KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **2V0-15.25**

Title : VMware Cloud Foundation 9.0 Support

Version : DEMO

1.A user wishes to publish a VMware Cloud Foundation (VCF) Operations Orchestrator workflow to their VCF Automation project catalog, but Is blocked from publishing any workflows.
The following information has been provided:
• In the VCF Automation Organization portal, the user cannot see the Workflows option under Content Hub.
• The organization is not a Provider Consumption Organization.
Which are the two likely causes of this issue? (Choose two.)
A. An external VCF Operations Orchestrator is not integrated with their Organization.
B. The user is logged in with Project User rights.
C. The user is logged in the Project Advanced User rights
D. An embedded VCF Operations Orchestrator is not integrated with their Organization.
E. The user is logged in with Project Administrator rights.
Answer: A, D
Explanation:
In VMware Cloud Foundation 9.0, publishing a VCF Operations Orchestrator workflow to a VCF Automation project catalog requires that the Organization has a valid integration with VCF Operations Orchestrator. The question states that the user cannot see the Workflows option under Content Hub, and the organization is not a Provider Consumption Organization (PCO). According to the VCF 9.0 documentation, only organizations with VCF Operations Orchestrator integration are allowed to publish workflows into the catalog. Both embedded and external orchestrator integrations must be configured depending on the environment. If no orchestrator (embedded or external) is integrated with the organization, workflows cannot be listed or published. This aligns with the documented VCF Automation and VCF Operations Orchestrator design requirements, which specify that workflow publishing is only available when the orchestrator instance is properly registered.
Additionally, user role permission issues could prevent workflow visibility, but the key blockers described in the scenario are the missing workflow section and the organization type. Because the organization is not a PCO, advanced provider features—including workflow publishing—are disabled unless a proper orchestrator integration exists.
Therefore, the two most likely causes are:
A: An external VCF Operations Orchestrator is not integrated with their Organization.
D: An embedded VCF Operations Orchestrator is not integrated with their Organization.
These two conditions directly match the documented behavior in VMware Cloud Foundation 9.0.

2.An administrator wants to expand a VMware vSAN cluster in a workload domain by adding an unassigned host from the vSphere client.
However, at the Host Selection screen no hosts are available and the following message displayed:
No unassigned hosts available with storage type VSAN.
Commission hosts with physical NICs 0 & 1 to Add Host from UI.
How can the administrator commission hosts?
A. From the vSphere client by navigating to Supervisor Management.
B. From VCF Operations by navigating to Fleet Management.
C. From the SDDC manager by navigating to Workload Domains.
D. From the vSphere client by navigating to the Global Inventory.
Answer: C

Explanation:
In VMware Cloud Foundation 9.0, host commissioning is performed exclusively through SDDC Manager, not from the vSphere Client. When expanding a vSAN cluster inside a workload domain, all ESXi hosts must first be placed in an Unassigned state and then commissioned in SDDC Manager before they can appear in the “Add Host” wizard of the vSphere Client. The message in the problem—“No unassigned hosts available with storage type VSAN. Commission hosts with physical NICs 0 & 1 to Add Host from UI”—indicates that SDDC Manager has not yet commissioned any suitable hosts with the required NIC layout.
VCF 9.0 documentation states that for workload domain expansion, hosts must be commissioned under:
SDDC Manager → Workload Domains → (Select WLD) → Hosts → Commission Hosts.
This validates hardware, storage type (such as vSAN ESA or OSA), NIC placement, and ensures the host is compatible with the domain’s configuration.
Options pointing to vSphere Client (A, D) or VCF Operations (B) do not perform the commissioning workflow. Therefore, the correct and verified answer is C, the only interface where host commissioning is officially supported.

3.An administrator is responsible for a VMware Cloud Foundation (VCF) fleet. The administrator has been tasked with commissioning four ESX hosts for a new workload domain that uses vSAN Express Storage Architecture (ESA) as the primary storage solution.
During the host validation stage in vSphere client, the process fails with the following errors:
esx-l.wld.vcf.local. Failed to validate vSAN HCL status.
esx-2.wld.vcf. local. Failed to validate vSAN HCL status.
esx-3.wld.vcf.local. Failed to validate vSAN HCL status.
esx~4.wid.vcf. local. Failed to validate vSAN HCL status.
What Is the cause of the errors?
A. The RAID controller in each ESX host is not configured to use RAID-O/Passthrough.
B. The ESX hosts are not using vSAN ESA certified storage devices.
C. The ESX hosts must have internet access to validate vSAN ESA compatibility.
D. The RAID controller in each ESX host needs to be reconfigured to use Tri-mode.
Answer: B
Explanation:
VMware Cloud Foundation 9.0 requires strict vSAN ESA hardware compatibility when creating a workload domain that uses vSAN Express Storage Architecture (ESA). During host validation, SDDC Manager and vSphere Client check whether each ESXi host meets ESA requirements, including CPU generation, storage controller type, and—most importantly—ESA-certified NVMe storage devices.
The validation errors provided:
“Failed to validate vSAN HCL status” for every host
indicate that the hosts do not meet the vSAN ESA HCL requirements.
VCF 9.0 documentation states that ESA uses a next-generation log-structured filesystem requiring certified NVMe devices only, with no RAID controller dependencies. Unlike OSA, ESA eliminates disk groups, but it requires certified devices listed on the vSAN ESA HCL to pass host validation. If non-certified or unsupported NVMe/SAS devices are present, validation fails exactly as described.
Option A is incorrect because RAID pass-through settings apply to OSA, not ESA.

