

VMware

2V0-32.22 Exam

VMware Cloud Operations 8.x Professional

**Questions & Answers
Demo**

Version: 4.0

Question: 1

DRAG DROP

An administrator has been tasked with importing a new certificate for vRealize Operations using vRealize Lifecycle Manager.

Drag and drop the four correct actions the administrator must complete from the action list on the left and place the actions into the correct sequence on the right. (Choose four.)

Action List	Sequential Order
In The Navigation pane, click Certificates	
Login as admin@local	
In the Security page, click Locker	
On the Certificates page, click Import	
Login as root@local	
In the My Services page, click Locker	

Answer:

Explanation:

To import a new certificate for vRealize Operations using vRealize Lifecycle Manager (vRSLCM), the correct sequence of actions is as follows:

Login as admin@local

In the My Services page, click Locker

In the Navigation pane, click Certificates

On the Certificates page, click Import

Login as admin@local:

The administrator must log in with administrative credentials to access vRSLCM's services and settings.

In the My Services page, click Locker:

The "Locker" service in vRSLCM is used to manage certificates, credentials, and licenses.

In the Navigation pane, click Certificates:

Once in the Locker service, navigate to the Certificates section to manage and import SSL certificates.

On the Certificates page, click Import:

The final step is to click "Import" to upload the new certificate into vRSLCM.

Incorrect Steps:

Login as root@local: Root login is typically not required for vRSLCM operations.

In the Security page, click Locker: Locker is accessed through the My Services page, not the Security page.

By following this sequence, the certificate import process will be completed successfully.

Question: 2

Which three deployment architectures are valid for vRealize Log Insight listed below? (Choose three.)

- A. Ten node deployment with the integrated load balancer
- B. Single node deployment with an external load balancer
- C. Single node deployment with no load balancer
- D. Three node deployment with an external load balancer
- E. Single node deployment with the integrated load balancer
- F. Two node deployment with the integrated load balancer

Answer: C, D, F

Explanation:

vRealize Log Insight offers flexible deployment architectures to suit various needs.

Single node deployment with no load balancer : This is suitable for smaller environments with limited log volume. A single vRealize Log Insight node handles all log management tasks.

Three node deployment with an external load balancer : This architecture provides high availability and scalability. An external load balancer distributes incoming traffic across the nodes. This offers flexibility in load balancer selection and configuration.

Clustered deployment with integrated load balancer : This architecture also provides high availability and scalability. In this configuration, a minimum of three vRealize Log Insight nodes are deployed. The integrated load balancer distributes incoming log traffic across the nodes, preventing a single point of failure.

The following architectures are not valid for vRealize Log Insight:

Ten node deployment with the integrated load balancer: The maximum number of nodes in a cluster is limited, and ten nodes with an integrated load balancer is not a supported configuration.

Single node deployment with an external load balancer: A single node deployment does not require a load balancer.

Single node deployment with the integrated load balancer: The integrated load balancer is designed for clustered deployments with a minimum of three nodes.

Two node deployment with the integrated load balancer: The integrated load balancer requires a minimum of three nodes for cluster functionality.

Question: 3

Forty days ago, an administrator provisioned a Virtual Machine (vm-01) in preparation for a new project. The project has now been delayed due to budgetary constraints. As part of the monthly service management checks, a second administrator executes the reclaim action on all idle virtual machines and vm-01 is listed. The second administrator accidentally reclaims all idle virtual machines including vm-01.

What action can the administrator complete to prevent this scenario from happening again?

- A. Create a dynamic group with membership based on vSphere tags so that all new virtual machines are included and then exclude the entire group from reclaim analysis.
- B. Disable Capacity reclamation on the policy applied to new virtual machines.
- C. Create a new policy that disables the capacity reclamation on the policy and apply the policy to the parent object hosting new virtual machines.
- D. Increase the default value of the Exclude VM provisioned in the last x days setting.

