

VMware 2V0-17.25

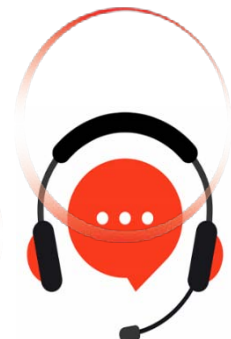
VMware Cloud Foundation 9.0 Administrator

For More Information – Visit link below:

<https://www.examsempire.com/>

Product Version

1. Up to Date products, reliable and verified.
2. Questions and Answers in PDF Format.



<https://examsempire.com/>

Visit us at: <https://www.examsempire.com/2v0-17-25>

Total Questions: 115

Latest Version: 8.5

Question: 1

An administrator is preparing to deploy a new VMware Cloud Foundation (VCF) fleet to an environment that does not have Internet access. Which two binaries must be uploaded to the VCF Installer appliance before initiating the deployment? (Choose two.)

- A. Identity Broker
- B. ESX
- C. NSX
- D. VCF Operations
- E. Lifecycle Manager

Answer: C, D

Explanation:

In VCF 9.x, air-gapped bring-up requires staging the required binaries in the VCF Installer. The documented list explicitly includes NSX and VCF Operations among the components to upload. The product guide states: “VMware Cloud Foundation required binaries include... NSX ... VMware Cloud Foundation Operations ... vCenter ... SDDC Manager...” (exact list excerpt). This list does not call for ESX images or the legacy “Lifecycle Manager.”

Therefore, from the given options the two binaries that must be uploaded are NSX and VCF Operations. ESX is pre-imaged on hosts per preparation guidance and is not a required VCF Installer binary; “Lifecycle Manager” is not used in VCF 9.0 bring-up.

=====

Question: 2

After a migration to VCF 9.0, an administrator must import only logging data newer than 90 days from Aria Operations for Logs 8.x into VCF Operations for Logs. If VCF Operations for Logs has enough space available, what is the correct way to achieve this?

- A. Configure log forwarding in Aria Operations for Logs.
- B. Import logs from an NFS archive used for Aria Operations for Logs.
- C. Initiate the transfer from the Control Panel in VCF Operations.
- D. Initiate the transfer from Aria Operations for Logs.

Answer: C

Explanation:

VCF 9.0 introduces Log Data Transfer initiated from VCF Operations. The docs say: "You can transfer log data for up to 90 days from Aria Operations for Logs 8.x... The migrated logs are stored in VCF Operations for logs." and "To transfer logs... navigate to the Logs Data Transfer card in Administration > Control Panel... click the INITIATE TRANSFER button... You can select the duration of logs to transfer..." (emphasis added).

They further clarify that simple forwarding does not transfer already ingested logs: "Forward logs... does not transfer already ingested logs. Transfer historical logs up to 90 days... using the Log Data Transfer feature in VCF Operations."

Hence, the correct action is to initiate the transfer in VCF Operations (Administration > Control Panel > Logs Data Transfer).

=====

Question: 3

Which tool does an administrator use to collect and validate the initial inputs for the deployment of a VMware Cloud Foundation (VCF) fleet?

- A. SDDC Manager
- B. Cloud Builder
- C. VCF Installer
- D. VCF Operations

Answer: C

Explanation:

VCF 9.0 replaces legacy bring-up tooling with the VCF Installer, which provides a deployment wizard that validates configuration before bring-up. The guide describes: "The deployment wizard validates your inputs... and displays errors and warnings if any." and that administrators "Download and complete the planning and preparation workbook and have the information ready for validating inputs in the deployment wizard."

While the workbook is used to collect information, the validation of those inputs is performed by the VCF Installer wizard prior to deployment. SDDC Manager is used after bring-up for lifecycle operations, and Cloud Builder is not used in VCF 9.0 deployments. Therefore, VCF Installer is the correct tool for collecting (via wizard prompts) and validating initial deployment inputs.

=====

Question: 4

Which two resources can be configured in a VM Class in VMware vSphere with vSphere Supervisor? (Choose two.)

- A. CPU
- B. Memory
- C. Network interface
- D. PCI devices
- E. Storage

Answer: A, B

Explanation:

A VM Class predefines hardware for Supervisor-managed VMs: “The VM class... defines such parameters as the number of virtual CPUs, memory capacity, and reservation settings.” Administration steps show these are configurable: “You can configure hardware resources such as CPU, memory, and different devices” when editing a VM class. Additionally, the DCLI/API specification underscores CPU and Memory fields: “--cpu-count ... Required.” and “--memory-mb ... Required.” for a VM class. While network adapters, PCI devices, and instance storage can also be added via advanced config, the question asks for two; CPU and Memory are canonical, always-present VM Class resources per the core definition above.

=====

Question: 5

An administrator must deploy a new VMware Cloud Foundation (VCF) instance using a supported VCF Operations model with the smallest possible resource footprint. Which VCF Operations deployment model should be used?

- A. Stretched Cluster
- B. Continuous Availability
- C. Simple
- D. High Availability

Answer: C

Explanation:

VCF 9.0 documents two Operations for Logs/Operations models—Simple (Standard) and High Availability (Cluster)—and highlight that Simple is the minimal footprint option intended for test/dev: “Architecture flexibility: Can be deployed in a Simple or Highly Available Cluster deployment. Recommended deployment is a HA Cluster... Simple deployment is for test/dev environments, it is not for production use cases.”

By contrast, HA/clustered models increase resources to provide redundancy at scale. Since the requirement is the smallest resource footprint, the Simple model is the correct selection. (Stretched/Continuous Availability options are not listed VCF Operations models in this context.)

Question: 6

An administrator is tasked to deploy a new vSAN Storage Cluster to an existing VCF instance. The VCF instance is deployed as a single workload domain. What must the administrator do to achieve this without deploying additional management components?

- A. Deploy an additional VCF instance and workload domain with a vSAN storage cluster.
- B. Deploy additional hosts as vSAN storage-only nodes within the existing cluster.
- C. Deploy a second cluster as a vSAN storage cluster in the existing workload domain.
- D. Deploy an additional workload domain with a vSAN storage cluster within the existing VCF instance.

Answer: C

Explanation:

Comprehensive and Detailed

The VCF 9.0 Architecture and Deployment Guide explains that within a single Workload Domain, administrators can scale resources by adding additional clusters, including compute or vSAN storage clusters. Specifically, “A Workload Domain can contain multiple clusters. You can deploy a new cluster, such as a vSAN cluster, into an existing domain without introducing new management components.” .

Options A and D both introduce new workload domains or VCF instances, which require their own management stack (vCenter, NSX Manager, etc.) and are unnecessary in this scenario. Option B is incorrect because “vSAN storage-only nodes” are supported in vSAN but are not the method for adding a new cluster within VCF automation. The correct approach is deploying a second cluster inside the same workload domain—this reuses the existing management components while meeting the requirement for a new vSAN storage cluster.

Question: 7

Which two types of group can be created to collect and manage objects in Istio Service Mesh? (Choose two.)

- A. Security
- B. Cluster
- C. Service
- D. API
- E. Node

Answer: B, C

Explanation:

Comprehensive and Detailed

The Istio integration in VCF 9.0 defines two main logical groupings for organizing workloads within a service mesh: Cluster groups and Service groups. The documentation notes: "Cluster groups allow you to organize and manage objects across different Kubernetes clusters. Service groups let you aggregate and manage services that share common policies, routing rules, or observability requirements."

These groups enable administrators to apply consistent service mesh policies across multiple deployments and clusters. They also simplify administration by centralizing traffic management, routing, and observability of workloads. Security, API, and Node are not Istio-specific grouping constructs but instead are other concepts used elsewhere (e.g., security policies, API endpoints, node objects in Kubernetes). Therefore, the correct group types used in Istio Service Mesh are Cluster and Service groups.

Question: 8

An administrator must configure a new Project in the Development tenant of VCF Automation. The requirement is to minimize ongoing management overhead as new developers onboard. Which four steps should be taken? (Choose four.)

- A. Log in to the Development tenant as a Project Administrator.
- B. Assign at least one Cloud Zone to the Project.
- C. Assign both Project Administrators and Project Members to the Project using Active Directory Users.
- D. Create a new Project.
- E. Assign at least one Namespace to the Project.
- F. Log in to the Development tenant as an Organization Administrator.
- G. Assign both Project Administrators and Project Members to the Project using Active Directory Groups.

Answer: A, B, D, G

Explanation:

Comprehensive and Detailed

According to the VCF Automation 9.0 Guide, project creation requires administrative login at the tenant level: "To create a new project, log in as a Project Administrator of that tenant." After creation, projects must be mapped to Cloud Zones to determine compute placement. The document also emphasizes: "For scalable user management, assign groups from Active Directory to roles within projects rather than individual users." This reduces management overhead as new members join.

Namespaces are not mandatory unless Kubernetes Supervisor is being integrated, which is not required in this scenario. Likewise, logging in as an Organization Administrator (F) is not needed for tenant-level project creation. Therefore, the correct steps are: Log in as Project Admin (A), Create a Project (D), Assign a Cloud Zone (B), and Use Active Directory Groups for membership (G). This ensures minimal ongoing administrative effort.

Question: 9

During creation of a new Organization for All Applications in VCF Automation, which four NSX constructs are automatically configured at the regional networking step? (Choose four.)

- A. A Default Virtual Private Cloud (VPC)
- B. A Provider Tier-0 Gateway
- C. An outbound Destination Network Address Translation (DNAT) rule
- D. An NSX Transit Gateway
- E. An outbound Source Network Address Translation (SNAT) rule
- F. A Virtual Distributed Switch (VDS)
- G. A Virtual Private Cloud (VPC) connectivity profile

Answer: A, B, E, G

Explanation:

Comprehensive and Detailed

The VCF Automation Networking Guide (9.0) documents that when an Organization for All Applications is created, networking constructs are provisioned automatically to provide immediate connectivity. Specifically, “During region creation, the system automatically deploys a Default VPC, a Provider Tier-0 Gateway, a VPC connectivity profile, and default SNAT rules to enable outbound access.” .

DNAT rules are not provisioned by default (they must be configured for inbound services). Likewise, NSX Transit Gateway is a multi-region design element, not automatically deployed for a single org setup. A VDS is a vSphere construct and not part of the NSX automation performed at this stage. Therefore, the automatically created items are: Default VPC (A), Provider Tier-0 Gateway (B), SNAT rule (E), and VPC Connectivity Profile (G).

Question: 10

An administrator creates a custom alert in VCF Operations for a VM with a symptom definition: “Read Latency > 1 ms.” The alert should trigger immediately once the symptom condition occurs. What additional step is required to ensure the alert functions?

- A. Enable the alert in an Active Policy.
- B. Create a new Payload Template.

- C. Create an instance of the REST Notification Plugin.
- D. Create and enable a super metric for read latency in the Active Policy.

Answer: A

Explanation:

Comprehensive and Detailed

The VCF Operations 9.0 Monitoring Guide specifies: “For any alert definition to be active in the environment, it must be associated with and enabled in an Active Policy.” . Creating symptom and alert definitions only defines conditions; they do not generate alerts until policies include them. REST notification plugins or payload templates are used for outbound integrations, not for enabling alerts. A super metric is only needed for custom composite KPIs, not for native read latency which is a standard metric already available. Therefore, the required step is to enable the alert in an Active Policy so that when the symptom triggers (latency > 1 ms), the alert activates.

Question: 11

A large corporation recently experienced a power outage at one of its primary data centers resulting in service disruption for customers in that region. An administrator is tasked to assess the current infrastructure and propose a plan to improve resiliency.

Current configuration:

Single-site vSAN Express Storage Architecture (ESA) cluster

12 hosts

Cluster resource utilization (CPU, memory, and storage) is under 30%

Which solution would improve resiliency and minimize service disruption in data center outages with a recovery point objective (RPO) of zero without requiring additional hosts?

- A. Relocate six ESX hosts to another data center and configure a vSAN Stretched Cluster.
- B. Deploy VMware Live Recovery to maintain an identical copy in a secondary site.
- C. Convert existing production workload to a 2 failures – RAID-1 storage policy.
- D. Configure the twelve ESX hosts into six fault domains.

Answer: A

Explanation:

The VCF 9.0 Design Guide highlights that for resiliency across sites with RPO = 0, the recommended approach is a vSAN Stretched Cluster. Documentation states: “Stretched clusters provide site-level resilience by mirroring data across two fault domains (sites). In the event of a full site outage, workloads remain available with no data loss (RPO = 0).” Relocating six hosts to another site creates the two fault domains required for vSAN Stretched Cluster. Options B and C provide backup or redundancy but not synchronous replication with zero RPO. Option D (fault domains) protects against host/rack failures, not entire data center loss. Therefore, the correct solution is to relocate hosts and configure a stretched cluster.

