Question 1

An administrator decides to restore VMware vCenter from a file-based backup following a failed upgrade. Which interface should the administrator use to complete the restore?

Options:

A- Direct Console User Interface (DCUI)

B- vCenter Management Interface (VAMI)

C- vSphere Client

D- vCenter GUI Installer

Answer:

D

Explanation:

Question 2

Question Type: **MultipleChoice**

An administrator is planning to upgrade a VMware vCenter instance to version 8. It is currently integrated with the following solutions:

* VMware Aria Automation

* VMware Cloud Director

Which tool can the administrator use to run Interoperability reports before the upgrade process?

Options:

A- sphere Update Manager

B- VMware Aria Suite Lifecycle

C- vCenter Server Update Planner

D- vSphere Lifecycle Manager

Answer:

C

Explanation:

The tool that can be used to run interoperability reports before upgrading a vCenter Server instance is vCenter Server Update Planner, which allows checking compatibility with other VMware products.

Question 3

Question Type: **MultipleChoice**

An administrator has a requirement to revert a running virtual machine to a previous snapshot after a failed attempt to upgrade an application. When the administrator originally took the snapshot, the following choices in the Take Snapshot dialog were made:

* Snapshot the virtual machine's memory = false

* Quiesce guest file system = false

What will be the result of the administrator selecting the 'Revert to Latest Snapshot? option to return the virtual machine to a previous snapshot? (Choose two.)

Options:

A- The virtual machine will be restored to the parent snapshot

B- The virtual machine will be restored in a powered off state

C- The virtual machine will be restored to the child snapshot

D- The virtual machine will be restored in a powered on state

E- The virtual machine will be restored in a suspended state

Answer:

A, B

Explanation:

https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-3E1BB630-9223-45E8-A64B-DCB90D450673.html

Question 4

An administrator is tasked with providing users access to objects within an existing VMware vCenter instance. The vCenter inventory has a single data center with one management vSphere cluster and five workload vSphere clusters.

The following requirements must be met for assigning the users access:

* Users must only be able to view all of the inventory objects associated with the management vSphere cluster.

* Users must be able to edit all of the inventory objects associated with the workload vSphere clusters.

The administrator creates a custom role to provide the permissions needed to allow users to edit inventory objects.

Which series of steps should the administrator complete to assign the custom role and provide the required level of access to users?

Options:

A- Apply Global permissions to assign the Read Only role to the root vCenter object.
Apply vCenter permissions to assign the custom role to the workload vSphere clusters and enable propagation.

B- Apply Global permissions to assign the Read Only role to the root vCenter object and enable propagation. Apply vCenter permissions

to assign the custom role to the workload vSphere clusters and enable propagation.

C- Apply Global permissions to assign the Read Only role to the root vCenter object. Apply vCenter permissions to assign the custom role to the workload vSphere clusters.

D- Apply Global permissions to assign the Read Only role to the root vCenter object and enable propagation. Apply vCenter permissions to assign the custom role to the workload vSphere clusters.

Answer:

D

Explanation:

Option D is correct because it allows the administrator to apply Global permissions to assign the Read Only role to the root vCenter object and enable propagation, which will apply to all of the inventory objects in vCenter, and then apply vCenter permissions to assign the custom role to the workload vSphere clusters, which will override the Global permissions and allow users to edit all of the inventory objects associated with the workload vSphere clusters. Option A is incorrect because it will not enable propagation for the Global permissions, which will limit the Read Only role to the root vCenter object only. Option B is incorrect because it will enable propagation for both the Global and vCenter permissions, which will create a conflict between the Read Only and custom roles. Option C is incorrect because it will not enable propagation for either the Global or vCenter permissions, which will limit the Read Only role to the root vCenter object only and the custom role to the workload vSphere clusters only. Reference: https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-A2A4371A-B888-404C-B23F-C422A8C40F54.html

Question 5

An administrator is tasked with migrating a single virtual machine (VM) from an existing VMware vCenter to a secure environment where corporate security policy requires that all VMs be encrypted. The secure environment consists of a dedicated vCenter instance with a 4-node vSphere cluster and already contains a number of encrypted VMs.

Which two steps must the administrator take to ensure the migration is a success? (Choose two.)

Options:

A- Ensure that the source and destination vCenter instances share the same Key Management Server (KMS).

B- Ensure that Encrypted vMotion Is turned off for the VM.

C- Ensure that the VM is encrypted before attempting the migration.

D- Ensure that the VM is powered off before attempting the migration.

E- Ensure that the source and destination vCenter Servers have a different Key Management Server (KMS).

Answer:

A, C

Explanation:

To ensure a successful migration of an encrypted VM to a secure environment, the administrator needs to ensure that the source and destination vCenter instances share the same Key Management Server (KMS), which provides encryption keys for both environments; and ensure that the VM is encrypted before attempting the migration, which allows preserving its encryption status during vMotion.

