Free Questions for 5V0-31.22 by dumpssheet

Shared by Bowers on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

An architect is decommissioning a host from a VI Workload Domain and wants to reuse it in a VMware Cloud Foundation environment.

Which statement accurately describes this process?

Options:

A- Use the decommission host workflow against a host with an unassigned state, and then run the commission host workflow.

B- Use the decommission host workflow against a host with an unassigned state, re-image the host, and then run the commission host workflow.

C- Use the decommission host workflow against a host with an assigned state, re-image the host, and then run the commission host workflow.

D- Use the decommission host workflow against a host with an assigned state, and then run the commission host workflow.

Answer:

B

Explanation:

https://docs.vmware.com/en/VMware-Cloud-Foundation/5.0/vcf-admin/GUID-2C3E06BA-7B77-4F4B-958C-1BFCB3E9CBA7.html
Removing hosts from the SDDC Manager inventory is called decommissioning. If you want to re-use a host in a different workload domain, you must decommission, re-image, and commission the host before adding it to the workload domain. The hosts that you want to decommission must not be assigned to a workload domain. If a host is assigned to a workload domain, you must remove it before you can decommission it. See Remove a Host from a vSphere Cluster in a Workload Domain.

Use the decommission host workflow against a host with an unassigned state, re-image the host, and then run the commission host workflow.According to the VMware Cloud Foundation documentation1, removing hosts from the SDDC Manager inventory is called decommissioning. If you want to re-use a host in a different workload domain, you must decommission, re-image, and commission the host before adding it to the workload domain. The hosts that you want to decommission must not be assigned to a workload domain. If a host is assigned to a workload domain, you must remove it before you can decommission it.

Question 2

Question Type: MultipleChoice

An administrator is tasked with deploying a new VI Workload Domain with VMFS on FC storage.

Which type of network pool must the hosts be associated with while adding them to VCF inventory?

Options:

A- NFS only network pool

B- Network pool with vMotion and iSCSI

C- vMotion only network pool

D- iSCSI only network pool

Answer:

C

Explanation:

To create a VI workload domain with VMFS on FC storage, the hosts must be commissioned with VMFS on FC as the storage type and must be associated with a vMotion only or vMotion and NFS network pool. https://docs.vmware.com/en/VMware-Cloud-Foundation/5.0/vcf-admin/GUID-4EBF9094-F732-4800-86FF-30C5D88B9758.html

To deploy a VI Workload Domain with VMFS on FC storage, the hosts must be associated with a network pool that contains the vMotion network information. This is because the vMotion network is required for adding a host to the SDDC Manager inventory and for migrating workloads between hosts.

A NFS only network pool, a network pool with vMotion and iSCSI, or an iSCSI only network pool are not valid options for deploying a VI Workload Domain with VMFS on FC storage. These network pools are used for different types of storage, such as NFS, vVols on iSCSI, or vSAN.

The references are:

Question 3

Question Type: **MultipleChoice**

An administrator is tasked with adding additional capacity to the existing VI workload domain to prepare for a requested workload migration.

Which supported storage types would the administrator configure to complete the task?

Options:

A- vVols. SMB 3.0, VMFS on FC

B- NFS v3, NFS v4.1, vSAN

C- SMB 3.0, VMFS on FC, NFS v4.1

D- NFS v2, NFS v3, vVols

Answer:

B

Explanation:

https://docs.vmware.com/en/VMware-Cloud-Foundation/4.5/vcf-getting-started/GUID-C68FD810-D270-43F2-AEBF-D522BA1F402B.html#:~:text=For%20each%20VI%20workload%20domain,vSphere%20maximum%20of%2064%20hosts. You create VI workload domains to run customer workloads. For each VI workload domain, you can choose the storage option - vSAN, NFS, vVols, or VMFS on FC.

VMware Cloud Foundation supports several storage types as principal and supplemental storage for VI workload domains. Principal storage is the initial shared storage type that is selected during the creation of a workload domain or cluster in SDDC Manager. Supplemental storage is the additional shared storage type that can be added after a cluster has been created using the vSphere Client.

The supported principal storage types for VI workload domains are:

vSAN

NFS v3

vVols (FC, iSCSI, or NFS)

The supported supplemental storage types for VI workload domains are:

vSAN

NFS v3 or v4.1

vVols (FC, iSCSI, or NFS)

VMFS on FC

iSCSI

NVMeoF/TCP

Therefore, the only option that contains only supported storage types for VI workload domains is B. NFS v3, NFS v4.1, vSAN.

For more information, please refer to the following sources:

Supported Storage Types for VMware Cloud Foundation

Managing Storage in VMware Cloud Foundation

VMWare Cloud Foundation Now Supports NVMeoF/TCP

Question 4

Question Type: **MultipleChoice**

Which product SSL certificate replacement can be automated using the SDDC Manager?

Options:

A- vRealize Automation

B- vRealize Log Insight

C- NSX Manager

D- Horizon

Answer:

C

Explanation:

https://docs.vmware.com/en/VMware-Cloud-Foundation/5.0/vcf-admin/GUID-80431626-B9CD-4F21-B681-A8F5024D2375.html

Question 5

Question Type: **MultipleChoice**

Where is the Harbor Image Registry service enabled?

Options:

A- vSAN Cluster

B- Supervisor Cluster

C- vSphere Cluster

D- Supervisor Namespace

Answer:

B

Explanation:

'In the vSphere Client, browse to the vCenter cluster where Workload Management is enabled. Select Configure. Select Supervisor Cluster. Select Image Registry. Click Enable Harbor. Select the Storage Policy for placement of container images. Click OK to complete the process' https://docs.vmware.com/en/VMware-vSphere/7.0/vmware-vsphere-with-tanzu/GUID-AE24CF79-3C74-4CCD-B7C7-757AD082D86A.html

Question 6

Which type of storage entity is used as the backing disks for persistent volumes in vSphere with Tanzu?