Question: 12

An organization wants to enable Service and Application Discovery across their VMware Cloud Foundation (VCF) fleet. Which optional VMware Cloud Foundation (VCF) solution must the administrator enable or deploy to facilitate this capability?

- A. vSphere Supervisor
- B. VCF Operations for Logs
- C. VCF Operations Collector
- D. VCF Operations for Networks

Answer: D

Explanation:

The VCF Operations for Networks (formerly vRNI) enables Application Discovery and Network Visibility. According to VCF 9.0: "Operations for Networks provides flow-based application discovery, dependency mapping, and security planning. This allows administrators to visualize application topology and relationships across the VCF fleet." By contrast, VCF Operations for Logs provides log aggregation, while the Collector provides integration for metrics, not discovery. The vSphere Supervisor enables Kubernetes workloads, not application discovery. Therefore, to achieve Service and Application Discovery, administrators must deploy VCF Operations for Networks.

Question: 13

An administrator is responsible for monitoring VMware vSAN performance across a VMware Cloud Foundation (VCF) instance. The administrator confirms VCF Operations is configured correctly. When viewing Storage Operations, the vSAN Cluster Performance widget is not displaying any data. What additional configuration should the administrator complete to ensure the widget displays data?

- A. Enable Support Insight for all vSAN Clusters in vCenter.
- B. Select a Cloud proxy as Collector in the vSAN integration.
- C. Select "Enable SMART data collection" in the vCenter integration.
- D. Enable Performance Service for all vSAN Clusters in vCenter.

Answer: D

Explanation:

According to the VCF 9.0 Operations and vSAN Integration Guide, performance metrics in the vSAN Cluster Performance widget are only available when the vSAN Performance Service is enabled. The documentation states:

“The vSAN Performance Service must be enabled in vCenter Server for each vSAN cluster to collect and visualize performance statistics in VCF Operations. Without this service, performance dashboards and widgets will not display data.”

Option A (Support Insight) relates to telemetry with VMware, not performance widgets.

Option B (Cloud proxy as Collector) is required for general collection but not specific to vSAN widget visibility.

Option C (SMART data collection) provides disk health analytics, not cluster-level performance stats.

Option D is correct, because enabling the vSAN Performance Service ensures that VCF Operations receives and displays data in the vSAN Performance dashboards.

Therefore, the administrator must enable the vSAN Performance Service for all vSAN clusters in vCenter.

Question: 14

An administrator is tasked to configure network connectivity to the organization's corporate network for their container workloads to be deployed on VMware Kubernetes Service (VKS) clusters backed by VMware NSX networking on a new VMware Cloud Foundation (VCF) deployment. Which gateway connectivity type should the administrator deploy?

- A. Round-robin Connectivity
- B. Distributed Connectivity
- C. Physical Connectivity
- D. Centralized Connectivity

Answer: D

Explanation:

The VMware Cloud Foundation 9.0 networking design documentation specifies that container workloads running on VMware Kubernetes Service (VKS) with NSX networking require external connectivity via a Centralized Connectivity model. This is implemented using an NSX Tier-0 (T0) Gateway which provides north-south routing to the corporate physical network.

The guide states: “In VKS deployments backed by NSX networking, workloads achieve external reachability through a centralized Tier-0 Gateway, ensuring integration with corporate networking and enterprise services.” This model ensures traffic consolidation, policy enforcement, and simplified routing for Kubernetes workloads.

Round-robin Connectivity is not a supported NSX gateway connectivity model.

Distributed Connectivity refers to east-west NSX overlay communication, not north-south connectivity.

Physical Connectivity is not precise, as workloads do not connect directly to the physical network; instead, they use logical routing.

Centralized Connectivity is the correct model, where the T0 Gateway centralizes external routing for container workloads.

Question: 15

What is the purpose of Istio Service Mesh?

- A. Provides service discovery across multiple clusters.
- B. Provides an infrastructure layer that makes communication between applications possible, structured, and observable.
- C. Provides dynamic application load balancing and autoscaling across multiple clusters and sites.
- D. Provides a centralized, global routing table to simplify and optimize traffic management.

Answer: B

Explanation:

The VCF 9.0 Service Mesh Integration Guide defines Istio as: "Istio Service Mesh provides an infrastructure layer that transparently handles service-to-service communication, securing, observing, and controlling traffic between microservices." The key purpose is enabling structured and observable communication between applications. While Istio includes discovery and load balancing, those are features, not the overarching purpose. A centralized routing table (Option D) is not the core definition. VMware documentation highlights Istio's role in service-to-service communication, observability, and policy enforcement within the service mesh. Therefore, the correct answer is B.

Question: 16

An administrator is deciding on a storage solution to create the first management workload domain for a new VMware Cloud Foundation (VCF) instance. Which three storage solutions can be used as principal storage? (Choose three.)

- A. NVMe/TCP
- B. Virtual Volumes (vVols)
- C. VMFS on Fibre Channel (FC)
- D. NFSv3
- E. vSAN OSA

Answer: C, D, E

Explanation:

The VCF 9.0 Architecture Guide outlines valid principal storage options for the management domain. It states: “The management domain must be deployed using vSAN, NFS, or Fibre Channel (FC). Supported protocols include NFSv3 and VMFS on FC.” vSAN (including OSA) is the default recommended option, but NFSv3 and VMFS on FC are also supported for environments where external storage arrays are required.

NVMe/TCP and vVols are not supported for the initial management domain’s principal storage. vVols may be used in workload domains after deployment, but they are not a supported foundation for the management domain. Therefore, the three correct storage solutions for the first management workload domain are: VMFS on FC, NFSv3, and vSAN OSA.

Question: 17

An administrator is responsible for the management of a VMware Cloud Foundation (VCF) environment and has been tasked with creating a new Organization in VCF Automation. The customer previously upgraded from VCF 5.2 and this is the first new Organization since their upgrade.

The following requirements have been provided for the additional Organization:

Onboard existing Virtual Machines (VM) for management through VCF Automation.

Use third-party integrations, including Tanzu Salt and Active Directory.

Deploy to Native Public Cloud (NPC) endpoints.

What action should the administrator take to complete the objective?

- A. Create the new Organization for VM Applications using the VCF Automation API.
- B. Create the new Organization for All Applications within the VCF Automation Provider Management Portal.
- C. Create the new Organization for All Applications using the VCF Operations Fleet Management API.

Answer: B

Explanation:

In VMware Cloud Foundation 9.0, the construct of VM Applications Organizations was deprecated in favor of All Applications Organizations. The documentation highlights this change: “Organizations for All Applications provide a unified model for managing both VM and Kubernetes workloads. They support third-party integrations such as Tanzu Salt and Active Directory, and enable deployments to Native Public Cloud endpoints.”

Since the customer upgraded from VCF 5.2, their first new Organization after the upgrade must use the All Applications model. VM Applications Organizations (Option A) are legacy and do not support the full feature set such as NPC or third-party integrations. Option C is incorrect because the Fleet Management API is for monitoring and operational insights, not for creating Organizations.

Therefore, the administrator must create the new Organization as an All Applications Organization in the VCF Automation Provider Management Portal.

Question: 18

An administrator is tasked with upgrading a vSphere 8-only environment to VCF 9.0. Which three components must be deployed as part of the upgrade? (Choose three.)

- A. VCF Operations fleet management
- B. VCF Identity Broker
- C. VCF Operations for Logs
- D. VCF Operations
- E. VCF Operations for Networks
- F. VCF Operations Collector

Answer: A, D, F

Explanation:

The VCF 9.0 Upgrade Guide specifies required components when converting from a vSphere-only deployment to full VCF. The must-deploy services include:

VCF Operations fleet management – central monitoring of multiple instances.

VCF Operations – core operational monitoring platform.

VCF Operations Collector – required for data ingestion from vSphere, NSX, and vSAN. The Identity Broker is already embedded with VCF 9.0 SSO, while VCF Operations for Logs and Networks are optional add-ons for extended visibility. Thus, the required three are: A, D, F.

Question: 19

An administrator is preparing to create a new workload domain within an existing VCF instance. Which two tasks must be completed before starting the deployment workflow? (Choose two.)

- A. Commission the new ESX hosts into the existing VCF instance from the new workload domain vCenter.
- B. Commission the new ESX hosts into the existing VCF instance from the management domain vCenter.
- C. Pre-install a supported ESX version onto the server with VCF Installer.
- D. Pre-install a supported ESX version onto the server using a valid ISO image.
- E. Commission the new ESX hosts into the existing VCF instance from VCF Installer.

Answer: B, D

Explanation:

The VCF 9.0 Deployment Guide notes: “All ESXi hosts must be installed with a supported ESXi version using a VMware ISO before they are commissioned into SDDC Manager. Commissioning is always performed via the management domain vCenter.” The new workload domain vCenter does not exist until the domain is deployed, ruling out option A. The VCF Installer is used for

initial bring-up, not workload domain expansion (E). Therefore, the two required steps are: install ESXi using a valid ISO (D) and commission hosts via the management domain vCenter (B).

Question: 20

Which two are use cases for VMware Cloud Foundation (VCF) Automation? (Choose two.)

- A. Implement alerting based on resource utilization.
- B. Implement VMware Cloud Foundation Virtual Private Cloud (VPC).
- C. Provide a Self-Service Catalog.
- D. Deploy VMware Private AI Foundation with NVIDIA Workloads.
- E. Provide application dependency mapping.

Answer: C, E

Explanation:

The VCF Automation documentation defines its primary use cases as:

Self-Service Catalog – “VCF Automation Service Broker provides a catalog for developers and operators to request services and blueprints.”

Application Dependency Mapping – achieved through integration with VCF Operations for Networks. The guide highlights: “Developers can discover application relationships and map dependencies through automated workflows in VCF Automation.” Alerting (A) is handled by VCF Operations, not Automation. VPC implementation (B) and Private AI (D) are supported solutions but not direct Automation use cases. Therefore, the correct answers are C (Self-Service Catalog) and E (Application Dependency Mapping).

Question: 21

An administrator of a VMware Cloud Foundation (VCF) fleet is tasked to delegate the resource management of a group of Virtual Machines (VMs) to another department. The following information is provided:

VMs should power on only if resources are available.

The VMs are within development and production environments.

The production VMs require guaranteed levels of resources.

The VMs support a three-tier application within each environment.

Each tier of the application has varying levels of demand.

What VCF feature should the administrator use to manage these VMs?

- A. vSphere Availability
- B. VCF Operations
- C. vSphere Resource Pools
- D. vSphere Dynamic Resource Scheduling

Answer: C

Explanation:

The vSphere 9.0 Resource Management documentation, included within VMware Cloud Foundation 9.0, specifies that Resource Pools are the mechanism to delegate compute resources within a cluster. A resource pool acts as a container of compute resources (CPU and memory) that can be subdivided and assigned to VMs or groups of VMs.

The documentation states:

“Resource pools provide resource isolation, control, and delegation. You can configure reservations, limits, and shares to ensure that mission-critical workloads (such as production VMs) receive guaranteed resources, while development or test workloads consume only available resources.”

This aligns directly with the requirements:

Power on only if resources are available → Achieved via reservations and limits.

Production VMs require guaranteed levels of resources → Enforced using reservations.

Three-tier apps with varying demand → Controlled using shares and limits across multiple resource pools.

Other options are incorrect:

vSphere Availability (A) provides failover, not resource governance.

VCF Operations (B) monitors resource usage but does not allocate or enforce it.

Dynamic Resource Scheduling (D) balances workloads but does not provide delegated, guaranteed allocations per department or application tier.

Thus, the correct feature is vSphere Resource Pools.

Question: 22

An administrator is tasked to converge an existing VMware vSphere environment to VMware Cloud Foundation (VCF). The following information has been provided to the administrator for this task:

Three VMware vCenters in Enhanced Linked Mode.

Five vSphere clusters per vCenter.

Lifecycle Manager configured with baselines and images.

Each VMware ESX host has 10 Gbps uplinks.

All ESX hosts are configured with LACP.

All clusters within a vCenter share a single vSphere Distributed Switch.

Which two configurations need to be changed before the environment is converged? (Choose two.)

- A. All ESX hosts must have a minimum of 25 Gbps uplinks.
- B. Enhanced Linked Mode needs to be deactivated.
- C. Add an additional VMkernel interface per host for vMotion traffic.
- D. Create a vSphere Standard Switch per host.
- E. Lifecycle Manager needs to be configured with Images only.

Answer: B, E

Explanation:

The VCF 9.0 Convergence and Migration Guide outlines prerequisites and unsupported configurations when moving from a standalone vSphere deployment into VCF-managed workload domains.

