Vendor: VMware

Exam Code: 2V0-15.25

Exam Name: VMware Cloud Foundation 9.0 Support

Version: DEMO

QUESTION 1
An administrator has been tasked with deploying a new workload domain consisting of six VMware ESX hosts with VMware vSAN into an existing VMware

Cloud Foundation (VCF) instance. After starting the deployment from VCF Operations, they discover that only four of the six hosts required are listed for selection in the UI. The administrator checks the Unassigned Host Inventory view in the vSphere Client and confirms that all six hosts are listed.

Which step should the administrator perform to identify why the two hosts are not available for selection?

A. Check that the management port group on the standard switch has been enabled for vSAN traffic.
B. Check that the failures to tolerate (FTT) setting for the workload domain is set to 0.
C. Check that all disk partitions have been deleted from the SSD drives of the hosts.
D. Check that the network pool the hosts have been associated with is enabled for vSAN.

Answer: D
Explanation:
When deploying a new workload domain in VMware Cloud Foundation (VCF), only ESXi hosts that fully meet all pre-requisites are displayed in the VCF Operations UI for selection. Although all six hosts appear in the Unassigned Host Inventory in vCenter, VCF performs additional validation before making them selectable for workload domain deployment.

One of the mandatory requirements for any vSAN-enabled workload domain is that the ESXi hosts must be associated with a Network Pool configured for vSAN traffic. A network pool defines the host network configuration (VLANs, MTU, NIC mapping) used during domain deployment.

If the two missing hosts are associated with a network pool that does not have vSAN traffic enabled, or are associated with no network pool at all, VCF will exclude them from the workload domain deployment wizard. This is documented behavior: VCF filters out hosts when required network intents--such as vSAN--are not present.

QUESTION 2
A VMware NSX Edge node is present in the inventory but shows "Not Ready" status In NSX Manager UI. What should the administrator check first?

A. The NSX Edge has been added to an Edge cluster
B. The license key in NSX Manager UI
C. The NSX Edge node's uplink network configuration
D. The NSX Edge node's CPU reservation

Answer: C
Explanation:
The status "Node Not Ready" in the NSX Manager UI (specifically in the Configuration State column of the Edge Transport Nodes view) indicates that the NSX Manager has failed to push or validate the necessary configuration to the Edge VM.

Check Uplink Network Configuration (Option C): This is the most common cause for a "Node Not Ready" state during deployment or operation. For an Edge Node to be "Ready" (Success/Up), it must have a valid Transport Node configuration, which includes the Uplink Profile, IP Pool (for TEPs), and mapping to the Fastpath Interfaces (N-VDS). If the uplink configuration is missing, incorrect, or the management plane cannot communicate with the edge to apply it, the node remains in a "Not Ready" state.

QUESTION 3
An administrator is asked to create a second provider gateway (provider gateway 02) in VMware Cloud Foundation (VCF) Automation Region-A.

After launching the Create Provider Gateway workflow in the VCF Automation Provider Management Portal, no Tier-0 Gateway is available for assignment.

How would you resolve this issue?

A. Create a new Region.
B. Log into the NSX Manager, create a new Tier-1 Gateway.
C. Log into the NSX Manager, create a new TO Gateway.
D. Retry the Create Provider Gateway workflow.

Answer: C
Explanation:
In VMware Cloud Foundation 9.0, a Provider Gateway in VCF Automation is always backed by an existing Tier-0 or Tier-0 VRF gateway in NSX. When the administrator launches the Create Provider Gateway workflow and no Tier-0 gateways appear for assignment, this indicates that VCF Automation cannot discover any valid Tier-0 gateways in the associated region.

The VMware Cloud Foundation 9.0 documentation explicitly states that before adding a Provider Gateway, an administrator must first create an Active-Standby Tier-0 Gateway in NSX Manager. The Provider Gateway workflow only lists Tier-0 gateways that already exist and are properly configured in NSX. If none are present, the list will be empty.

From the documentation: "To add a provider gateway, first you must create an Active Standby tier-0 gateway in the NSX Manager associated with the region to back it." . Provider gateways in VCF Automation are discovered from these preexisting Tier-0 gateways and cannot be created until they exist.

Creating a Tier-1 gateway (Option B) does not satisfy the requirement because Provider Gateways must map specifically to Tier-0, not Tier-1. Retrying the workflow (Option D) will not resolve the issue because the Tier-0 backing resource is missing. Creating a new region (Option A) is unnecessary unless required for other organizational reasons, and it still would not produce a Tier-0 gateway.

Therefore, the correct and verified solution is to log in to NSX Manager and create the required Tier-0 gateway, after which it will appear in the Provider Gateway creation workflow.

QUESTION 4
An administrator is troubleshooting an issue relating to VMware Cloud Foundation (VCF) Automation. While troubleshooting, the administrator realizes that debug-level information is not displayed in the VCF Automation Task Log.

How would the Administrator enable debug-level information in the Task Log?

A. Enable "display debug information" in the Administer > Settings section of the Organization Management portal.
B. Enable "display debug information" in the Administration > Feature Flag section of the Provider Management portal.
C. Enable "display debug information" in the Administration > Events and Tasks section of the

Provider Management portal.

D. Enable "display debug information" in the Administration > General Settings section of the Provider Management portal.

Answer: B
Explanation:
In VMware Cloud Foundation (VCF) 9.0 Automation, the visibility of debug-level information in Task Logs is controlled centrally by the Provider Administrator through the Provider Management portal. Debug logging is not enabled by default because it exposes verbose operational details intended primarily for troubleshooting. According to the VCF Automation architecture and operations model, advanced logging capabilities--including debug output--are gated behind feature flags.

