can be based on specific queries, they are not automatically updated like Dynamic groups.

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 28

Refer to Exhibit:



iDRAC Settings

iDRAC Auto Discovery

Auto Discovery: ● On
Enable Auto Discovery to allow any 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

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

- Redfish
- Automatic Discovery Jobs
- Server Initiated Discovery
- Global Exclude

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&#8217;s how it works:

* iDRAC Auto Discovery: This setting, when enabled on the server&#8217;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&#8217;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 29

Which page displays the history of all jobs and tasks in OpenManage Enterprise console?
* Monitor
* Configuration
* Application Settings
* Discovery
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&#8217;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 30

An OpenManage Enterprise administrator plans to deploy a previously created template on a repurposed server. They want to ensure that the server boots from an ISO once the template is applied so that the OS is installed immediately.

Which share type should the user specify for the Deploy Template wizard?
* HTTP
* SCP
* FTP
* CIFS
When deploying a template that includes booting from an ISO in OpenManage Enterprise, specifying the share type is crucial for the

server to access and boot from the ISO image. The correct share type to use in the Deploy Template wizard for this purpose is HTTP.

Here&#8217;s why HTTP is the appropriate choice:

* HTTP (Hypertext Transfer Protocol) is widely used for transmitting files over the internet or a network. When a server boots from an ISO, it requires a protocol that can be used to access the file over a network. HTTP is suitable for this because it allows the server to download the ISO image as if it were accessing a web page or file on the internet1.

The other options, such as SCP (Secure Copy Protocol), FTP (File Transfer Protocol), and CIFS (Common Internet File System), are also used for file transfers but may not be supported for this specific scenario within the Deploy Template wizard of OpenManage Enterprise.

For detailed instructions on deploying server templates and configuring boot from ISO, administrators should refer to the official Dell OpenManage Enterprise documentation and support resources1.

QUESTION 31

Which role or roles in OpenManage Enterprise can edit a report?
* Administrators only
* Device Managers and Viewers only
* Administrators, Device Managers, and Viewers
* Administrators and Device Managers only
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 32

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

- Once per hour
- Once per week
- Once per day
- Manually as needed

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.