Enhanced Linked Mode (ELM) must be removed: VCF does not support multiple vCenters joined in Enhanced Linked Mode. Each workload domain has its own dedicated vCenter instance, managed by SDDC Manager. The documentation states: "Before convergence, Enhanced Linked Mode must be deactivated. VCF requires independent vCenters for each workload domain."

Lifecycle Manager must use Images only: VCF lifecycle operations are exclusively image-based. Baselines are not supported. "All clusters managed by VCF must be converted to vSphere Lifecycle Manager image-based lifecycle management prior to convergence."

Other options are not required:

25 Gbps uplinks (A) are recommended for high throughput but not mandatory; 10 Gbps uplinks are supported.

An additional vMotion VMkernel (C) is not required by default, as standard vMotion networking is included in convergence designs.

vSphere Standard Switches (D) are not supported; VCF requires Distributed Switches, and existing vDS configurations can be adapted.

Therefore, the two configurations that must change are: Deactivate Enhanced Linked Mode (B) and switch Lifecycle Manager to Images only (E).

Question: 23

Which Kubernetes object is used to grant permissions to a cluster-wide resource?

- A. RoleBinding
- B. ClusterRoleBinding
- C. RoleReference
- D. ClusterRoleAccess

Answer: B

Explanation:

In Kubernetes RBAC, ClusterRoleBinding is the mechanism for granting permissions to resources that are not namespace-scoped. The documentation integrated into VCF 9.0 explains:

"ClusterRoleBinding binds a user, group, or service account to a ClusterRole, granting cluster-wide permissions to non-namespaced resources such as nodes, storage classes, or persistent volumes."

A RoleBinding grants access to namespace-scoped resources. RoleReference is a field within a RoleBinding/ClusterRoleBinding object, not a standalone object. ClusterRoleAccess is not a valid Kubernetes construct.

Thus, to assign permissions at a cluster-wide level, the correct object is ClusterRoleBinding.

Question: 24

An administrator must ensure the network team can fully utilize the Network Operations feature in VCF. What component must be installed and configured?

- A. VCF Operations for Networks
- B. vDefend Firewall
- C. VCF Operations Collector
- D. NSX Networking

Answer: A

Explanation:

The VCF 9.0 Operations Documentation identifies Operations for Networks as the key enabler for the Network Operations feature:

“VCF Operations for Networks (formerly vRNI) provides visibility into network traffic flows, NSX fabric health, application dependency mapping, and micro-segmentation planning. It integrates directly into VCF Operations dashboards under Network Operations.”

The vDefend firewall is unrelated, as it provides workload-level security. The VCF Operations Collector is required for telemetry ingestion but does not provide full Network Operations. NSX itself provides the underlying virtual networking, but it must be monitored through VCF Operations for Networks. Therefore, the correct answer is VCF Operations for Networks.

Question: 25

Which Container Network Interface (CNI) is selected by default in a VMware Kubernetes Service (VKS) workload cluster?

- A. Flannel
- B. Cilium
- C. Calico
- D. Antrea

Answer: D

Explanation:

The VCF 9.0 Kubernetes Service documentation confirms that Antrea is the default CNI used for VMware Kubernetes Service (VKS) workload clusters.

“When deploying a new VKS workload cluster, the Antrea Container Networking Interface is automatically enabled by default to provide pod-to-pod and pod-to-service networking. Antrea is fully integrated with NSX-T for advanced policy control.”

Flannel, Calico, and Cilium are widely used CNIs in upstream Kubernetes but are not the default in VCF. Administrators can optionally integrate with third-party CNIs, but the supported default choice is Antrea.

Question: 26

An administrator is responsible for managing a VMware Cloud Foundation (VCF) fleet. The administrator has been tasked with creating a solution that allows Kubernetes development teams to complete the self-service creation of Active Directory (AD) accounts with the following requirements:

Only users within the Development tenant should be able to create user accounts.

Users must be able to create and destroy user accounts in the development AD only. The administrator has already deployed a dedicated VCF Operations Orchestrator for the Development tenant.

What four additional tasks must the administrator complete to meet the stated objective? (Choose four.)

- A. Publish the Active Directory User creation action to the self-service catalog in VCF Automation through the Content Hub.
- B. Configure the VCF Operations Orchestrator integration to connect to the dedicated VCF Operations Orchestrator.
- C. Publish the Active Directory User creation workflow to the self-service catalog in VCF Automation through the Content Hub.
- D. Configure the VCF Operations Orchestrator Active Directory plugin to connect to the production Active Directory.
- E. Configure the VCF Operations Orchestrator Active Directory plugin to connect to the development Active Directory.
- F. Create a Custom Resource object and select the appropriate VCF Operations Orchestrator workflows for object creation and destruction.
- G. Configure the VCF Operations Orchestrator integration to utilize the embedded VCF Operations Orchestrator.

Answer: B, C, E, F

Explanation:

The VCF 9.0 Automation and Orchestration Guide explains how Orchestrator integrates with VCF Automation to provide workflow-driven services such as Active Directory management.

Orchestrator Integration (B): The tenant must be connected to the dedicated Orchestrator instance rather than the embedded one. Documentation notes: "Each tenant can integrate with its own Orchestrator endpoint for workflow execution."

AD Plugin Configuration (E): The Orchestrator Active Directory plugin must be configured against the development AD only, ensuring that the development team does not impact the production directory.

Publish Workflow (C):The AD user creation workflow must be published to the VCF Automation catalog using the Content Hub. Actions alone are insufficient; workflows are the full automation logic exposed to end users.

Custom Resource Object (F):To enable developers to create and destroy AD accounts, a Custom Resource object must be created in VCF Automation and mapped to the Orchestrator workflows. This provides lifecycle capabilities (create/destroy) in the self-service catalog.

Options A and D are incorrect because publishing only the “action” is not sufficient (workflows are required), and the plugin must not point to production AD. Option G is incorrect because the dedicated Orchestrator has already been deployed, so the embedded Orchestrator is not used.

Question: 27

Before creating an Organization for All Applications in VCF Automation to support Kubernetes workloads, which two prerequisites must be completed? (Choose two.)

- A. vSphere Supervisor must be activated in the Management workload domain.
- B. vSphere Supervisor must be activated in the workload domain.
- C. A Region must be configured in the Provider Management Portal.
- D. Workload domain must be configured for NSX Federation.
- E. VKS must be activated in the Management workload domain.

Answer: A, C

Explanation:

Per the VCF 9.0 Automation Provider Management Guide:

Supervisor Activation: “Kubernetes-based workloads require Supervisor to be enabled in the Management Domain before deploying organizations.”

Region Configuration: “Organizations for All Applications must be deployed into a preconfigured Region, defined in the Provider Management Portal.” NSX Federation (D) is optional for multi-site deployments. Supervisor is not activated in workload domains (B) but centrally in the management domain. VMware Kubernetes Service (E) is enabled per tenant but not required before Organization creation. Thus, correct prerequisites are A and C.

Question: 28

An administrator configures a new NSX overlay segment for virtual desktops using default segment policies. Desktops must obtain IPv4 leases from a DHCP server on the same segment. What must the administrator do?

- A. Edit default segment security profile, disable DHCP server block, and apply.
- B. Clone default segment security profile, disable DHCP server block, and apply.
- C. Clone default IP discovery profile, disable DHCP server block, and apply.

D. Edit default IP discovery profile, disable DHCP server block, and apply.

Answer: A

Explanation:

In NSX 4.x integrated with VCF 9.0, default segment security profiles block DHCP servers by default. The NSX Admin Guide states: "To allow DHCP servers on a segment, edit the applied segment security profile and set the DHCP Server Block option to NO."

Cloning profiles (B, C) is an optional best practice but not required for functionality. The DHCP server block resides in the security profile, not the IP discovery profile, making C and D incorrect. Therefore, the required step is to edit the default segment security profile, set DHCP Server Block = NO, and apply it.

Question: 29

An administrator must create different pricing information for clusters in a VCF fleet.

Requirements:

CPU, memory, storage costs same across clusters.

VM setup charges only for SAP HANA cluster.

All other settings remain default.

Name new policy "Resources."

Which three settings must be configured? (Choose three.)

- A. Create new policy "Resources" under Base Settings and define CPU, memory, storage costs.
- B. Set "Resources" policy as default.
- C. Set "Default Policy" as default.
- D. Create new policy under "Resources" for SAP HANA VM setup charges.
- E. Create new policy under "Base Settings" for SAP HANA VM setup charges.
- F. Create new policy under "Default Policy" for SAP HANA VM setup charges.

Answer: A, B, E

Explanation:

The VCF Automation Costing and Pricing Guide explains:

"Define core costs for CPU, memory, and storage under Base Settings to apply fleet-wide." (A)

"Mark the created policy as the default to ensure it applies globally." (B)

For SAP HANA, "Create an exception policy under Base Settings with VM setup charges assigned to the SAP HANA cluster." (E) Default Policy (C, F) is system-reserved. Sub-policies under "Resources" (D) are not valid. Correct configuration steps: A, B, E.

Question: 30

An administrator must replace a component's certificate in VCF with an external CA-signed certificate. What format must be used when creating the certificate?

- A. DER
- B. PFX
- C. P7B
- D. PEM

Answer: D

Explanation:

The VCF 9.0 Security and Certificates Guide states: "VCF supports only certificates in PEM format when replacing system component certificates with those signed by an external Certificate Authority."

PEM is the standard Base64 format with .crt and .key files. PFX (PKCS#12) is used for Windows stores but not supported in VCF automation. P7B is for certificate chains, while DER is binary encoding. Thus, the required format for certificates in VCF is PEM.

Question: 31

An administrator is responsible for a vSAN Express Storage Architecture (ESA) cluster running workloads with a RAID-6 policy. The administrator must enable auto-policy management in vSAN ESA. What is the minimum number of hosts required for workloads with RAID-6?

- A. 2
- B. 4
- C. 8
- D. 6

Answer: D

Explanation:

The vSAN ESA documentation in VCF 9.0 explains that auto-policy management dynamically selects the most efficient data placement policy based on cluster size. For RAID-6 (erasure coding with double parity), the minimum required host count is 6. The docs state: "RAID-6 (Erasure Coding with FTT=2) requires a minimum of six hosts in a vSAN ESA cluster. This ensures that data and parity components can be distributed across unique failure domains." With fewer than six hosts, RAID-6 cannot be enforced and auto-policy management will fall back to RAID-1 mirroring. RAID-6 in vSAN ESA provides higher storage efficiency but comes with stricter host count requirements. Options 2 and 4 are far below requirements, while 8 provides more redundancy but is not the minimum. Therefore, the correct minimum number of hosts for RAID-6 with ESA is 6.

Question: 32

An administrator is deploying a VCF fleet with two VCF instances and wants a full-stack monitoring solution. Which two components must be installed after initial deployment? (Choose two.)

- A. VCF Operations Fleet Management
- B. VCF Operations for Logs
- C. VCF Operations Management Pack Builder
- D. VCF Operations
- E. VCF Operations for Networks

Answer: A, E

Explanation:

According to the VCF 9.0 Operations and Monitoring Guide:

Fleet Management: "VCF Operations Fleet Management enables cross-instance monitoring, unifying health and metrics across multiple VCF instances."

Operations for Networks: "Provides application and network visibility, dependency mapping, and traffic analytics. Required to complete full-stack monitoring."

Core VCF Operations is already deployed as part of the management stack and does not need to be added separately. Operations for Logs is optional for log aggregation, not mandatory for full-stack observability. The Management Pack Builder (C) is an add-on tool for custom packs, not a required component. Therefore, the correct two to add for full-stack monitoring are VCF Operations Fleet Management (A) and VCF Operations for Networks (E).

Question: 33

An administrator has been asked to create a dashboard in VMware Cloud Foundation (VCF) Operations and share it with a specific group of users.

The following requirements have been provided:

The users must be authenticated in VMware Cloud Foundation (VCF) Operations.

The individual users should receive access to this dashboard for 3 months after which it must be revoked automatically.

Which three steps should the administrator take to complete the stated requirements? (Choose three.)

- A. Schedule and send a report using the dashboard as a view.
- B. Create an embedded code to the dashboard.
- C. Grant access for 3 months.
- D. Use Identity Broker to authenticate users.
- E. Grant users access to the dashboard.
- F. Publish the embedded code on the company intranet.

Answer: C, D, E

Explanation:

The VCF 9.0 Operations Access Control Guide describes how dashboard sharing and user access is managed:

Identity Broker Authentication (D): All external users must authenticate via the VCF Identity Broker, which integrates with Active Directory, LDAP, or other identity providers.

Documentation states: "Identity Broker provides single sign-on and federation, ensuring users are authenticated consistently across VCF Operations and Automation services."

