



VMware VCP VMware Cloud Foundation Support 2V0-15.25 Practice Questions

Shared by Hardin on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

An administrator configures a new VMware Cloud Foundation (VCF) instance in a remote site using a vSAN Express Storage Architecture (ESA) for the workload domain cluster. vSAN ESA is configured with Auto-Policy Management and is designed to tolerate a single failure. The cluster experiences a hardware failure and on investigation, the administrator discovers that the affected objects did not re-protect and remain in a "Reduced availability with no rebuild" state.

How can the administrator explain why the vSAN objects did not rebuild as expected?

Options:

- A- The storage devices are not certified for vSAN.
- B- The number of ESX hosts doesn't support rebuilds during an outage.
- C- The storage policy needs to be modified to support forced provisioning.
- D- The existing disk groups need to be expanded to support additional capacity.

Answer:

B

Explanation:

In VMware Cloud Foundation 9.0, using vSAN Express Storage Architecture (ESA) with Auto-Policy Management, the system automatically selects the correct storage policy based on the cluster size and desired failure protection. When the administrator configures tolerance for a single failure (FTT=1 using RAID-1 mirroring), vSAN ESA requires sufficient remaining hosts during a failure event to reprotect objects.

A minimum of 3 ESA-capable hosts is required for RAID-1, and re-protection after a failure requires enough hosts with available capacity to place new replica components. In small ESA clusters (e.g., 3 or 4 nodes), if one host fails, the remaining hosts may not meet the placement rules for automatic rebuild to restore compliance. ESA enforces strict placement rules to maintain consistent performance and resilience; if vSAN determines that object layout compliance cannot be restored without violating these rules, it enters Reduced availability with no rebuild state.

This behavior is expected and documented: rebuilds cannot occur if the cluster does not have sufficient hosts or free capacity to recreate absent components. The administrator's ESA configuration behaved correctly given the cluster size limitation, making B the correct answer.

Question 2

Question Type: MultipleChoice

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?

Options:

- 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.

Options A, C, and D are incorrect because Organization-level settings do not control system-wide logging, and the Events/Tasks or General Settings sections do not contain the mechanism for enabling debug output. Only the Feature Flag section controls this capability.

Question 3

Question Type: MultipleChoice

An administrator has observed that the vSphere Global Inventory is only available from the management domain vCenter. The Global Inventory is not available from the workload domain's vCenter.

Why is the "Global Inventory" missing from the workload domain's vCenter?

Options:

- A- VCF SSO and vCenter Linking have not been configured.
- B- Supervisor Management has not been enabled.
- C- An inventory sync was not run following the workload domain creation.
- D- An external VIDB instance has not been configured.

Answer:

A

Explanation:

The Global Inventory List (GIL) is only available when multi-vCenter SSO domain linking is configured. In VMware Cloud Foundation, the management domain vCenter is deployed first and becomes the root vCenter for global inventory data. For workload domains, their vCenter Servers must be registered into the same SSO domain and linked with the management-domain vCenter in order for the global inventory data (VMs, hosts, clusters, content libraries) to appear.

If a workload domain vCenter is not SSO-linked, it operates in its own identity domain, and therefore cannot access or present Global Inventory, resulting in exactly the symptom described: the management domain vCenter shows the GIL, while the workload domain vCenter does not.

Option B (Supervisor Management) relates to vSphere with Tanzu and has no impact on Global Inventory. Option C (inventory sync) is incorrect---there is no manual sync required; GIL relies entirely on SSO linking. Option D (VIDB) is not related to vCenter linking or inventory visibility; it is used by VCF Identity Broker.

Therefore, the reason the Global Inventory is missing from the workload domain vCenter is that SSO/vCenter Linking has not been configured, which is required for federation across all VCF vCenters.

Question 4

Question Type: MultipleChoice

An administrator has identified that the VMware NSX Admin account is locked out. The administrator is unable to login to the NSX Manager UI using this account.

How could the administrator resolve this issue?