To enable debug-level information, the Provider Admin must navigate to:

Provider Management Administration Feature Flags Display Debug Information

Once this flag is enabled, the system begins emitting additional diagnostic detail into Task Logs, improving insight into failures, orchestration flows, API calls, and service-to-service interactions. This aligns with VCF's multi-tenant design, where only the Provider tier has permission to modify global settings that affect all Organizations.

QUESTION 5
An administrator is preparing to import a vSphere environment into VMware Cloud Foundation (VCF) as a workload domain. The vSphere environment has the following configuration:

```
- vSphere version 8.0 update 3.
- Three-node vSAN cluster with a single OSA datastore.
- Two vSphere Distributed Switches (VDS).
- Three vmkernel adapters with DHCP assigned IP addresses.
```

What change must the administrator make before importing this environment?

A. Consolidate to a single vSphere Distributed Switch.
B. Upgrade vCenter and ESXi to vSphere 9.0.
C. Update the vmkernel adapters with statically assigned IPs.
D. Convert the vSAN datastore from OSA to ESA.

Answer: C
Explanation:
When importing an existing vSphere environment into VMware Cloud Foundation (VCF) as a workload domain, several strict prerequisites must be met. One of the key requirements documented in VCF 9.0 is that all VMkernel adapters (vmk ports) used for vSAN, vMotion, management, or other system traffic must have statically assigned IP addresses. DHCP-assigned VMkernel IPs are not supported for VCF workload domain bring-up or import operations.

In the provided scenario, the environment includes:

vSphere 8.0 U3
A 3-node vSAN OSA cluster
Two VDS switches
VMkernel adapters using DHCP

Before VCF can successfully validate and import the environment, the administrator must convert

these VMkernel interfaces to static IP addressing. VCF uses IPAM assumptions and deterministic host networking configurations; DHCP introduces variability incompatible with automated lifecycle operations.

QUESTION 6
An administrator has successfully created a new Organization for All Apps In VMware Cloud Foundation (VCF) Automation. When logging into the new organization using the first user account, only the Overview tab is visible.

What is a possible cause of this issue?

A. The first user account was assigned the Organization Auditor Role.
B. The first user account was assigned the Organization User Role.
C. The first user account was assigned a Custom Role.
D. The first user account was assigned the Organization Administrator Role.

Answer: B
Explanation:
This issue stems from an incorrect role assignment during the user creation process in VMware Cloud Director (VCF Automation).

Organization User Role (Option B): This is a consumer-level role designed for deploying and managing vApps. By default, this role does not have access to the Administration tab or high-level organization settings. If the organization is new and has no vApps or VDCs populated yet, a user with this role might see a very restricted view (effectively just a dashboard or "Overview") because they lack the rights to see the administrative configuration menus.

QUESTION 7
An administrator discovers that a VMware Cloud Foundation (VCF) workload domain four-node vSAN cluster is experiencing a network partition. The workload domain vCenter displays a "vSAN duster partition" warning. The performance across the cluster is degraded and the objects are showing as non-compliant.

What could be causing the network partition?

A. IGMP snooping is disabled on the multicast group.
B. The VLAN was changed on the physical switch port.
C. Jumbo frames are configured on the vSphere distributed switch (VDS).
D. The vSAN Witness service was added to the vMotion network.

Answer: B
Explanation:
A vSAN cluster network partition occurs when vSAN nodes cannot communicate over the designated vSAN network. In VMware Cloud Foundation workload domains, the vSAN network relies on L2 adjacency, consistent VLAN configuration, and stable multicast/BUM behavior (in older versions). VCF 9.0 uses unicast-mode vSAN, so multicast-related issues (such as IGMP snooping configuration) are no longer relevant.

A network partition can occur when the VLAN ID on the physical switch port differs from the VLAN configured on the vSphere Distributed Switch (VDS) for the vSAN VMkernel adapters. The documentation emphasizes that consistent VLAN configuration across the physical and virtual network is required for proper vSAN cluster communication. If a switch port is reconfigured--intentionally or accidentally--to use a different VLAN, the node becomes isolated from the rest of

the vSAN cluster, causing:

"vSAN cluster partition" warnings in vCenter
degraded performance
objects marked as non-compliant
resyncs that cannot complete

QUESTION 8
After upgrading from VMware Cloud Foundation (VCF) 5.2 to VMware Cloud Foundation (VCF) 9.0 the administrator attempts to enable SSH access through the vCenter console to the newly upgraded VCF Ops instance and Is not able to. They attempt to log in through SSH as the root user and they are unable to. What needs to be done to enable SSH access to the VCF Ops instance?

A. Reset the root password.
B. Reboot the appliance and enable SSH.
C. Rollback to snapshot because the upgrade did not work as expected.
D. Use VCF Operations to remediate the password

Answer: D
Explanation:
In VMware Cloud Foundation (VCF) 9.0, the management of appliance credentials and lifecycle operations is centralized within the VCF Operations Fleet Manager (which subsumes the roles of the legacy SDDC Manager Life Cycle Management).

The Problem: The administrator is unable to log in as root via the console or SSH. This indicates a credential synchronization issue or account lockout, which prevents them from manually enabling SSH via the console (the traditional method).

The Solution (Remediate Password): The "Remediate Password" workflow in VCF Operations allows the administrator to reset and synchronize the root password for VCF components (like the VCF Ops instance itself) directly from the management plane.

By navigating to Fleet Management > Passwords (or similar path in VCF 9.0), the administrator can select the affected instance and choose Remediate.

This process updates the password in the centralized database and on the appliance, restoring the ability to log in.

Once the root access is restored via remediation, the administrator can then proceed to enable SSH (either via the VCF Operations settings UI or the console). Without the correct password (which "Remediate" fixes), SSH cannot be enabled.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**