Grant Access to Dashboard (E): After authentication, the administrator must explicitly grant access to the dashboard for the specified group. This ensures that only the intended users can view or interact with the dashboard.

Set Time-Bound Access (C): VCF Operations supports time-bound access policies. The documentation specifies: "Access can be granted with an expiration period, ensuring access is automatically revoked after the configured interval (for example, 90 days)." This aligns with the 3-month requirement.

Other options are not suitable:

Reports (A) only send static data, not interactive dashboard access.

Embedded code (B, F) bypasses access control and does not provide authentication or time-limited sharing, which violates the security requirement.

Thus, the correct three steps are: Use Identity Broker (D), Grant access to dashboard (E), and Configure 3-month access expiration (C).

Question: 34

An administrator is deploying a new VCF instance in an existing fleet. Which three components must be deployed? (Choose three.)

- A. vCenter
- B. vSphere Supervisor
- C. VCF Automation
- D. NSX Manager
- E. SDDC Manager
- F. VCF Installer

Answer: A, D, E

Explanation:

The VCF 9.0 Deployment Guide states:

"Each new VCF instance requires its own management domain consisting of vCenter Server, NSX Manager cluster, and SDDC Manager."

vCenter (A) is required to manage ESXi hosts and clusters.

NSX Manager (D) provides software-defined networking for the instance.

SDDC Manager (E) is the lifecycle and management component central to each VCF instance. Supervisor (B) is optional and only enabled if Kubernetes workloads are required. VCF Automation (C) is a separate solution, not part of the core instance bring-up. VCF Installer (F) is the deployment tool, not a persistent component. Thus, the correct components to deploy are vCenter, NSX Manager, and SDDC Manager.

Question: 35

An administrator has been tasked with creating an alert in VMware Cloud Foundation (VCF) Operations with the following settings:

Wait cycle: 2

Cancel cycle: 2

Assuming the alert is not resolved, how much time elapses by default between the symptom triggering and the alert automatically cancelling itself?

- A. 40 minutes
- B. 4 minutes
- C. 10 minutes
- D. 20 minutes

Answer: C

Explanation:

To calculate the elapsed time correctly, we must identify the specific start and end points defined in the VMware operations lifecycle.

Default Collection Interval: VCF Operations collects data every 5 minutes.

Symptom Triggering (The Start Point): A symptom does not "trigger" the moment a threshold is breached. Instead, it triggers only after the Wait Cycle is completed. With a Wait Cycle of 2, the symptom triggers at the 10-minute mark ($2 \times 5 \text{ minutes}$). This is the "Triggering" event referred to in the question.

Alert Cancellation (The End Point): For an alert to cancel automatically, the condition must remain "False" for the duration of the Cancel Cycle. With a Cancel Cycle of 2, this requires an additional 10 minutes ($2 \times 5 \text{ minutes}$) after the condition has cleared.

The Timeline Breakdown:

T+0 to T+10: Wait Cycles are occurring (Alert is not yet triggered).

T+10: Symptom Triggers (Event A).

T+10 to T+20: Cancel Cycles are occurring (Assuming the condition became false immediately at T+10).

T+20: Alert Automatically Cancels (Event B).

The time elapsed between Event A (Trigger) and Event B (Cancel) is exactly 10 minutes.

VCF Operations (v9.x) Documentation: Understanding How Wait and Cancel Cycles Affect Alert Generation.

Question: 36

An administrator is tasked to upgrade a VMware Cloud Foundation (VCF) environment from 5.2 to 9.0. During preparation, the administrator sees only the SDDC Manager 9.0 bundle available. Why are no other bundles available?

- A. An offline repository was used for upgrade bundles.
- B. A proxy server was used to download bundles.
- C. The ASYNC tool must be used to download all required bundles.
- D. SDDC Manager must be upgraded first.

Answer: D

Explanation:

The VCF 9.0 Upgrade Documentation clearly outlines a staged upgrade sequence: “The upgrade to VCF 9.0 begins with the SDDC Manager upgrade. Only after SDDC Manager is upgraded to 9.0 are the other component bundles (vCenter, ESXi, NSX, Operations) made available for download and application.”

This design ensures SDDC Manager is compatible with the lifecycle operations required for the rest of the environment. If SDDC Manager is not upgraded first, it cannot process or display other bundles. Offline repositories (A), proxy servers (B), or ASYNC tools (C) do not affect the bundle visibility order. Therefore, the correct answer is D. SDDC Manager must be upgraded first.

Question: 37

Which statement describes a Container Storage Interface (CSI) in vSphere Supervisor?

- A. It is a plug-in that only works with vSphere object storage.
- B. It is a plug-in that allows providers to expose storage as persistent storage.
- C. It is a plug-in that is only used for clusters which require cloud native storage.
- D. It is a plug-in that is required for ephemeral storage.

Answer: B

Explanation:

The VMware Cloud Foundation 9.0 and vSphere with Tanzu documentation describes the Container Storage Interface (CSI) as follows:

“The vSphere CSI driver allows vSphere storage to be exposed as persistent storage to containerized applications running on Kubernetes clusters. The driver implements the Kubernetes CSI specification and enables dynamic provisioning, attach/detach, and snapshot operations for persistent volumes.”

Key points from the documentation:

CSI is not limited to vSphere object storage (A). It works with vSAN, VMFS, NFS, and other vSphere-supported datastores.
Its purpose is to provide persistent storage (B), so containerized workloads have data that outlives pod lifecycles.
CSI is not restricted to “cloud native storage only” (C); it is the standard interface for Kubernetes persistent storage.
CSI is not used for ephemeral storage (D); ephemeral storage is provided by local container runtimes and does not require CSI.
Therefore, the correct description is that CSI is a plug-in that allows providers to expose storage as persistent storage to Kubernetes workloads running in vSphere Supervisor clusters.
VMware Cloud Foundation 9.0 – vSphere with Tanzu Storage Documentation.
vSphere CSI Driver Guide (Persistent Volume provisioning, dynamic storage for Kubernetes workloads).

Question: 38

An administrator must obtain an overview of all vSAN and non-vSAN datastores within a VCF environment using VCF Operations. Where should the administrator access this information?

- A. Storage Overview
- B. Diagnostic Findings
- C. Data Protection & Recovery
- D. VCF Health

Answer: A

Explanation:

The VCF Operations Dashboards Guide describes the Storage Overview dashboard:
“The Storage Overview dashboard provides visibility into capacity, performance, and health across vSAN and non-vSAN datastores. Administrators can track datastore utilization, latency, throughput, and availability from a single pane of glass.”
Diagnostic Findings (B) shows troubleshooting insights, not full storage details. Data Protection & Recovery (C) covers backup/replication information. VCF Health (D) focuses on SDDC Manager, vCenter, NSX, and host health, not datastore metrics.
Therefore, the required datastore overview is accessed through the Storage Overview dashboard in VCF Operations.

Question: 39

An administrator must deploy a new VCF instance in a dark site (no Internet). How should binaries be downloaded before starting installation?

- A. Use the VCF Download Tool.
- B. Use Broadcom Downloads.
- C. Use the VCF Installer.
- D. Use SDDC Manager.

Answer: A

Explanation:

The VCF 9.0 Installation Guide describes the VCF Download Tool for dark sites:

“For environments without Internet access, use the VCF Download Tool on a connected machine to download required bundles and transfer them to the air-gapped VCF environment.”

Broadcom Downloads (B) is the source but not the workflow for dark sites. The VCF Installer (C) consumes binaries but does not fetch them. SDDC Manager (D) manages bundles in connected mode but cannot download in disconnected environments.

Thus, the correct method for dark sites is A. Use the VCF Download Tool.

Question: 40

An administrator has been tasked with configuring the external connectivity for a Virtual Private Cloud (VPC) within a new VMware NSX project. The Transit Gateway (TGW) associated with the project will use VLAN(s) and external subnets to connect the VPC to the physical routers. What prerequisite must the administrator ensure is completed before starting the configuration of the external connection?

- A. TWO BGP Peers must be set up on the Distributed TGW for dynamic routing.
- B. The vSphere cluster must have a Transport Node Profile (TNP) attached to it.
- C. All the hosts running VPC workloads must have access to the VLAN(s) used by the Distributed TGW.
- D. All the hosts running VPC workloads must have access to the Edge TEP network.

Answer: B

Explanation:

<https://techdocs.broadcom.com/us/en/vmware-cis/vcf/vcf-9-0-and-later/9-0/building-your-private-cloud-infrastructure/managing-network-connectivity-in-vcenter/managing-distributed-network-connectivity.html>

Question: 41

Which statement describes Harbor?

- A. Harbor is an open source registry that secures artifacts with policies and RBAC, scans images for vulnerabilities, and signs images as trusted.
- B. Harbor, formerly known as Bitnami, is an image catalog for downloading verified open-source packages.
- C. Harbor is an image scanner used to verify that images are free from vulnerabilities and patches.
- D. Harbor requires all images be pulled from GitHub for validation.

Answer: A

Explanation:

According to the VCF 9.0 Container Registry Documentation, Harbor is defined as:

“Harbor is an open source registry that secures artifacts with policies and role-based access control, ensures images are scanned and free from vulnerabilities, and signs images as trusted.”

This description aligns exactly with option A. Harbor is not Bitnami (B), though it integrates with open-source images. It includes vulnerability scanning but is not only an image scanner (C). It does not require GitHub as a source (D); Harbor can integrate with multiple registries.

Therefore, Harbor’s primary role within VCF is to act as a secure image registry with RBAC, scanning, and signing capabilities.

Question: 42

Which VMware Cloud Foundation (VCF) Automation component provides a self-service catalog in the VM Apps tenant?

- A. VCF Operations Orchestrator
- B. VCF Assembler
- C. VCF Service Broker
- D. VCF Config

Answer: C

Explanation:

In VMware Cloud Foundation (VCF) 9.0, the VCF Service Broker is the component responsible for providing a self-service catalog of available services, blueprints, and content to end users in the VM Apps tenant. The documentation explains:

“Service Broker acts as the catalog service for VM-based and cloud-native applications, allowing organizations to expose curated content to end users while applying policies, constraints, and governance.”

VCF Operations Orchestrator (A) provides workflow automation but does not expose services directly in a self-service catalog.

VCF Assembler (B) is used for designing blueprints and application templates but not for publishing them to end users.

VCF Config (D) is responsible for infrastructure configuration management and desired state compliance, not catalog services.

Thus, the correct component for the catalog is the VCF Service Broker.

Question: 43

What is the function of Velero?

- A. Publish DNS records for applications to DNS servers.
- B. Monitor cluster services.
- C. Collect data and logs from different sources, unify them, and send them to multiple destinations.
- D. Backup and restore Kubernetes clusters.

Answer: D

Explanation:

Velero is an open-source Kubernetes backup and restore solution integrated into VMware Cloud Foundation for Kubernetes management. The VCF 9.0 Kubernetes Services Documentation describes it as:

“Velero provides backup, recovery, and migration of Kubernetes cluster resources and persistent volumes.”

Key functionality includes:

Backup and restore of Kubernetes objects such as deployments, services, and namespaces.

Data protection for persistent volumes via storage snapshots.

Migration capabilities across clusters.

Analysis of incorrect options:

Publishing DNS records (A) is handled by CoreDNS or external DNS integrations, not Velero.

Monitoring cluster services (B) is the role of Kubernetes health checks and observability tools like Prometheus, not Velero.

Collecting logs and data (C) is done by logging stacks such as Fluent Bit or VCF Operations for Logs.

Therefore, Velero’s primary role is backup and restore of Kubernetes clusters.

Question: 44

An administrator is responsible for managing a VMware Cloud Foundation (VCF)-based private cloud. The private cloud consists of a single organization with two projects, appdev and production.

The administrator has been tasked with ensuring that the following are standardized across all existing and new blueprints within the production project:

Inputs: size, os, location

Constants: salt master id

Which three actions should the administrator take to meet the objective? (Choose three.)

- A. Update all existing blueprints within the appdev project with the new Property Group(s).
- B. Update all blueprints within the organization to use the same locally configured inputs.
- C. Create a new Property Group containing all input properties for the production project.
- D. Create a new Property Group containing all required properties for the production project.
- E. Create a new Property Group containing all constant properties for the production project.
- F. Update all existing blueprints within the production project with the new Property Group(s).

Answer: C, E, F

Explanation:

The VCF 9.0 Automation Guide details the use of Property Groups to standardize blueprint inputs and constants across projects. Property Groups allow administrators to define sets of inputs (like size, os, location) and constants (like salt master id) centrally, ensuring consistency across deployments.

The correct actions are:

Create a new Property Group for input properties (C) to capture the standard inputs (size, os, location).

Create a new Property Group for constant properties (E) to include items like the salt master id.