Option C is incorrect because ESA compatibility validation is performed offline using the SDDC Manager BOM, not via internet lookup.
Option D is incorrect because ESA does not use tri-mode RAID controllers.
Therefore, the documented and verified cause is B: hosts are not using vSAN ESA certified storage devices.

4.An administrator has a vSphere 8.0 update 3 environment with the following configuration:
• A 3-node vSAN cluster
• A vSphere Standard Switch (VSS)
• Several standalone ESX hosts in the vCenter inventory
They want to convert this vSphere environment into a new VMware Cloud Foundation (VCF) 9.0 management domain.
Identify two changes they will need to make before converting this vSphere environment into a VMWare Cloud Foundation (VCF) Management domain? (Choose two.)
A. Remove the vSphere Standard Switch from the vCenter Inventory.
B. Upgrade vSphere 8.0 Update 3 to vSphere 9.0.
C. Configure a vSphere Distributed Switch.
D. Remove the standalone hosts from the vCenter inventory.
Answer: BC
Explanation:
To convert an existing vSphere environment into a VMware Cloud Foundation (VCF) 9.0 Management Domain, several prerequisites must be met as defined in the VCF 9.x documentation.
First, VCF 9.0 requires vSphere 9.0 as part of its Bill of Materials (BOM). The uploaded VCF 9.0 documentation confirms that VCF 9.0 is built on vSphere 9.0, vCenter 9.0, and NSX versions that align with the 9.x stack. A vSphere 8.0 Update 3 environment is not supported as a foundation for a VCF 9.0 management domain; therefore, the administrator must upgrade the entire vSphere platform to vSphere 9.0 before VCF deployment.
(Reference: VCF 9.0 BOM — vSphere 9.0 is mandatory.)
Second, VCF management domain creation strictly requires vSphere Distributed Switches (vDS). VCF does not support vSphere Standard Switches (VSS) for any management domain hosts. The VCF 9.0 design and deployment guides state that all ESXi hosts intended for a management domain must use vDS for management, vSAN, and vMotion networking. Therefore, the existence of a VSS must be corrected by deploying and configuring a vSphere Distributed Switch and migrating host networking accordingly before Cloud Builder deployment.
Removing standalone hosts or removing a VSS from inventory is not required. Only the hosts selected for the management domain need to be prepared.
Thus, the required changes are:
✓ B. Upgrade vSphere 8.0 Update 3 to vSphere 9.0
✓ C. Configure a vSphere Distributed Switch
These are the only changes explicitly required by VCF 9.0 documentation.

5.An administrator determined that the VMware NSX admin password expired on their VMware NSX Edge Transport nodes. The administrator manually resets the password in the console of each Edge Transport node.

What additional action is required to synchronize the new password in VMWare Cloud Foundation (VCF) Operations?

A. In VCF Operations, rotate the admin password for each NSX Edge Transport node.

B. In VCF Operations, remediate the admin password for each NSX Edge Transport node.

C. In VCF Operations, sync the admin password for each NSX Edge Transport node.

D. In VCF Operations, update the admin password for each NSX Edge Transport node.

Answer: B

Explanation:

In VMware Cloud Foundation 9.0, password changes made manually on an NSX Edge Transport Node are not automatically synchronized with VCF Operations. VCF Operations maintains secure credential records for all managed components, including NSX Manager appliances and NSX Edge Transport Nodes. When credentials become stale—such as after a password expiration and manual reset—VCF Operations marks the credential object as out of sync and requires administrative remediation.

The official workflow described in VCF 9.0 Operations documentation states that administrators must use the “Remediate Password” function whenever a password was changed outside of VCF Operations, ensuring that the platform revalidates and updates the stored credentials used for monitoring, log collection, and automation tasks. Options such as “rotate,” “sync,” or “update” do not apply because rotation implies generating a new password managed by VCF, and “sync” does not overwrite the stored credential. Only remediation forces VCF Operations to re-validate and align credentials with the external system.

Therefore, after manually resetting the NSX Edge admin password, the administrator must perform password remediation in VCF Operations to restore operational consistency, making B the correct and verified answer.