Question 6

An administrator creates a new corporate virtual machine (VM) template every month to include all of the latest patches. The administrator needs to ensure that the new VM template is synchronized from the primary data center site (London) to two secondary data center sites (Tokyo and New York). The administrator is aware that datastore space is limited within the secondary data center sites. The administrator needs to ensure that the VM template is available in the secondary sites the first time a new virtual machine is requested.

Which four steps should the administrator take to meet these requirements? (Choose four.)

Options:

A- Create a new published content library at the primary site.

B- Add the virtual machine template to the subscribed content library.

C- Create a new published content library in each secondary site.

D- Create a new subscribed content library in each secondary site.

E- Configure the subscribed content library to download content when needed.

F- Configure each subscribed content library to download content immediately.

G- Add the virtual machine template to the published content library.

Answer:

A, D, E, G

Explanation:

To meet the requirements of synchronizing and protecting images and templates with limited datastore space, the administrator needs to create a new published content library at the primary site, which makes it available for subscription by other vCenter Server instances; create a new subscribed content library in each secondary site, which allows accessing content from a published content library; configure the subscribed content library to download content when needed, which saves datastore space by only downloading content on demand; and add the virtual machine template to the published content library, which makes it available for other hosts to use.

Question 7

An administrator is configuring vSphere Lifecycle Manager to install patches to a vSphere cluster. The cluster runs workload virtual machines (VMs) that are incompatible with vSphere vMotion, and therefore cannot be live migrated between hosts during the installation of the patches.

Which configuration in vSphere Lifecycle Manager will allow the administrator to reduce the downtime associated with the patching operation without migrating the VMs?

Options:

A- Enable Distributed Power Management (DPM) and set the VM power state to the suspend to disk option

B- Enable Quick Boot and set the VM power state to the suspend to disk option

C- Enable vSphere High Availability (HA) admission control and set the VM power state to the suspend to memory option

D- Enable Quick Boot and set the VM power state to the suspend to memory option

Answer:

D

Explanation:

Question 8

Question Type: **MultipleChoice**

Which three features are only available when using vSphere Distributed Switches instead of vSphere Standard Switches? (Choose three.)

Options:

A- 802.1Q tagging

B- Port mirroring

C- Netflow

D- Configuration backup and restore

E- IPv6 support

F- IPv4 support

Answer:

B, C, D

Explanation:

Three features that are only available when using vSphere Distributed Switches instead of vSphere Standard Switches are port mirroring, which allows monitoring network traffic on a virtual switch port; Netflow, which allows collecting IP traffic information from a virtual switch; and configuration backup and restore, which allows saving and restoring distributed switch settings.

Question 9

Question Type: **MultipleChoice**

An administrator has Windows virtual machines (VMs) and VMware Tools is installed in each VM. The administrator performs a status check of VMware Tools using vSphere Lifecycle Manager.

What is the VMware Tools status for the Windows VMs if the version of VMware Tools has a known problem and must be immediately upgraded?

Options:

A- Version Unsupported

B- Guest Managed

C- Unknown

D- Upgrade Available

Answer:

A

Explanation:

If VMware Tools has a known problem, the tools status will be Version Unsupported https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere-lifecycle-manager.doc/GUID-12649CBB-F69A-4199-8957-B4C0170B4E9A.html

Question 10

An administrator is tasked with deploying a new on-premises software-defined data center (SDDC) that will contain a total of eight VMware vCenter instances.

The following requirements must be met:

* All vCenter instances should be visible in a single vSphere Client session.

* All vCenter inventory should be searchable from a single vSphere Client session.

* Any administrator must be able to complete operations on any vCenter instance using a single set of credentials.

What should the administrator configure to meet these requirements?

Options:

A- Two Enhanced Linked Mode groups consisting of four vCenter instances each in a Single Sign-On domain.

B- A single Hybrid Linked Mode group consisting of four vCenter instances each in a Single Sign-On domain.

C- A single Enhanced Linked Mode group consisting of eight vCenter instances in one Single Sign-On domain.

D- A single Hybrid Linked Mode group consisting of eight vCenter instances in one Single Sign-On domain.

Answer:

B

Explanation:

To meet the requirements of viewing and searching all vCenter instances and inventory with a single vSphere Client session and a single set of credentials, the administrator needs to configure a single Enhanced Linked Mode group consisting of eight vCenter instances in one Single Sign-On domain.

https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-vcenter-installation/GUID-4394EA1C-0800-4A6A-ADBF-D35C41868C53.html

Question 11

Question Type: **MultipleChoice**

After adding a new vSphere ESXi host with identical hardware configuration to an existing vSphere cluster, which task would an administrator complete prior to checking the compliance with an existing host profile?

Options:

A- Attach the host profile to the new host

B- Duplicate the host profile

C- Copy the host settings from the new host

D- Import the host profile

Answer:

A

Explanation:

The task that should be completed prior to checking the compliance with an existing host profile is to attach the host profile to the new host, which allows applying the configuration template of the reference host to the new host.