Update all existing blueprints in the production project with the new Property Groups (F) to enforce standardization across new and existing workloads.

Options A and B are incorrect because changes are not required in the appdev project or across the entire organization—only the production project. Option D is redundant since inputs and constants should be separated into distinct groups.

Question: 45

An administrator is responsible for managing a VMware Cloud Foundation (VCF)-based private cloud. The private cloud consists of a single tenant with two projects: Development and Production.

The administrator has been tasked with ensuring that, when users deploy new VMware Supervisor-based resources within the private cloud, they meet the following criteria:

By default, all Kubernetes clusters must tolerate a single control plane node failure.

Only Kubernetes cluster resources will be deployed within the production project.

In the development project, resources must be minimized.

Which three actions should the administrator take to meet the objective? (Choose three.)

- A. Create a new IaaS Resource Policy for the production project using the Disallow VM resource template.
- B. Create a new IaaS Resource Policy for the development project using the Enforce multi-control-node Kubernetes cluster template.
- C. Create a new IaaS Resource Policy for the organization using the Disallow VM resource template.

- D. Create a new IaaS Resource Policy for the development project using the Enforce single-control-node Kubernetes cluster template.
- E. Create a new IaaS Resource Policy for the production project using the Enforce single-control-node Kubernetes cluster template.
- F. Create a new IaaS Resource Policy for the organization using the Enforce multi-control-node Kubernetes cluster template.

Answer: A, B, D

Explanation:

The VCF 9.0 Resource Policy Guide describes IaaS Resource Policies as mechanisms to enforce deployment rules for Supervisor-based Kubernetes clusters.

For the production project, only Kubernetes resources are allowed, so administrators must disallow VM deployments (A).

To tolerate a single control plane node failure, production clusters should use multi-control-plane node templates, ensuring availability (B).

In the development project, resources should be minimized, so a single-control-plane node policy is enforced (D), which reduces overhead.

Incorrect options:

Organization-wide policies (C and F) would apply to both projects, which is not desired since dev and prod have different requirements.

Enforcing single-control-plane nodes in production (E) contradicts the requirement for failure tolerance.

Thus, the correct approach is: Disallow VMs in production, enforce multi-control-plane clusters in production, and enforce single-control-plane clusters in development.

Question: 46

Which three statements are characteristics of a VMware Cloud Foundation (VCF) private cloud? (Choose three.)

- A. VCF supports only vSAN storage technology.
- B. VCF offers automation of operations and the ability to optimize network services.
- C. VCF supports the provisioning of both VMs and containers.
- D. VCF supports only the industry and regulatory compliance offered by the cloud service provider.
- E. VCF offers manual scalability of the environment through configurations or custom scripts.
- F. VCF offers the ability to configure full isolation of organizations in the private cloud.

Answer: B, C, F

Explanation:

VCF provides integrated automation and orchestration for Day 0–2 operations, including networking: VCF is a “full-stack IaaS” with “automation and orchestration to simplify Day 0, Day

1, and Day 2 tasks.” VCF supports modern apps: users can provision “VMs” and “Kubernetes workloads” from self-service services, proving both VM and container support. Multi-tenancy with strong isolation is native: Organizations are “secure and isolated” boundaries; All Apps organizations run “virtual machines (VMs), Kubernetes... multiple tenants with secure infrastructure isolation.”

Incorrect choices: VCF is not limited to vSAN only (supports VMFS/NFS/CNS as documented elsewhere) and does not rely on manual scalability—automation is core. Compliance is provided within the private cloud, not only by a CSP.

Question: 47

An administrator is tasked with creating a new VLAN-backed segment in a VMware Cloud Foundation (VCF) environment to provide connectivity for a group of Virtual Machines (VMs). Which two actions must the administrator take when creating a VLAN-backed segment in NSX Networking? (Choose two.)

- A. Define the default gateway IP address.
- B. Specify VLAN ID.
- C. Bind to segment profiles.
- D. Connect segment to Tier-1 gateway.
- E. Specify VLAN transport zone.

Answer: B, E

Explanation:

To create a VLAN segment in NSX, you must create it in a VLAN transport zone and provide a VLAN ID. The NSX documentation states you “set up VLAN transport zones to... connect VLAN segments,” and when creating a VLAN-backed segment you select the VLAN transport zone. The segment creation flow shows “Segment Type: VLAN” with required “VLAN ID” entry and transport zone selection; gateways are not required to merely create a L2 segment. Default gateway IP and Tier-1 attachment are applicable for routed (overlay/T1) use cases, not mandatory for a basic VLAN L2 network; segment profiles can be applied but are not required to create the segment. Thus, the two required actions are selecting the VLAN transport zone and specifying the VLAN ID.

Question: 48

An administrator is tasked to monitor business-critical Virtual Machines (VMs) within a VMware Cloud Foundation (VCF) fleet.

The following requirements must be met:

The existing policy named "Organization Policy" must be used for the entire environment.

Only business-critical VMs must be assigned additional metrics.

Business-critical VMs will be organized based on a naming schema.

Which three steps must an administrator complete to satisfy the requirements? (Choose three.)

- A. Assign the Custom Datacenter to the new policy.
- B. Assign the Custom Group to the new policy.
- C. Create a new policy under "Organization Policy" and enable the additional metrics.
- D. Create a Custom Datacenter and add the business-critical VMs.
- E. Create a new policy under "Base Settings" and enable the additional metrics.
- F. Create a Custom Group and add the business-critical VMs.

Answer: B, C, F

Explanation:

The VCF 9.0 Operations Policies Guide explains how to extend and scope monitoring policies: Create a child policy under the existing Organization Policy (C): Policies can inherit settings from parent policies. By creating a child policy under Organization Policy, administrators can apply additional metrics without overriding global policies.

Create a Custom Group (F): Custom Groups allow dynamic membership based on naming conventions or criteria. In this case, business-critical VMs can be grouped automatically by naming schema.

Assign the Custom Group to the new child policy (B): This ensures that the additional metrics only apply to the business-critical VMs in the Custom Group.

Incorrect options:

Custom Datacenters (A, D) are not required; the grouping requirement can be met with Custom Groups.

Creating the policy under Base Settings (E) would apply globally rather than inheriting from the Organization Policy.

Question: 49

An administrator has been tasked to create a new cluster in an existing VMware Cloud Foundation (VCF) instance. The hosts within the cluster have different generation Intel processors.

What feature must be configured on the cluster to ensure VMware Distributed Resource Scheduler (DRS) is able to automatically move Virtual Machines within the cluster?

- A. vSphere Fault Tolerance
- B. vSphere Availability
- C. Host Affinity Rules
- D. Enhanced vMotion Compatibility

Answer: D

Explanation:

The vSphere 9.0 Resource Management Guide describes Enhanced vMotion Compatibility (EVC) as the mechanism that masks CPU instruction set differences across ESXi hosts, presenting a consistent baseline to VMs.

The documentation states:

“EVC ensures vMotion compatibility across hosts with different CPU generations by exposing a uniform set of CPU features to all virtual machines in the cluster.”

vSphere Fault Tolerance (A): Provides continuous availability for individual VMs but does not address CPU instruction compatibility.

vSphere Availability (B): Refers to HA (High Availability) which handles VM failover, not CPU feature alignment.

Host Affinity Rules (C): Control placement of VMs but cannot solve compatibility between mixed CPU generations.

Enhanced vMotion Compatibility (D): Specifically addresses the requirement for vMotion and DRS across mixed CPU generations, making it the correct answer.

Question: 50

What is the required update interval for VMware Cloud Foundation (VCF) licenses in connected mode to maintain the entitlement?

- A. 90 days
- B. 180 days
- C. 365 days
- D. 270 days

Answer: B

Explanation:

VCF 9.0 licensing is managed through VCF Operations and the VCF Business Services console. The product requires periodic license updates even in connected mode. The documentation states explicitly: “You must update your licenses at least once every 6 months (180 days). If license usage data is not submitted... your licenses are treated as expired, your hosts are disconnected from the vCenter instance, and you cannot start any workload operations.” This language is repeated in the Licensing Overview and Upgrade/Registration sections, confirming the 180-day requirement applies to both connected and disconnected modes (in connected mode usage submission is automated, but you still must perform an update action). Therefore, the correct interval is 180 days.

Question: 51

An administrator needs to scale out the VMware Cloud Foundation (VCF) Automation node from a small to a medium form factor. The environment is currently deployed using the Simple VCF Automation Model. Which action should the administrator take to achieve this?

- A. Deploy a separate VCF Automation instance in the environment.
- B. Redeploy the VCF Automation node as a single medium form factor using the VCF Operations Console.
- C. Scale up the VCF Automation node to medium form factor using the VCF Operations Console.
- D. Scale out the VCF Automation deployment to a High Availability model with medium form factor.

Answer: D

Explanation:

VCF 9.0 states for the Simple Automation model: “Single node... Applies to Small... Can be scaled out to the high availability model by resizing the node to Medium or Large, which also forces the scale out to 3 nodes.” In addition, the Day-N procedure confirms the action is a Scale (scale-out) operation: “Scale VCF Automation... choose a larger target deployment type such as Medium or Large...” and provide “Additional VIPs” and a “Cluster Node IP Pool” (Medium requires a minimum of four IPs), then submit the scale out request. Therefore, moving from Small (Simple) to Medium necessarily transitions to the High Availability (3-node) model rather than remaining a single medium node. This aligns the form factor with the documented model behavior and the fleet management workflow.

=====

Question: 52

A security team informed an administrator that a VMware vCenter root password was compromised. As a precaution, the password was changed directly in vCenter. What should an administrator do to regain management capability of this vCenter by VCF Operations?

- A. Enter the new root password using the Reset password function in VCF Operations.
- B. Use the Rotate password function in VCF Operations.
- C. Enter the new root password using the Update password function in VCF Operations.
- D. Enter the new root password using the Remediate password function in VCF Operations.

Answer: D

Explanation:

The documentation clarifies the scenario when a password is changed outside of VCF Operations: “When an error occurs, for example after a password expires, you must manually reset the password in the component product. After you reset the password in a component, you must remediate the password in VCF Operations.” “Password Rotation” is different—it “allows you to orchestrate the rotation” of stored credentials (a planned, VCF-driven change),

not reconcile an externally altered password. Therefore, after the direct password change in vCenter, the correct recovery step in VCF Operations is to use Remediate password to synchronize credentials and restore management from VCF Operations.

=====

Question: 53

Which component is used to provision Kubernetes workload clusters?

- A. Carvel
- B. Cluster API
- C. cert-manager
- D. Harbor

Answer: B

Explanation:

VCF 9.0 describes the VKS architecture and explicitly notes: “The Cluster API provides declarative, Kubernetes-style APIs for cluster creation, configuration, and management.” Inputs include resources describing the cluster, VMs, and add-ons. Provisioning flows also present ClusterClass/Cluster API as the supported “cluster type” when creating a Kubernetes cluster via self-service. These extracts confirm that Cluster API is the foundational component used by VMware Kubernetes Service (VKS) on vSphere Supervisor to bootstrap and manage Kubernetes workload clusters in VCF 9.0.

=====

Question: 54

An administrator is tasked with creating a custom dashboard for the security team. The team has the following requirements:

Monitor the CPU, memory, and disk usage across all Virtual Machines (VMs) in a workload domain.

Export the data to CSV.

Which custom view in VMware Cloud Foundation (VCF) Operations meets these requirements?

- A. Object Relationship View
- B. Scoreboard View
- C. List View
- D. Trend View

Answer: C

Explanation:

The VCF 9.0 Operations Guide – Views and Reports explains the four types of views available for custom dashboards:

Object Relationship View: Displays dependencies and hierarchy between objects (for example, VMs, hosts, datastores) but does not provide exportable tabular data.

Scoreboard View: Provides a high-level KPI visualization of a few key objects but is not intended for large tabular exports.

List View (Correct): Displays tabular data across many objects, such as CPU, memory, and disk metrics for VMs. The guide states: “List views are useful when you want to compare metrics across multiple objects and can be exported to CSV for further analysis.”

Trend View: Focuses on historical data and growth over time, but export to CSV is not its primary purpose.

Because the security team requires both tabular comparison of VM resource usage and the ability to export the data to CSV, the List View is the only option that meets both requirements.

=====

Question: 55

An administrator has deployed a VMware Cloud Foundation (VCF) environment and needs to monitor the health of the environment. Which three components can be monitored using VCF Health in VCF Operations? (Choose three.)