Options:

- A- SSH into NSX Manager as Admin and remove API and CLI password lockouts.
- B- Login into vCenter and increasing the password age policy.
- C- Login to SDDC Manager and rotate admin account password.
- D- Console into NSX Manager as root and clear API and CLI password lockouts.

Answer:

D

Explanation:

When an NSX Admin account becomes locked in NSX Manager, this occurs due to failed login attempts exceeding the lockout threshold for either:

CLI access,

API access, or

UI login, which is tied to API authentication.

Once locked, the only supported method to recover the NSX admin account is to log in to the NSX Manager console as the root user and manually clear the lockout counters. This is documented in NSX Manager password-recovery procedures and is the standard administrative recovery action.

The root console provides access to:

clear account-lockout admin

or the equivalent reset methods within NSX Manager.

Why the other options are incorrect:

A. SSH into NSX Manager as Admin Impossible --- the admin account is locked and cannot be used to SSH.

B. Change password age policy in vCenter NSX Manager accounts are not governed by vCenter

password policy.

C. Rotate admin password in SDDC Manager SDDC Manager rotates NSX passwords when unlocked; it cannot unlock a locked account.

Question 5

Question Type: MultipleChoice

An administrator is responsible for managing a remote VMware Cloud Foundation (VCF) fleet with the following configuration:

- * A single VCF instance with a single Workload Domain.
- * The Workload Domain has a single VMware vSAN Express Storage Architecture (ESA) cluster.
- * VCF is licensed using the disconnected mode.

The administrator discovers a notification in VCF Operations showing that the VCF licenses have expired. Which three steps should the administrator take to resolve the issue? (Choose three.)

Options:

- A- Increase the license core count in SDDC Manager.
- B- Restart SDDC Lifecycle Manager Service in the VCF Operations console.
- C- Export the usage file from VCF Operations and upload to the VCF Business Services console.
- D- Use the VCF Business Services console to export a new VCF license file.
- E- Import the license file into VCF Operations and assign to the workload domain vCenter.
- F- Import the license file into VCF Operations and assign to the SDDC Manager.

Answer:

C, D, F

Explanation:

In VMware Cloud Foundation (VCF) 9.0 using disconnected mode licensing, VCF Operations does not automatically synchronize license status with VMware's cloud services. Instead, the administrator must periodically refresh the license file using a manual offline workflow. When the VCF Operations console reports that licenses have expired, it means the license entitlement in the VCF Business Services portal is out of date, and therefore VCF Operations cannot validate the current usage.

The VMware-documented offline licensing workflow requires the following steps:

Export the usage file from VCF Operations. This usage file contains consumption details needed to generate a new offline license. C is correct.

Upload the usage file to the VCF Business Services console and generate a new offline license file. In disconnected mode, the Business Services portal is the only mechanism to create updated license entitlements. D is correct.

Import the updated VCF license file into VCF Operations, specifically assigning it to the SDDC Manager. SDDC Manager is the system that validates and enforces licensing across workload domains, so the new license must be applied there---not only to a vCenter. F is correct.

Options A and B do not affect license validation. Option E is incorrect because workload-domain vCenter licensing is independent and not the root cause of VCF license expiration.

Question 6

Question Type: MultipleChoice

An administrator logs into the VMware NSX Manage UI and observes a "Remote Logging Not Configured" alarm for each NSX Management node. What is a possible reason for this issue?

Options:

- A- Update the NSX Edge Cluster Profile to configure a remote logging server.
- B- Update the NSX Uplink Profile to configure a remote logging server.
- C- Update the NSX Node Profile to configure a remote logging server.
- D- Update the NSX Configuration Profile to configure a remote logging server.

Answer:

C

Explanation:

The 'Remote Logging Not Configured' alarm in NSX Manager is a system-health alert indicating that one or more Transport Nodes (Edges or Hypervisors) or Management Nodes do not have a Syslog server defined.

