VMware

5V0-31.22 Exam

VMware Cloud Foundation Specialist (v2)

Questions & Answers
Demo

Version: 4.0

Question: 1

An administrator needs additional capacity on a vSAN cluster. Each host currently has only one disk group. Which two approaches can be used to expand storage capacity in this situation? (Choose two.)

A. Increase the number of cache disks in the existing disk group.

B. Add an additional disk group.

C. Disable compression.

D. Increase the number of capacity disks in the existing disk group

E. Disable deduplication.

Answer: BD

Explanation:

To expand storage capacity in a vSAN cluster with one disk group, you can either add more drives to hosts in the cluster, which is commonly referred to as scaling up, or add capacity drives to existing disk groups

Option B: Add an additional disk group - According to search result [1], adding additional drives to a host will increase both capacity and performance [1], and each disk group contains one flash cache device and one or multiple capacity devices for persistent storage [2]. Therefore, adding an additional disk group to each host would increase the storage capacity of the vSAN cluster.

Option D: Increase the number of capacity disks in the existing disk group - Search result [1] explains that vSAN clusters require capacity and cache devices to function, and each disk group can contain multiple capacity devices for persistent storage [2]. Thus, an additional way to expand storage capacity in the vSAN cluster would be to increase the number of capacity disks in the existing disk group.

Reference: 1: VMware vSAN documentation 2: VMware vSAN documentation

A disk group is a collection of one or more flash-based cache devices and one or more capacity devices that provide storage capacity for a vSAN cluster. A vSAN cluster can have multiple disk groups, and each disk group can have a different configuration.

To expand storage capacity in a vSAN cluster where each host currently has only one disk group, the administrator can add an additional disk group or increase the number of capacity disks in the existing disk group.

Adding an additional disk group involves adding more disks to the host and creating a new disk group. This approach can provide additional capacity and performance benefits, as the new disk group can be configured with different settings to optimize performance and capacity.

Increasing the number of capacity disks in the existing disk group involves adding more capacity devices to the existing disk group. This approach can provide additional capacity, but may not necessarily provide performance benefits as the existing disk group may already be fully utilized.

Reference:

VMware vSAN 7.0 Design and Sizing Guide: https://storagehub.vmware.com/t/vmware-vsan/vmware-vsan-7-0-design-and-sizing-guide-2/

VMware vSAN Documentation: https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vsan-planning.doc/GUID-9B7C9685-64C5-49C2-8E3C-CC2E47AFBC6F.html

Question: 2

A VCF architect collected the following requirements when designing the expansion of a new VI Workload Domain with twenty four vSAN Ready nodes, each with a dual-port 25Gbps network interface card:

- Provide scalable high-performance networking with layer-3 termination at top-of-rack
- Protect workloads from switch/NIC/rack failure
- Provide isolation for DMZ workloads

- Provide at-least 25Gbps dedicated bandwidth to backup traffic
- Easily accept workloads on traditional VLAN-backed networks
- Fully-supported by VMware

Which three design considerations meet all of these requirements? (Choose three.)

A. Two-node Edge Cluster with ECMP

B. Spine and Leaf network topology with layer-3 at Spine

C. Stretched Clustering

D. Spine and Leaf network topology with layer-3 at top of rack

E. Two-node Edge Cluster with BFD

F. Core Aggregation network topology

Answer: BDF

Explanation:

Option B: Spine and Leaf network topology with layer-3 at Spine - A spine and leaf network topology is designed for high scalability and performance, and layer-3 at the spine ensures that there is no single point of failure for the layer-3 termination. This meets several of the requirements, including scalable high-performance networking with layer-3 termination at top-of-rack, protecting workloads from switch/NIC/rack failure, and providing isolation for DMZ workloads.

Option D: Spine and Leaf network topology with layer-3 at top of rack - Similar to Option B, this topology also provides high scalability and performance, and layer-3 at the top of rack meets the requirement for layer-3 termination at top-of-rack.

Option F: Core Aggregation network topology - This topology provides a highly available, redundant core switch for aggregation and routing, which meets the requirement for protecting workloads from switch/NIC/rack failure.

Based on the given choices, the correct answers would be B, D, and F.

Sources: [1] Designing VMware Infrastructure Topology and Architecture; Authors: Russel Nolan, Eiad Al-Aqqad [2] Network Topology Considerations for VMware vSAN; https://docs.vmware.com/en/VMware-vSAN/7.0/com.vmware.vsan.networking.doc/GUID-1A901C10-4894-4E9B-8A36-AD15ED52E61B.html [3]

Spine-Leaf Architecture: Introduction; https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-733553.html

Question: 3

An administrator has registered an external identity source in a consolidated architecture and would like to make sure that any subsequent workload domains can be accessed using the same identity sources.