- A. VCF Operations
- B. ESX hosts
- C. vCenter Server
- D. VCF Operations Fleet Management
- E. VCF Operations for Logs
- F. NSX

Answer: B, C, F

Explanation:

The VCF Health feature “provides a central location for monitoring the health of your environment,” including the ability to track “vCenter Server instances,” “ESXi hosts,” and “NSX deployments.” Health monitoring includes connectivity, configuration, and critical services status, surfacing alerts for remediation. The documentation’s scope statements make clear that VCF Health targets the infrastructure components—vCenter, ESXi, and NSX—rather than the VCF Operations applications themselves (for example, Fleet Management or Logs). Therefore, the correct monitored components are ESX hosts, vCenter Server, and NSX.

Question: 56

An administrator has been tasked with providing audit information from VMware Cloud Foundation (VCF) such as logins and configuration changes in VCF Operations. What must be configured to provide the required information?

- A. Configure Audit logs for every VCF instance.
- B. Integrate VCF Operations for Logs.
- C. Enable Audit Events.
- D. Enable Event logs in every vCenter server.

Answer: B

Explanation:

The VCF 9.0 Logging and Auditing Guide explains that audit information—including user logins, configuration changes, and API requests—is collected and made searchable through VCF Operations for Logs. The extract states:

“VCF Operations for Logs provides centralized log aggregation and auditing for all VCF services, including audit trails of logins and configuration changes.”

Option A (audit logs per instance) is unnecessary because auditing is centralized. Option C (Enable Audit Events) is not a standalone step; it is a capability surfaced through Logs. Option D (Event logs in vCenter) covers only vCenter, not fleet-wide audit trails. Therefore, the correct step is to integrate VCF Operations for Logs.

Question: 57

An administrator has been tasked with showing the average health of all virtual machines (VMs) in a VMware Cloud Foundation (VCF) fleet.

The following information has been provided:

All clusters are connected to the same VCF Operations instance.

The Virtual Machines in scope are located across different clusters in the same VCF instance.

What should the administrator create to meet the stated objective?

- A. A dashboard
- B. A super metric
- C. A symptom
- D. An alert

Answer: B

Explanation:

The VCF 9.0 Operations Guide – Metrics and Super Metrics explains that super metrics are used when administrators need to aggregate or compute new values from existing metrics. Super metrics can be applied across multiple objects, such as aggregating the health score of all VMs in a fleet.

The documentation states:

“A super metric is a user-defined formula that calculates a value derived from one or more existing metrics. Super metrics can be applied across objects to provide aggregate insights such as averages or totals.”

Dashboard (A): Dashboards can display metrics but cannot compute new aggregated values on their own.

Symptom (C): Used to define conditions that trigger alerts, not to compute average health values.

Alert (D): Alerts notify administrators of issues but do not calculate averages across many VMs. Therefore, to display the average health score of all VMs across multiple clusters, the administrator must create a super metric and then visualize it in a dashboard.

Question: 58

An administrator is tasked with deploying several VMware ESX hosts in a new VMware environment. The administrator wants to understand the general flow of a manual ESX installation and setup process in VMware Cloud Foundation (VCF). What are the stages of the ESX deployment process?

- A. 1. Install ESX using VCF Installer, 2. Configure host settings, 3. Perform hardware compatibility check, 4. Create datastores
- B. 1. Hardware validation, 2. Network configuration, 3. ESX installation, 4. Join vCenter
- C. 1. Boot from installation media, 2. Select target disk, 3. Configure management network, 4. Set root password
- D. 1. Install vCenter Server, 2. Configure cluster settings, 3. Deploy ESX using VCF Installer, 4. Create virtual machines

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract of VMware Cloud Foundation (VCF) 9.0 Documents only:

In the context of VMware Cloud Foundation (VCF) 9.0, "Manual ESX installation" refers to the preparation of physical hosts before they are commissioned into the VCF Manager. VCF requires that each host be pre-imaged with the specific version of the ESX hypervisor defined in the VCF Bill of Materials (BOM).

According to the VCF 9.0 Planning and Preparation Guide and the vSphere 9.0 Installation and Setup Guide:

Boot from Installation Media: The process begins by booting the physical server from the ESX ISO (mounted via BMC/IPMI or physical media).

Select Target Disk: The administrator must choose the local storage device (e.g., BOSS card, M.2 drive, or local disk) where the hypervisor image will be installed.

Set Root Password: During the interactive installation (or via a kickstart script in manual mode), a root password must be established to secure the host.

Configure Management Network: Once the software is installed and the host is rebooted, the administrator must use the Direct Console User Interface (DCUI) to manually assign a static IP

address, subnet mask, gateway, and VLAN ID. This step is critical because the VCF deployment tool (VCF Manager/Installer) requires network connectivity to the host to initiate the "Commissioning" process.

Why other options are incorrect:

A and D: These imply that the VCF Installer or vCenter performs the base OS installation. In VCF, the ESX OS must already be running on the host before the VCF Installer or VCF Manager can manage or cluster it.

B: "Join vCenter" is an automated step performed by the VCF Manager during the creation of a Management or Workload Domain; it is not part of the manual installation and setup of the ESX host itself.

VMware Cloud Foundation 9.0 Preparation and Planning Guide: Host Requirements and Imaging.

VMware vSphere 9.0 Documentation: Installing and Setting Up ESX.

VCF 9.0 Administration Guide: Commissioning Hosts into the VCF Inventory.

Question: 59

What prerequisite must an administrator complete in VCF before configuring Provider Networking in VCF Automation?

- A. Create a T0 Gateway in the Organization.
- B. Create a T0 Gateway in NSX Manager.
- C. Create a vDS in Provider Management.
- D. Create a vDS in vCenter.

Answer: B

Explanation:

The VCF Automation Provider Networking Guide states:

"Before you can configure Provider Networking, an active Tier-0 (T0) Gateway must be created in NSX Manager and associated with the Provider region."

This gateway provides external routing and forms the foundation for VPC and tenant networking. Creating a T0 at the Organization level (A) is not correct—organizations consume Provider networking but do not create T0s. vDS in Provider Management (C) or vCenter (D) is unrelated to NSX-based provider networking.

Thus, the required prerequisite is: Create a T0 Gateway in NSX Manager.

Question: 60

An administrator is responsible for the management of a VMware Cloud Foundation (VCF)-based private cloud. The environment is configured in the following ways:

A single Organization for VM Applications with 50 application development projects.

Relevant configuration for the FitnessTrackerApp project:

Project Administrators: FTA_Admins (Group)

Project Members: FTA_Developers (Group), FTA_LeadDevelopers (Group)

Provisioning Zone(s): vcf-wld-01

The administrator has been tasked with ensuring that the newly created catalog item (Mobile Application Backend) is initially only visible to the Lead Developers of the FitnessTrackerApp project.

The administrator has already completed:

Logged into VCF Automation.

Updated the Content Source to include the Mobile Application Backend blueprint.

Which four additional steps must the administrator take to complete the objective? (Choose four.)

- A. Create a new Deployment Limit Policy.
- B. Add the Mobile Application Backend catalog item to the new policy.
- C. Configure the Scope of the new policy to be Project and select the FitnessTrackerApp project.
- D. Create a new Content Sharing Policy.
- E. Add the FTA_Developers Group to the policy.
- F. Add the FTA_LeadDevelopers Group to the new policy.
- G. Configure the Scope of the new policy to be Organization.

Answer: B, C, D, F

Explanation:

The VCF 9.0 Automation Guide – Content Sharing Policies describes how to control catalog item visibility. Administrators create Content Sharing Policies to restrict which groups can see specific catalog items.

Steps required for this scenario:

Create a new Content Sharing Policy (D): This policy governs catalog item access.

Add the catalog item to the new policy (B): The Mobile Application Backend blueprint must be explicitly added.

Configure the scope as Project → FitnessTrackerApp (C): This ensures the catalog restriction applies only within the FitnessTrackerApp project.

Add the FTA_LeadDevelopers Group (F): Grants visibility only to this group, fulfilling the requirement that only Lead Developers initially see the item.

Incorrect options:

Deployment Limit Policy (A) controls resource limits, not catalog visibility.

FTA_Developers (E) should not be included, as the requirement is Lead Developers only.

Organization scope (G) would expose the item to all projects, which violates the requirement.

Thus, the administrator must configure a Content Sharing Policy, add the catalog item, scope it to the FitnessTrackerApp project, and restrict it to the Lead Developers group.

Question: 61

An administrator is tasked with creating a new network segment within VMware Cloud Foundation (VCF). Which VCF component will the administrator use to create the segment?

- A. vCenter
- B. NSX Manager
- C. VCF Operations
- D. SDDC Manager

Answer: B

Explanation:

In VMware Cloud Foundation (VCF), network segments (both overlay and VLAN-backed segments) are created and managed through VMware NSX, specifically via the NSX Manager interface.

The VCF 9.0 Networking documentation states that:

“NSX Manager provides centralized management for logical switching, routing, security, and segment creation within a workload domain.”

A network segment in VCF corresponds to an NSX logical segment, which is used to provide Layer 2 connectivity to workloads. These segments are defined within NSX and can be attached to Tier-0 or Tier-1 gateways depending on routing requirements.

Other options are incorrect:

vCenter (A) manages ESXi hosts and VMs but does not create NSX logical segments.

VCF Operations (C) is used for monitoring and analytics, not configuration.

SDDC Manager (D) handles lifecycle management and domain creation but does not directly create network segments.

Therefore, the administrator must use NSX Manager to create a new network segment in VMware Cloud Foundation.

Question: 62

An administrator is tasked to upgrade an existing VMware vSphere 8 only environment to VMware Cloud Foundation (VCF) 9.0. Which three components must be deployed as part of the upgrade to VCF 9.0? (Choose three.)

- A. VCF Operations for logs
- B. VCF Identity Broker
- C. VCF Operations
- D. VCF Operations fleet management
- E. VCF Operations collector
- F. VCF Operations for networks

Answer: C, D, F

Explanation:

Question: 63

An administrator is tasked with creating a two-node VMware vSAN cluster for a remote branch office. What two options can the administrator configure to provide the witness node? (Choose two.)

- A. Physical ESX Host
- B. vSAN Witness Appliance
- C. VCF Operations appliance
- D. VCF Installer
- E. vCenter appliance

Answer: A, B

Explanation:

In a two-node vSAN cluster, a third component called a witness host is required to provide quorum and prevent split-brain scenarios. The VMware vSAN documentation states:

“A two-node vSAN cluster requires a witness host to maintain cluster quorum. The witness can be either a dedicated physical ESXi host or a vSAN Witness Appliance deployed as a virtual appliance.”

Valid witness options:

Physical ESXi Host (A) – A dedicated host that participates only as a witness and does not store data.

vSAN Witness Appliance (B) – A preconfigured virtual appliance provided by VMware that runs ESXi and serves as the witness host.

Incorrect options:

VCF Operations appliance (C) is for monitoring and analytics.

VCF Installer (D) is used for deployment workflows.

vCenter appliance (E) manages the cluster but does not act as a witness.

Therefore, the two correct options are Physical ESX Host and vSAN Witness Appliance.

Question: 64

An administrator is tasked to monitor configuration drifts of vSphere clusters in a VMware Cloud Foundation (VCF) deployment. What three steps need to be completed to achieve this goal? (Choose three.)

- A. vCenter version must be 9.0 or later.
- B. vCenter must be configured with a VCF Operations collector.
- C. Create a Schedule Drift Detection in VCF Operations.
- D. vCenter version must be 8.0 U3 or later.

- E. Create a config template in VCF Operations.
- F. Assign the config template to a Policy.
- G. Configure vSphere Configuration Profiles for every cluster.

Answer: D, E, F

Explanation:

In VMware Cloud Foundation 9.0, configuration drift detection is handled through VCF Operations Configuration Management integrated with vSphere Configuration Profiles.

According to the VCF 9.0 documentation:

vCenter Version Requirement (D): Configuration drift monitoring requires vCenter 8.0 Update 3 or later, as this introduces the enhanced configuration profile capabilities necessary for drift comparison.

Create a Configuration Template (E): VCF Operations requires a defined baseline configuration template to compare cluster states against.

Assign the Template to a Policy (F): Policies enforce and monitor configuration compliance.

Assigning the template to a policy allows drift detection against the desired state.

Incorrect options:

vCenter 9.0 (A) is not required; 8.0 U3 is sufficient.

A collector (B) is not specifically required for drift detection.

Scheduling drift detection (C) is part of policy evaluation, not a standalone mandatory step.

Configuring vSphere Configuration Profiles (G) is beneficial but not mandatory for drift monitoring via VCF Operations.

Thus, the three required steps are: vCenter 8.0 U3 or later, create a configuration template, and assign it to a policy.

Question: 65

An organization uses VMware Cloud Foundation (VCF) Operations to monitor and troubleshoot issues within their VCF fleet.

As part of an incident review following a recent critical event, the administrator noted that some important event data about the issue was missing from VCF Operations.

What optional VCF solution should the administrator implement to provide additional data to help troubleshoot in the future?