Options:

A- Thick provisioned VMDK

B- Raw Device Mapping (RDM)

C- First Class Disk (FCD)

D- Virtual Volumes (vVOLs)

Answer:

C

Explanation:

https://docs.vmware.com/en/VMware-vSphere/7.0/vmware-vsphere-with-tanzu/GUID-1B136277-E46C-41FC-9C8C-3E78E9B97F5C.html

vSphere with Tanzu uses the First Class Disk (FCD) type of virtual disks to back persistent volumes. FCD, also known as Improved Virtual Disk, is a named virtual disk not associated with a VM. FCDs are identified by UUID and can be managed independently of VMs.

Thick provisioned VMDK, Raw Device Mapping (RDM), and Virtual Volumes (vVOLs) are not used as the backing disks for persistent volumes in vSphere with Tanzu.

The references are:

Using Persistent Storage in vSphere with Tanzu, section "Persistent Volume"

vSphere with Tanzu Storage, section "First Class Disk"

Question 7

Question Type: **MultipleChoice**

Which vSphere Lifecycle Manager (LCM) function is supported in VMware Cloud Foundation (VCF)?

Options:

A- Manage certificate replacement for ESXi hosts.

B- Rotate passwords for ESXi hosts.

C- Downgrade VM hardware version.

D- Install and update third-party software on ESXi hosts.

Answer:

D

Explanation:

The vSphere Lifecycle Manager (LCM) function that is supported in VMware Cloud Foundation (VCF) is D. Install and update third-party software on ESXi hosts.According to the VMware Cloud Foundation documentation1, vSphere Lifecycle Manager images can include components that are created and published by third-party software vendors, such as drivers, patches, and solutions. These components can be added to the image to install and update the third-party software on the ESXi hosts in a cluster.VMware Cloud Foundation allows you to manage all images in a single place and re-use them for clusters across workload domains2

Question 8

Question Type: **MultipleChoice**

Which functionality does a NSX Tier-1 Gateway provide to a vSphere with Tanzu deployment?

Options:

A- Downlink connection to segments

B- Downlink connection to Tier-0 gateway

C- Layer 2 Switching

D- Static or dynamic routing

Answer:

A

Explanation:

https://docs.vmware.com/en/VMware-Validated-Design/6.2/sddc-architecture-and-design-for-a-vsphere-with-tanzu-workload-domain/GUID-8E524188-65F6-4FF2-B8A3-2D9B0C86FE2A.html

A NSX Tier-1 Gateway provides the functionality of a downlink connection to segments in a vSphere with Tanzu deployment.According to the VMware documentation1, a segment is a virtual layer-2 domain that can be either overlay-backed or VLAN-backed. A NSX Tier-1 Gateway connects to one or more segments and provides routing and security services for the workloads attached to those segments.A NSX Tier-1 Gateway also connects to a NSX Tier-0 Gateway, which provides uplink connectivity to external networks2

Question 9

What are the correct steps to grant the DevOps team permissions to a vSphere Namespace in a VMware Cloud Foundation (VCF) developer-ready workload domain while following the principle of least privilege access?

Options:

A- At the Permissions setting, add the DevOps group and assign the "Editor" permission

B- At the Global Permissions setting, add the DevOps group and assign the vSphere Kubernetes Manager role

C- At the Global Permissions setting, add the DevOps group and assign the SupervisorService Cluster Operator role

D- At the Permissions setting, add the DevOps group and assign the "Can edit" permission

Answer:

A

Explanation:

At the Permissions setting, add the DevOps group and assign the "Editor" permission. This is the recommended way to grant the DevOps team permissions to a vSphere Namespace in a VMware Cloud Foundation (VCF) developer-ready workload domain while following the principle of least privilege access.According to the VMware Cloud Foundation documentation1, the Editor permission allows users to create, modify, and delete objects within a vSphere Namespace, such as vSphere Pods, Tanzu Kubernetes clusters, and stand-alone VMs.The Editor permission also allows users to view and manage storage policies, VM classes, and content libraries for the namespace1

B) At the Global Permissions setting, add the DevOps group and assign the vSphere Kubernetes Manager role is not a correct option, because it will grant more privileges than necessary to the DevOps team. The vSphere Kubernetes Manager role is a global role that allows users to manage all aspects of vSphere with Tanzu, such as enabling Workload Management on clusters, creating and configuring vSphere Namespaces, and managing storage policies and VM classes.This role should be assigned only to vSphere administrators who are responsible for configuring and maintaining the VCF developer-ready workload domain1

C) At the Global Permissions setting, add the DevOps group and assign the SupervisorService Cluster Operator role is not a correct option, because it will also grant more privileges than necessary to the DevOps team. The SupervisorService Cluster Operator role is a global role that allows users to manage all aspects of Supervisor Services on clusters, such as creating and configuring Supervisor Service namespaces, managing service accounts and roles, and deploying service instances.This role should be assigned only to vSphere administrators who are responsible for enabling and managing Supervisor Services on VCF developer-ready workload domains1

D) At the Permissions setting, add the DevOps group and assign the "Can edit" permission is not a correct option, because there is no such permission in vSphere with Tanzu. The available permissions for vSphere Namespaces are Viewer, Editor, and Admin. The Viewer permission allows users to view objects within a vSphere Namespace, but not create or modify them.The Admin permission allows users to perform all actions within a vSphere Namespace, as well as manage permissions for other users or groups1