How can this goal be achieved with VMware Cloud Foundation?

A. By configuring IWA as an identity source

B. By configuring LDAPS as an identity source

C. By keeping the pre-configured defaults

D. By replicating vSphere SSO configuration

Answer: D

Explanation:

vSphere Single Sign-On (SSO) provides secure authentication and authorization services for VMware Cloud Foundation components, including vCenter Server and Platform Services Controller (PSC). In a consolidated architecture deployment of VMware Cloud Foundation, the vSphere SSO configuration is shared across all the workload domains.

To ensure that subsequent workload domains can use the same identity sources as an external identity source registered in a consolidated architecture, the administrator needs to replicate the vSphere SSO configuration. This can be achieved by configuring the same identity sources for vSphere SSO across all the workload domains.

Configuring IWA (Integrated Windows Authentication) or LDAPS (Lightweight Directory Access Protocol over SSL) as an identity source is a part of configuring the vSphere SSO configuration for identity sources.

Keeping the pre-configured defaults does not guarantee that the subsequent workload domains will use the same identity sources as the external identity source registered in a consolidated architecture.

Reference:

VMware Cloud Foundation Operations and Administration Guide: https://docs.vmware.com/en/VMware-Cloud-Foundation/index.html

VMware vSphere Security Guide: https://docs.vmware.com/en/VMware-vSphere/7.0/vsphere-security-guide.pdf

To ensure that any subsequent workload domains can be accessed using the same identity sources, it is necessary to replicate the vSphere SSO configuration across all the workload domains in a consolidated architecture deployment. This can be achieved by replicating the vSphere SSO configuration between the primary and additional SDDC Manager instances. This ensures that all the workload domains registered with the SDDC Manager will be able to consume resources and services from the same identity sources without any additional configuration in each individual workload domain.

Reference: VMware Cloud Foundation: Consolidated Architecture Deployment 4.0 on Dell EMC VxRail - Technical Overview (Page 24) https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/vcf/tech-overview/vmware-cloud-foundation-consolidated-architecture-dell-emc-vxrail.pdf

VMware Cloud Foundation Administration Guide https://docs.vmware.com/en/VMware-Cloud-Foundation/index.html

Question: 4

Which two options can be used to create a new VMware Cloud Foundation VI workload domain? (Choose two.)

A. SDDC Manager UI

B. PowerCLI

C. Cloud Builder UI

D. vCenter UI

E. REST API

Answer: AE

Explanation:

The SDDC Manager UI provides a single point of control for managing and monitoring your VMware Cloud Foundation instance and for provisioning workload domains. You use the navigation bar to move between the main areas of the user interface 1. The SDDC Manager UI provides an integrated view of the physical and virtual infrastructure and centralized access to manage the physical and logical resources 2.

The REST API can also be used to create a new VI workload domain using VMware Cloud Foundation. The VMware Cloud Foundation API Reference Guide provides information on available operations 3.

Question: 5

What is a valid procedure to replace an expired vSAN license in a VMware Cloud Foundation environment?

A.

1 Add a new vSAN license to the SDDC Manager and vCenter Server.

2. Reassign the vSAN license to the cluster in the vCenter Server.

3. Remove the expired vSAN license from the SDDC Manager and vCenter Server.

B.

1 Add a new vSAN license to the SDDC Manager.

2. Connect to SDDC Manager via SSH, and then restart Domain Manager using systemctl restart domainmanager. 3 Verify in the SDDC Manager whether a new vSAN license has been assigned to the cluster.

C.

1 Add a new vSAN license to the vCenter Server.

2. Connect to SDDC Manager via SSH, and then restart Lifecycle Management using systemctl restart lcm.

3. Verify in the vCenter Server whether a new vSAN license has been assigned to the cluster.

D.

1 Add a new vSAN license to the SDDC Manager.

2. Reassign the vSAN license to the cluster in the SDDC Manager.

3. Remove the expired vSAN license from the SDDC Manager

Answer: A

Explanation:

a valid procedure to replace an expired vSAN license in a VMware Cloud Foundation environment is Option A. You can add a new vSAN license to both the SDDC Manager and vCenter Server. Then reassign the vSAN license to the cluster in the vCenter Server 1. Finally, remove the expired vSAN license from both SDDC Manager and vCenter Server 2.

https://my-cloudy-world.com/2022/06/28/updating-a-vsan-license-in-vmware-cloud-foundation/