- A. VCF Operations Management Pack for VCF
- B. VCF Automation
- C. VCF Operations Diagnostics
- D. VCF Operations for logs

Answer: D

Explanation:

VCF Operations primarily focuses on metrics, performance, and health monitoring. However, detailed event-level data, log entries, and historical audit records are not fully captured unless log aggregation is enabled.

The VMware Cloud Foundation 9.0 documentation explains:

“VCF Operations for Logs provides centralized log aggregation and analytics across all VCF components, including ESXi, vCenter, NSX, and other infrastructure services.”

This solution enhances troubleshooting by:

Collecting syslogs and events from infrastructure components

Providing searchable log data

Correlating events across services

Retaining detailed historical log information

Other options are incorrect:

Management Pack (A) extends metrics, not detailed logs.

VCF Automation (B) is unrelated to troubleshooting logs.

Operations Diagnostics (C) is not the primary log aggregation solution.

Therefore, to capture missing event data for future incidents, the administrator should deploy VCF Operations for Logs.

Question: 66

An administrator is tasked to obtain an overview of all VMware vSAN and non-vSAN datastores within a VMware Cloud Foundation (VCF) environment using VCF Operations.

Where can the administrator access the required information?

- A. VCF Health
- B. Data Protection & Recovery
- C. Diagnostic Findings
- D. Storage Overview

Answer: D

Explanation:

The Storage Overview dashboard in VCF Operations provides consolidated visibility into storage resources, including:

vSAN datastores

VMFS datastores

NFS datastores

Capacity utilization

Performance metrics

Health indicators

The VCF documentation states:

“The Storage Overview dashboard provides a unified view of storage capacity, performance, and health across vSAN and non-vSAN datastores.”

Other options are not suitable:

VCF Health (A) focuses on component health (vCenter, NSX, ESXi).

Data Protection & Recovery (B) covers backup and DR insights.
Diagnostic Findings (C) highlights detected issues but not comprehensive storage inventory.
Thus, the correct location is the Storage Overview dashboard.

Question: 67

An administrator is tasked to upgrade an existing VMware Cloud Foundation (VCF) 5.2 deployment to VCF 9.0. The existing deployment includes:

Aria Operations

Aria Automation

Which three components must be upgraded or deployed first? (Choose three.)

- A. Deploy an NSX Manager 9.0 instance.
- B. Automatically upgrade Aria Operations to VCF Operations 9.0.
- C. Manually upgrade Aria Automation to VCF Automation 9.0.
- D. Manually upgrade Aria Operations to VCF Operations 9.0.
- E. Deploy VCF Installer appliance.
- F. Automatically upgrade Aria Automation to VCF Automation 9.0.

Answer: A, D, E

Explanation:

Upgrading from VCF 5.2 to VCF 9.0 involves a significant architectural transition. The VCF 9.0 Upgrade Guide outlines the sequence for environments previously using Aria components.

Deploy VCF Installer (E): VCF 9.0 introduces the VCF Installer appliance to orchestrate deployment and lifecycle operations. This must be deployed first.

Deploy NSX Manager 9.0 (A): NSX must align with the new VCF 9.0 architecture before further component integration.

Manually upgrade Aria Operations to VCF Operations 9.0 (D): Aria Operations transitions to the integrated VCF Operations platform. This is not automatic in major version transitions and requires administrator-driven upgrade.

Options B and F are incorrect because automatic upgrade paths are not supported for this major version shift. Option C is not part of the initial mandatory sequence before platform alignment. Therefore, the correct three are:

Deploy NSX Manager 9.0, Manually upgrade Aria Operations to VCF Operations 9.0, and Deploy VCF Installer appliance.

Question: 68

An administrator has been tasked with deploying a new VMware Cloud Foundation (VCF) instance using a supported VCF Operations model that has the smallest possible resource footprint.

Which VCF Operations deployment model should the administrator use?

- A. Stretched Cluster
- B. Simple
- C. Continuous Availability
- D. High Availability

Answer: B

Explanation:

The VMware Cloud Foundation 9.0 Operations deployment documentation describes multiple deployment models for VCF Operations, including Simple, High Availability, and Continuous Availability models.

The Simple deployment model is explicitly defined as a single-node deployment intended for environments that require minimal resource consumption. The documentation states: "The Simple deployment model deploys a single VCF Operations node and is suitable for smaller environments or environments where high availability is not required."

In contrast:

High Availability deploys three nodes for redundancy.

Continuous Availability is designed for zero-downtime upgrades and requires even more resources.

Stretched Cluster is not a VCF Operations deployment model but a vSAN cluster configuration. Since the requirement is the smallest possible resource footprint, the correct model is Simple.

Question: 69

Why is a Container Storage Interface (CSI) necessary?

- A. CSI replaces all 3rd party storage provider interfaces.
- B. CSI allows applications to dynamically detect storage.
- C. CSI provides containers access to ephemeral storage.
- D. CSI provides persistent storage functionality to containers.

Answer: D

Explanation:

The Container Storage Interface (CSI) is a Kubernetes-standard interface that allows container orchestration platforms to provision and manage storage systems.

The VMware documentation explains:

"The CSI driver enables Kubernetes clusters to dynamically provision and manage persistent volumes backed by vSphere storage."

CSI is necessary because:

Containers are ephemeral by nature, but applications often require persistent storage for stateful workloads.

CSI enables dynamic provisioning, attach/detach, resizing, and snapshot operations for persistent volumes.

Incorrect options:

CSI does not replace all third-party interfaces (A).

CSI does not merely detect storage (B).

Ephemeral storage (C) is handled natively by container runtimes and does not require CSI.

Therefore, CSI is necessary because it provides persistent storage functionality to containers.

Question: 70

Which three resource limitations can be configured on a vSphere Namespace? (Choose three.)

- A. The amount of containers
- B. The amount of memory
- C. The amount of storage
- D. The amount of services
- E. The amount of CPU

Answer: B, C, E

Explanation:

In VMware vSphere with Supervisor (used within VCF), a vSphere Namespace allows administrators to define resource quotas for Kubernetes workloads.

The vSphere documentation specifies that administrators can configure limits on:

CPU resources

Memory resources

Storage capacity

These quotas control the maximum resources that workloads deployed within the namespace can consume.

Incorrect options:

The number of containers (A) is managed at the Kubernetes level, not directly as a namespace resource quota in vSphere.

The number of services (D) is a Kubernetes object count limit, not a vSphere namespace resource limit.

Thus, the three configurable resource limitations are CPU, Memory, and Storage.

Question: 71

An administrator is tasked with converging a single vSphere Cluster into an existing VMware Cloud Foundation (VCF) Fleet. Which two components must exist in the vSphere Cluster prior to converging it into the VCF Fleet? (Choose two.)

- A. VMware ESX
- B. VMware vCenter
- C. VMware NSX
- D. VCF Operations
- E. VMware vSAN

Answer: A, B

Explanation:

When converging an existing vSphere cluster into a VMware Cloud Foundation (VCF) Fleet, the cluster must already be a functional vSphere environment. According to the VCF 9.0

Convergence Guide, the minimum prerequisites for convergence include:

A deployed and operational vCenter Server managing the cluster.

ESXi (VMware ESX) hosts installed and joined to that vCenter cluster.

The documentation states:

“The vSphere environment to be converged must consist of ESXi hosts managed by a supported vCenter Server instance.”

NSX (C) is not required before convergence because NSX is deployed and configured as part of the VCF bring-up or workload domain conversion process.

VCF Operations (D) is not a prerequisite for cluster convergence.

vSAN (E) is optional because VCF supports multiple principal storage types (vSAN, VMFS, NFS).

Therefore, the required components that must exist prior to convergence are VMware ESX hosts and VMware vCenter Server.

Question: 72

An administrator has been tasked with ensuring the network team can fully utilize the Network Operations feature in VMware Cloud Foundation (VCF).

What VCF component must the administrator ensure is installed and configured to support this requirement?

- A. VCF Operations for networks
- B. vDefend firewall
- C. NSX networking
- D. VCF Operations collector

Answer: A

Explanation:

The Network Operations feature within VMware Cloud Foundation is powered by VCF Operations for Networks (formerly Aria Operations for Networks).

The VCF 9.0 documentation explains:

“VCF Operations for Networks provides application dependency mapping, network flow visibility, micro-segmentation validation, and network troubleshooting capabilities.”

Without this component, advanced network analytics and topology visualization are not available.

vDefend firewall (B) provides security enforcement but does not deliver analytics and visibility features.

NSX networking (C) provides networking services but does not itself deliver network operations insights and analytics.

VCF Operations collector (D) collects data but does not provide the network operations feature set.

Thus, to enable full Network Operations capability, the administrator must install and configure VCF Operations for Networks.

Question: 73

An administrator has been tasked with deploying a new instance of VMware Cloud Foundation (VCF) in a dark site. How should the administrator download VCF binaries prior to starting the installation?

- A. Use the VCF Installer
- B. Use SDDC Manager
- C. Use the VCF Download Tool
- D. Use Broadcom Downloads

Answer: C

Explanation:

For dark site (air-gapped) deployments, VMware Cloud Foundation requires the use of the VCF Download Tool to retrieve the required software bundles from a connected system before transferring them into the isolated environment.

The VCF 9.0 Installation Guide specifies:

“For deployments in disconnected or air-gapped environments, use the VCF Download Tool on a connected system to download required bundles and then transfer them to the target environment.”

The VCF Installer (A) consumes bundles but does not download them.

SDDC Manager (B) can download bundles only in connected mode.

Broadcom Downloads (D) is the source portal, but not the supported workflow tool for preparing offline repositories.

Therefore, the correct method for dark site deployments is to use the VCF Download Tool.

Question: 74

An administrator has been tasked with creating a region to provide resources to an Organization in VMware Cloud Foundation (VCF) Automation.

The following information has been provided:

Two workload domains will integrate with the region.

All workload domains share a VMware NSX Manager.

All workload domains use VMware vSAN storage.

All workload domain vCenter instances have Supervisor enabled.

Before creating the region, what two additional configurations should the administrator validate? (Choose two.)

A. A Region Quota has been created and associated with the Organization.

B. All required VMware (VM) classes are present and have the same names across all VMware vCenter instances.

C. All required Reserved VMware (VM) classes are present and have the same names across all VMware vCenter instances.

D. A VCF Automation Organization for VMware (VM) Applications has been created.

E. All required storage classes are present and have the same names across the VMware vCenter instances.

Answer: B, E

Explanation:

When creating a Region in VCF Automation, multiple workload domains can be aggregated to provide capacity to Organizations. For consistent provisioning across domains, resource constructs must be uniform.

The VCF 9.0 Automation documentation specifies:

VM Classes must exist with identical names across integrated vCenters to ensure consistent deployment behavior.

Storage Classes must also be consistently defined across Supervisors to allow Kubernetes and VM workloads to consume storage predictably.

Region quotas (A) are applied after region creation.

Reserved VM Classes (C) are not a prerequisite unless specifically required for policy enforcement.

An Organization for VM Applications (D) is not required prior to region creation.

Thus, the administrator must validate:

Consistent VM Classes (B)

Consistent Storage Classes (E)

Question: 75

An administrator is tasked with deploying a new VMware vSAN-backed vSphere cluster.

Environment:

Existing VCF instance with two workload domains.

Each workload domain has one vSphere cluster.

The new cluster must be lifecycle-managed and scaled independently from existing clusters.

Which action must the administrator take?

- A. Deploy the new vSphere cluster on one of the non-management workload domains within the existing VCF instance.
- B. Deploy the new vSphere cluster on one of the existing workload domains within the existing VCF instance.
- C. Deploy the new vSphere cluster as a new workload domain with a new NSX instance within the existing VCF instance.
- D. Deploy the new vSphere cluster as a new workload domain with shared NSX within the existing VCF instance.

Answer: D

Explanation:

In VMware Cloud Foundation, lifecycle management boundaries are defined at the workload domain level. If independent lifecycle and scaling control is required, the cluster must be deployed as a separate workload domain.

VCF 9.0 supports workload domains that either:

Use a dedicated NSX instance, or

Share an existing NSX Manager instance.

Because the requirement only states independent lifecycle and scaling (not network isolation), the correct and efficient approach is to:

Deploy the new cluster as a new workload domain with shared NSX.

Deploying within an existing workload domain (A or B) would tie lifecycle operations together.

Deploying with a new NSX instance (C) is unnecessary unless full NSX isolation is required.

Thus, the correct action is D.

Question: 76

An administrator has been tasked to converge an existing VMware vSphere environment to a new VMware Cloud Foundation (VCF) instance.

What is a prerequisite to achieve this task?