NSX Node Profiles: In VMware NSX (and by extension VCF), the standard method to apply consistent administrative settings---such as Syslog Servers, NTP settings, and Core Dump configurations---across a fleet of nodes is to use an NSX Node Profile.

Configuration Path: The administrator should navigate to System > Fabric > Profiles > Node Profiles. Here, they can create or edit a profile that specifies the remote syslog server's IP/FQDN, port, and protocol.

Application: Once the Node Profile is applied to the NSX Management Cluster or Edge Clusters, the configuration is pushed to all respective appliances, clearing the alarm.

Why not A/B: Edge Cluster Profiles manage networking/BFD settings; Uplink Profiles manage NIC teaming and MTU.

Question 7

Question Type: MultipleChoice

An administrator is creating a new workload domain from VMware Cloud Foundation (VCF) Operations. They are blocked at the Hosts selection screen as no ESX hosts are available. They see the following message:

"No suitable hosts available to create a VI workload domain. Hosts must be unassigned, commissioned with at least one physical NIC and the same storage type as the VI workload domain, and the ESX version must be compatible with the lowest ESX version present in the management domain."

How can the administrator commission new hosts to enable the creation of the VI workload domain?

Options:

- A- Using the Cloud Builder.
- B- Using the vSphere client.
- C- Using the VCF Installer.
- D- Using VCF Operations.

Answer:

D

Explanation:

In VMware Cloud Foundation 9.0, all host commissioning operations are performed through VCF Operations, not through vSphere Client, Cloud Builder, or the VCF Installer. Once VCF is deployed, Cloud Builder is no longer used, and the VCF Installer is for lifecycle and bundle management--not for host workflows. The vSphere Client also cannot commission hosts

because host commissioning is a foundational VCF workflow requiring hardware validation, storage type checks, NIC checks, HCL conformance, and version compatibility.

The error message provided:

"Hosts must be unassigned, commissioned with at least one physical NIC and the same storage type... and the ESX version must be compatible..."

is a standard VCF 9.0 validation message shown when no commissioned hosts matching the workload domain requirements exist. VMware documentation states that hosts must be commissioned under:

VCF Operations Fleet Management Hosts Commission Host

Here, VCF validates:

Storage type (vSAN ESA, vSAN OSA, NFS, FC, etc.)

Network pool membership (matching the WLD plan)

ESXi version compatibility with the Management Domain baseline

NIC mapping and certifications

Until hosts are commissioned, they cannot appear in the workload domain creation wizard.

Thus, the correct method to commission hosts is D. Using VCF Operations.

Question 8

Question Type: MultipleChoice

A VMware Cloud Foundation (VCF) administrator cannot deploy Virtual Machines (VMs) to a compute cluster.

The administrator discovers that the vCLS VMs on the problematic cluster are powered off and cannot be powered on.

What action can the administrator take to enable deployment of VMs?

Options:

- A- Delete all resource pools in the affected cluster.
- B- Disable HA on the affected cluster.
- C- Enable retreat mode on the affected cluster.
- D- Set DRS Automation level to fully automated.

Answer:

C

Explanation:

In vSphere 7+ and VCF-managed clusters, the vSphere Cluster Services (vCLS) VMs must remain powered on for DRS, cluster health, and policy enforcement to function. If the vCLS VMs cannot power on, no workloads—including new VMs—can be deployed to the cluster because vSphere considers the cluster unhealthy.

A common cause is insufficient **resources** (CPU/memory), **datastore** issues, or policy conflicts preventing vCLS VMs from starting. VMware provides Retreat Mode as a troubleshooting mechanism to temporarily disable vCLS, allowing the administrator to deploy VMs and correct underlying issues. Enabling retreat mode:

Removes vCLS from the cluster

Restores ability to deploy VMs

Allows remediation of storage/placement issues

Can later be disabled to restore DRS health

Option A (deleting resource pools) does not restore vCLS VM power state. Option B (disabling HA) does not affect vCLS behavior. Option D (setting DRS automation level) does not correct vCLS placement problems.