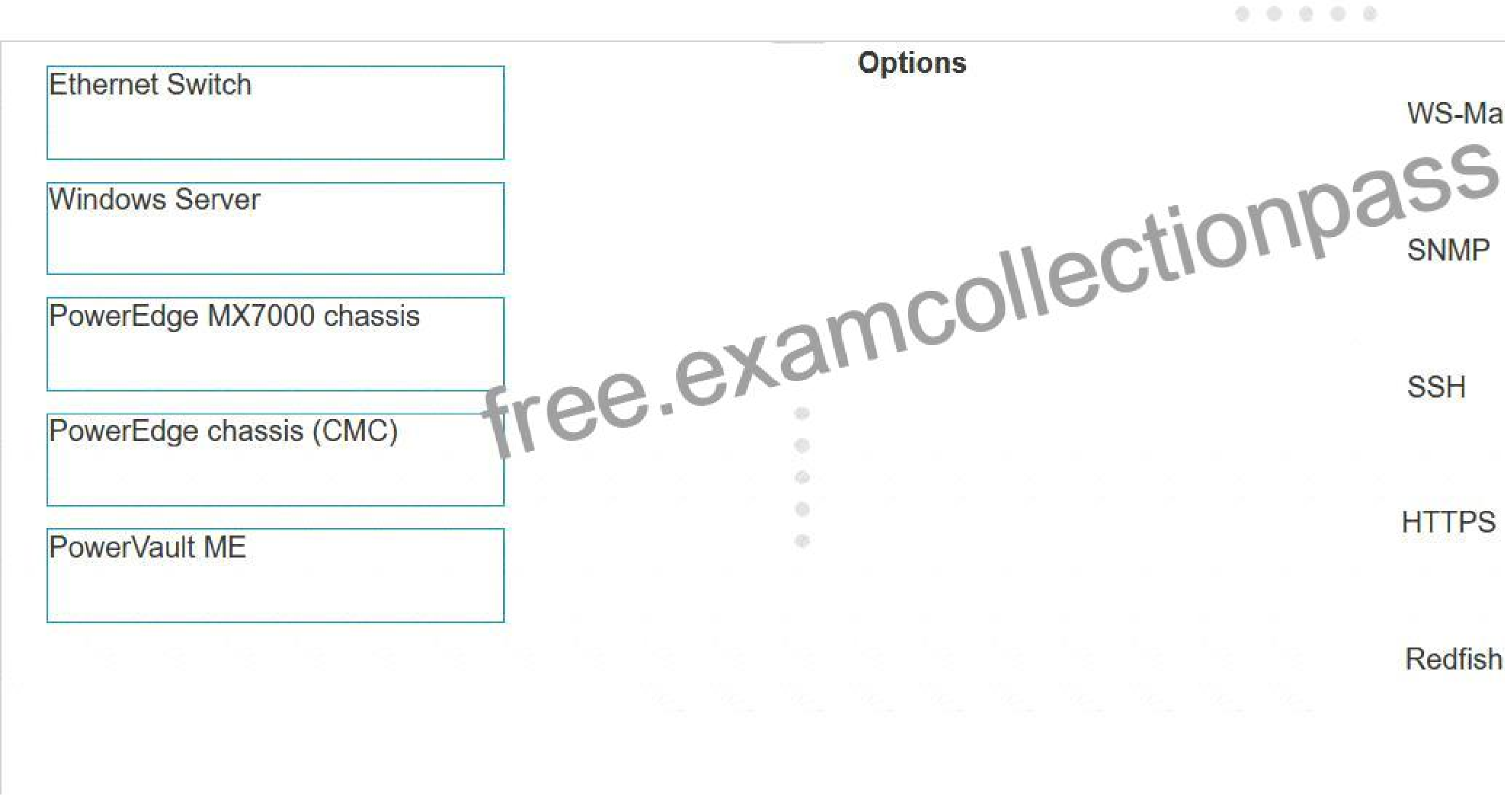
* Balancing Load and Currency: Running Discovery tasks too frequently (e.g., every hour) could lead to unnecessary load on the network and OpenManage Enterprise system, while running them too infrequently (e.g., weekly) might result in outdated information. Daily discovery strikes a balance between these two extremes.