Answer: D

Explanation:

Questions no: 3 Verified Answer = D Comprehensive Detailed Explanation with all VMware Reference = To prevent the accidental reclamation of recently provisioned VMs, the administrator should increase the default value of the "Exclude VM provisioned in the last x days" setting. This setting determines the period during which newly provisioned VMs are excluded from reclamation analysis. By increasing this value, the administrator can ensure that VMs provisioned for new projects are not inadvertently reclaimed .

Here's why the other options are not the best solution:

A . Create a dynamic group with membership based on vSphere tags so that all new virtual machines are included and then exclude the entire group from reclaim analysis. While this approach can be effective, it requires additional configuration and management of dynamic groups and vSphere tags. Increasing the "Exclude VM provisioned in the last x days" setting is a simpler and more direct solution.

B . Disable Capacity reclamation on the policy applied to new virtual machines. Disabling capacity reclamation entirely would prevent vRealize Operations from identifying and reclaiming any idle resources on those VMs, which may not be desirable.

C . Create a new policy that disables the capacity reclamation on the policy and apply the policy to the parent object hosting new virtual machines. Similar to option B, this would disable capacity reclamation for all VMs under the parent object, which may be too broad and prevent the reclamation of other idle resources.

Question: 4

An administrator needs to deploy a 3-node High Availability duster of vRealize Operations using custom CA-signed certificates. An existing vRealize Operations development environment has previously been deployed using vRealize Suite Lifecycle Manager
Which method should the Administrator use to complete this objective?

- A. Deploy 3 nodes independently, replace certificates and then form the 3-node duster
- B. Deploy a single node duster at the beginning to further expand it to 3 nodes in the next step.
- C. Deploy vRealize Operations analytics duster using Command Line Interface.
- D. Deploy vRealize Operations analytics duster using vRealize Suite Lifecycle Manager.

Answer: D

Explanation:

The administrator should deploy the vRealize Operations analytics cluster using vRealize Suite Lifecycle Manager (vRSLCM) . vRSLCM simplifies the deployment and management of vRealize Suite products, including vRealize Operations. It allows the administrator to deploy a 3-node High Availability cluster with custom CA-signed certificates in a streamlined manner.

Here's why the other options are not suitable:

A . Deploy 3 nodes independently, replace certificates and then form the 3-node cluster: This approach is more complex and prone to errors. It involves manual configuration and certificate replacement on each node.

B . Deploy a single node cluster at the beginning to further expand it to 3 nodes in the next step:

While possible, this method is not as efficient as deploying a 3-node cluster directly using vRSLCM.

C . Deploy vRealize Operations analytics cluster using Command Line Interface: Deploying using the CLI requires more expertise and manual intervention compared to using vRSLCM.

vRSLCM provides a centralized platform for managing the entire lifecycle of vRealize Suite products, including deployment, configuration, and upgrades. It simplifies the process of deploying a 3-node High Availability cluster of vRealize Operations with custom CA-signed certificates, ensuring a secure and efficient deployment.

Question: 5

In vRealize Operations, a user applies a CPU License to a custom group which has existing hosts. How will the Virtual Machines (VMs) on the existing hosts be affected?

- A. The CPU license gets converted to a CPU and VM license.
- B. The VMs running on the hosts show a 'License is Invalid*' watermark.
- C. The VMs running on the hosts are not affected.
- D. vRealize Operations prompts the user to apply a VM license key to the VMs running.

Answer: B

Explanation:

When a CPU license is applied to a custom group containing existing hosts in vRealize Operations, the VMs running on those hosts will show a "License is Invalid" watermark . This is because CPU licenses in vRealize Operations are specifically designed for licensing hosts and their CPU capacity. To license the VMs running on those hosts, you need to apply a separate VM license key.

Here's why the other options are incorrect:

- A . The CPU license gets converted to a CPU and VM license: vRealize Operations does not automatically convert CPU licenses to VM licenses.
- C . The VMs running on the hosts are not affected: This is incorrect, as the VMs will be affected by the lack of a valid VM license.
- D . vRealize Operations prompts the user to apply a VM license key to the VMs running: While vRealize Operations may indicate that the VMs are not properly licensed, it does not explicitly prompt the user to apply a VM license key.