Question 9

Question Type: MultipleChoice

An administrator is planning to apply updates to a VMware vCenter instance.

What two actions can the administrator take to confirm the status of the vCenter services? (Select two.)

Options:

- A- Connect to the vSphere Client and review vCenter performance charts.
- B- Connect to the vCenter appliance shell and run the services-control -status command.
- C- Connect to the vCenter Server Management console and review the services statuses.
- D- Connect to the vCenter appliance shell and run the vim-top command.
- E- Connect to the ESX DCUI where the vCenter Appliance is running and run the services.sh

script.

Answer:

B, C

Explanation:

Before applying updates to a vCenter Server Appliance (VCSA), an administrator must validate that all vCenter services are healthy. VMware provides two supported and documented methods for checking vCenter service status:

1. Using the vCenter Appliance Shell

Running the command:

```
services-control --status
```

This command displays the status of all vCenter-related services (vmdird, vmcad, vpxd, vsan-health, etc.). It is the authoritative diagnostic tool embedded in the appliance for confirming whether services are running, stopped, or in a degraded state. This method is explicitly documented in vSphere 9.0 service management procedures.

This matches Option B.

2. Using the vCenter Server Management Interface (VAMI)

Accessed at:

```
https://<vcenter-fqdn>:5480
```

The VAMI console provides a graphical interface under Services, showing the real-time health, status, and start/stop controls for all vCenter services. VMware documentation instructs administrators to review service status here before performing upgrades or maintenance operations.

This matches Option C.

Incorrect Options Explained

A . vSphere performance charts These show workload data, not service health.

D . vim-top command Displays vSphere hosts' runtime metrics, not vCenter services.

E . Running services.sh on ESXi DCUI vCenter does not run ESXi services; this script is for ESXi hosts only.

Question 10

Question Type: MultipleChoice

An administrator logs into the VMware NSX Manager UI and discovers a time sync issue that has been reported in the VMWare Cloud Foundation (VCF) installer.

The administrator performs the following steps:

1. Validates that the NTP server IP addresses are present in the NTP configuration on the VCF Installer.
2. Validates that the DNS records are correctly set for the FQDN and IP address of the two NTP servers.
3. Validates that the NTP servers can be pinged by name and IP address from the VCF Installer.
4. Validates that the time between the NTP servers and the VCF Installer is synchronized successfully.

What additional step should the administrator perform to help identify the cause of the error?

Options:

- A- Confirm that the ESX hosts have been configured to use host time synchronization.
- B- Confirm that the NTP service has an allowed rule in the iptables on the VCF Installer.
- C- Confirm that the NTP server details have been specified in the deployment parameter workbook using the required FQDN format.
- D- Confirm that the time on the ESX hosts allocated for the management domain is synchronized with the same NTP servers as the VCF Installer.

Answer:

D

Explanation:

During VMware Cloud Foundation bring-up, time synchronization across all management components is mandatory. The VCF Installer, ESXi hosts, NSX Manager nodes, and vCenter must all sync to the same NTP servers. If even one host or component has a time skew exceeding VMware's allowed limits, VCF will report time sync errors during bring-up or post-deployment.

The administrator validated NTP configuration, DNS resolution, ping connectivity, and time sync only on the VCF Installer appliance, but did not verify the ESXi hosts' time synchronization. NSX Manager obtains its time reference from the underlying ESXi host during deployment, so if the ESXi hosts are not synchronized with the same NTP sources, NSX Manager will drift,

triggering the exact error described.

Option B (iptables) does not apply---the VCF Installer does not block outbound NTP by default. Option C refers to workbook formatting, which would fail earlier in deployment---not after NSX Manager is running. Option A is incorrect because ESXi should never use "host time sync"; NTP must be used.



To Get Premium Files for 2V0-15.25 Visit

<https://www.p2pexams.com/products/2v0-15.25>

For More Free Questions Visit

<https://www.p2pexams.com/vmware/pdf/2v0-15.25>

20%
DISCOUNT

P2P
exams