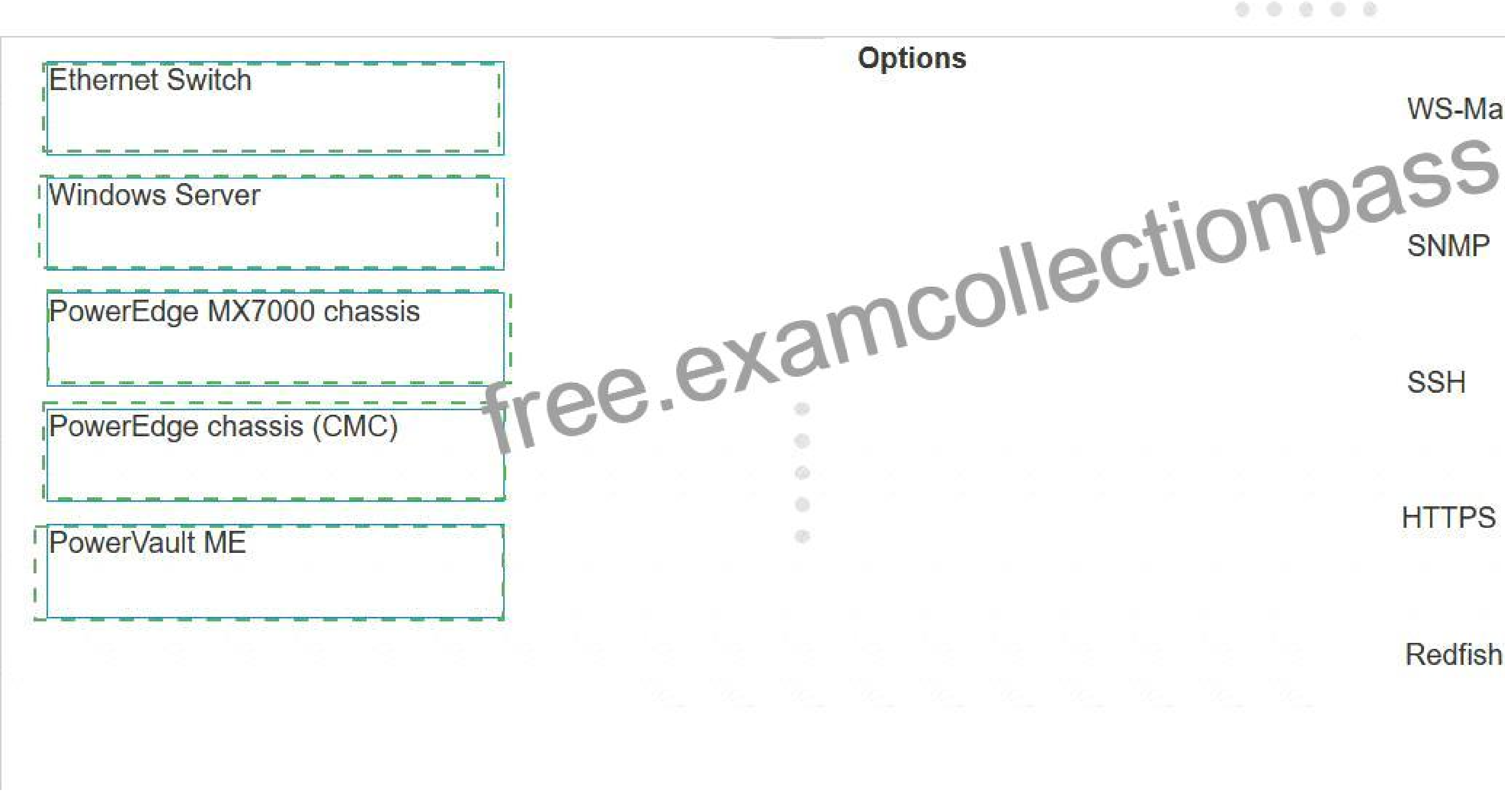
* Automated Scheduling: OpenManage Enterprise allows for Discovery tasks to be scheduled automatically, which can be set to occur daily to maintain an up-to-date inventory with minimal manual intervention1.

It&#8217;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 33

Match the device to be discovered with the correct discovery protocol.





Explanation:

* Ethernet Switch &#8211; SNMP

* Windows Server &#8211; WS-Man

* PowerEdge MX7000 chassis &#8211; Redfish

* PowerEdge chassis (iCMC) &#8211; HTTPS

* PowerVault ME &#8211; SSH

* Ethernet Switch: SNMP (Simple Network Management Protocol) is the standard protocol for network management. It&#8217;s used for collecting information from, and configuring, network devices, such as switches and routers.

* Windows Server: WS-Man (Web Services-Management) is a protocol for managing servers and devices. It&#8217;s particularly suited for Windows Servers as it&#8217;s built into the Windows Management Framework.

* PowerEdge MX7000 chassis: Redfish is a standard designed to deliver simple and secure management for hardware platforms. Given the advanced features of the PowerEdge MX7000 chassis, Redfish is the appropriate protocol for discovery and management.

* PowerEdge chassis (iCMC): HTTPS (Hypertext Transfer Protocol Secure) is used for secure communication over a computer network within a web browser. It&#8217;s suitable for devices like the PowerEdge chassis with an integrated Dell Remote Access Controller (iDRAC) that supports web-based management.

* PowerVault ME: SSH (Secure Shell) is a protocol for operating network services securely over an unsecured network. It&#8217;s ideal for storage systems like PowerVault, which require secure data transfer.

References for these answers can be found in the Dell OpenManage documentation, which provides detailed information on the management protocols supported by different Dell devices.

QUESTION 34

What type of device health monitoring capability is implemented in OpenManage Enterprise?
* Real-time
* Scheduled
* On-demand
* Interval based

Download Exam D-OME-OE-A-24 Practice Test Questions with 100% Verified Answers:
https://www.examcollectionpass.com/EMC/D-OME-OE-A-24-practice-exam-dumps.html]