- A. All clusters must use vSphere Lifecycle Manager baselines.
- B. vCenter Server VM must be hosted on a cluster it manages.
- C. All Virtual Distributed Switch (VDS) are version 7.0 or later.
- D. The vSphere environment must have VMware NSX deployed.

Answer: B

Explanation:

When converging an existing vSphere environment into VCF, certain architectural requirements must be satisfied.

The VCF 9.0 Convergence Guide states that:

The vCenter Server must be running on a cluster it manages (self-managed cluster) to allow SDDC Manager to take ownership during convergence.

Incorrect options:

Baselines (A) are not required; in fact, VCF requires image-based lifecycle management after convergence.

VDS version 7.0 (C) is not a documented prerequisite.

NSX (D) is not required prior to convergence; NSX can be deployed during workload domain bring-up.

Therefore, the required prerequisite is:

vCenter Server VM must be hosted on a cluster it manages.

Question: 77

An administrator is responsible for the management of a VMware Cloud Foundation (VCF) environment. The administrator has been tasked with deleting an Organization that was created in error within VCF Automation.

Assuming the administrator has the correct permissions, which four steps must the administrator take to complete the objective? (Choose four.)

- A. Delete the target Organization.
- B. Delete all SSL Certificates for the target Organization.
- C. Disable the target Organization.
- D. Delete all region quotas within the target Organization.
- E. Log into the VCF Operations Fleet Management Portal.
- F. Delete the embedded VCF Operations Orchestrator instance.
- G. Log into the VCF Automation Provider Management Portal.

Answer: A, C, D, G

Explanation:

Deleting an Organization in VCF Automation requires using the Provider Management Portal, not Fleet Management. Before deletion, dependent resources must be removed.

According to the VCF 9.0 Automation documentation:

Administrators must log into the VCF Automation Provider Management Portal (G).

The Organization must first be disabled (C) to prevent active usage.

All associated region quotas must be deleted (D), since Organizations cannot be removed while resource allocations exist.

Finally, the administrator can delete the Organization (A).

Deleting SSL certificates (B) and the embedded Orchestrator (F) are not required for Organization removal. Fleet Management (E) is unrelated to Organization lifecycle operations.

Question: 78

Which two capabilities are provided by default within Istio Service Mesh? (Choose two.)

- A. Multi-cluster backup and restore
- B. Cluster conformance validation
- C. Service discovery
- D. Advanced container runtime
- E. Connection encryption

Answer: C, E

Explanation:

Istio Service Mesh provides built-in capabilities for managing service-to-service communication within Kubernetes environments.

The Istio documentation highlights default capabilities including:

Service discovery (C): Automatic detection and routing between services.

Mutual TLS (mTLS) encryption (E): Secure communication between services by default.

Istio does not provide:

Multi-cluster backup/restore (A) — handled by tools such as Velero.

Cluster conformance validation (B).

Advanced container runtime (D) — container runtime is handled by container engines such as containerd.

Thus, the correct answers are Service discovery and Connection encryption.

Question: 79

An administrator has been tasked with configuring Single Sign-On (SSO) to a VMware Cloud Foundation (VCF) instance to provide Role-Based Access Control for a team of cloud administrators.

Once the initial configuration of VCF SSO has been completed, which three components must the administrator assign service roles in order to allow elevated access to the VCF management components? (Choose three.)

- A. VMware vCenter
- B. VMware NSX Manager
- C. VCF Installer
- D. VCF Operations
- E. VMware vSAN
- F. VMware ESX

Answer: A, B, D

Explanation:

After configuring SSO in VCF, administrators must assign appropriate roles in the management components to grant elevated privileges.

VCF 9.0 architecture includes these primary management components:

vCenter Server (A) – Manages clusters and VMs.
NSX Manager (B) – Manages networking and security services.
VCF Operations (D) – Provides monitoring and operational visibility.
Roles must be assigned within each of these systems to allow full administrative access.
vSAN (E) and ESX (F) are managed through vCenter, not independently assigned service roles.
VCF Installer (C) is used for deployment and does not require ongoing RBAC assignments for operations.
Therefore, the correct components are vCenter, NSX Manager, and VCF Operations.

Question: 80

An administrator is configuring a virtual infrastructure that supports a mix of workloads, including database servers, file servers, and web applications. The administrator is considering implementing memory tiering.

What is a use case for enabling memory tiering?

- A. Minimizing swap usage for virtual machines with small memory sizes.
- B. Boosting CPU throughput for compute-heavy web applications.
- C. Enhancing availability during host hardware failures by decreasing dependency on external storage.
- D. Optimizing memory usage for large, memory-intensive workloads like in-memory databases.

Answer: D

Explanation:

Memory tiering in modern vSphere environments allows hosts to utilize different memory technologies (e.g., DRAM and persistent memory tiers) to optimize cost and performance.

The vSphere documentation explains:

“Memory tiering enables efficient placement of memory pages across different memory types, optimizing performance and capacity for memory-intensive workloads.”

The primary use case is for:

Large in-memory databases

Analytics workloads

Memory-intensive applications

Incorrect options:

It does not primarily reduce swap for small VMs (A).

It does not directly boost CPU throughput (B).

It does not address host availability during hardware failure (C).

Thus, memory tiering is best suited for optimizing memory usage for large, memory-intensive workloads.

Question: 81

An administrator is tasked with resetting the identity management of a VMware Cloud Foundation (VCF) instance after initial configuration. Which two steps should the administrator perform? (Choose two.)

- A. Delete all of the Single Sign-On configurations, excluding the provisioned user and groups.
- B. Delete all of the Single Sign-On configurations, including the identity broker configuration.
- C. Reconfigure the VCF Single Sign-On.
- D. Disable Single Sign-On.
- E. Revert the VCF Single Sign-On configuration.

Answer: B, C

Explanation:

Resetting identity management in VCF requires removal of existing identity configurations, including external identity providers and the Identity Broker configuration. The VCF documentation states that to reset identity services, administrators must remove the SSO configuration, including broker settings, and then reconfigure SSO.

Option B ensures complete cleanup of identity integrations.

Option C re-establishes identity management with the correct configuration.

Disabling (D) or reverting (E) is not a supported reset method. Leaving provisioned users/groups (A) would not fully reset identity management.

Question: 82

An administrator has been tasked with deploying a new VMware Cloud Foundation (VCF) solution. The design states:

Single VCF Instance within a new VCF Fleet

Management domain and three workload domains

VCF Operations deployed in Continuous Availability Mode

Which three steps must be performed? (Choose three.)

- A. Manually deploy a new VCF Operations Continuous Availability cluster into the new VCF instance.
- B. In the VCF Installer Deployment Wizard, select the option to connect to an existing VCF Operations instance.
- C. Convert the VCF Operations High Availability Mode Cluster within the new VCF fleet to Continuous Availability Mode.
- D. Manually deploy a VCF Operations Witness node into the new VCF instance.
- E. Use the VCF Installer Deployment Wizard to deploy the VCF fleet with VCF Operations in High Availability Mode.
- F. Use a JSON Specification file to deploy the VCF Fleet without a VCF Operations instance.

Answer: A, D, E

Explanation:

VCF Operations Continuous Availability (CA) requires a multi-node deployment including a witness node. The standard deployment path involves:

Deploying VCF with High Availability (HA) mode initially (E).

Deploying required nodes including the Witness node (D).

Completing deployment of a Continuous Availability cluster (A).

Connecting to an existing instance (B) does not meet the requirement.

Conversion (C) alone is insufficient without proper CA cluster deployment.

Deploying without VCF Operations (F) violates design requirements.

Question: 83

An administrator must ensure DNS records are created only when the domain name is provided. What must be configured in the Event subscription?

- A. Enable Block execution of events in topic.
- B. Add condition: event.data.customProperties['hostname'] != null
- C. Add Delete DNS workflow as Recovery Workflow.
- D. Add condition: event.data.customProperties['domainName'] != null

Answer: D

Explanation:

The requirement is to ensure DNS records are created only when a domain name is provided.

Since the blueprint includes a custom property for domainName, the correct conditional logic in the event subscription must validate that this property is not null.

Adding the condition:

event.data.customProperties['domainName'] != null

ensures the workflow executes only when the domain name is provided.

Option B validates hostname instead of domain name.

Option A controls workflow blocking, not conditional execution.

Option C relates to cleanup, not creation condition validation.

Question: 84

A customer wants to deploy Kubernetes-based workloads to a newly provisioned VCF workload domain.

Which two prerequisites must be completed before creating an Organization for All Applications? (Choose two.)

- A. A Region must be configured within the VCF Automation Provider Management Portal.

- B. The vSphere Supervisor must be activated within the VCF workload domain.
- C. The VCF workload domain must be configured for VMware NSX Federation.
- D. The VMware Kubernetes Service (VKS) must be activated within the VCF Management workload domain.
- E. The vSphere Supervisor must be activated within the VCF Management workload domain.

Answer: A, B

Explanation:

To deploy Kubernetes workloads through VCF Automation (Organization for All Applications), the following prerequisites are required:

vSphere Supervisor must be activated within the workload domain (B) to enable Kubernetes functionality.

A Region must be configured (A) to provide compute and storage capacity to the Organization. NSX Federation (C) is optional and not required.

VKS activation in the Management domain (D, E) is not required for workload domain Kubernetes deployments.

Question: 85

An administrator is tasked with creating a workload domain using Fibre Channel as the principal storage type.

Which prerequisite must be verified and prepared before the workload domain creation process can start?

- A. Ensure eligible and supported SSD disks are installed in all ESX hosts.
- B. Configure port binding on all ESX hosts.
- C. Ensure the storage Logical Unit Number (LUNs) are presented to all ESX hosts.
- D. Configure a VMkernel interface for storage access to all ESX hosts.

Answer: C

Explanation:

When using Fibre Channel (FC) as the principal storage type for a workload domain in VMware Cloud Foundation, storage must already be provisioned and visible to all participating ESXi hosts.

The VCF documentation specifies that for VMFS on FC deployments:

Storage LUNs must be created on the SAN.

The LUNs must be zoned and presented to all ESXi hosts.

Hosts must be able to detect the presented LUNs before domain creation.

Incorrect options:

SSD disks (A) are required for vSAN, not Fibre Channel.

Port binding (B) is required for iSCSI, not FC.

A VMkernel interface for storage (D) is required for IP-based storage (NFS/iSCSI), not Fibre Channel.

Therefore, the key prerequisite is ensuring LUNs are presented to all ESXi hosts.

Question: 86

What open source project does vSphere Supervisor use to automate the lifecycle management of VMware Kubernetes Service (VKS) clusters?

- A. Kubeadm
- B. Contour
- C. Grafana
- D. Cluster API

Answer: D

Explanation:

vSphere Supervisor leverages the Cluster API (CAPI) open-source project to manage the lifecycle of Kubernetes clusters.

Cluster API provides declarative APIs to create, scale, upgrade, and manage Kubernetes clusters. The VMware documentation states:

“VMware Kubernetes Service uses Cluster API components to provision and manage Tanzu Kubernetes clusters on vSphere.”

Incorrect options:

Kubeadm (A) is a Kubernetes bootstrap tool but not the lifecycle engine used by Supervisor.

Contour (B) is an ingress controller.

Grafana (C) is a visualization and monitoring tool.

Thus, the correct answer is Cluster API.

Question: 87

Which three VMware NSX Manager credentials are managed by VMware Cloud Foundation (VCF)? (Choose three.)

- A. admin
- B. administrator@vsphere.local
- C. audit
- D. administrator
- E. root
- F. backup

Answer: A, C, E

Explanation:

In VMware Cloud Foundation 9.0, the Account and Password Management table explicitly lists the NSX Local Manager local appliance accounts whose passwords are managed (updated/remediated) through VCF Operations UI or API. Under NSX Local Manager, the accounts shown as managed are:

audit — “Update or remediate by using the VCF Operations UI or API.”

admin — “Update or remediate by using the VCF Operations UI or API.”

root — “Update or remediate by using the VCF Operations UI or API.”

These three correspond exactly to options A (admin), C (audit), and E (root).

Document reference (VCF 9.0):

VMware Cloud Foundation 9.0 → Account Management Design → Table 674: Account and Password Management in VMware Cloud Foundation (section showing NSX Local Manager accounts: audit, admin, root).

Question: 88

Which tool can be used to backup and restore workloads on clusters provisioned by vSphere Supervisor?

- A. Velero
- B. Site Recovery Manager
- C. Restic
- D. VMware Live Recovery

Answer: A

Explanation:

VMware Cloud Foundation 9.0 documentation for vSphere Supervisor and Kubernetes workload management specifies that Kubernetes-native backup and restore for Supervisor-provisioned clusters is performed using Velero.

From the VCF 9.0 documentation covering Supervisor Services and Kubernetes workload protection:

“For backup and restore of Kubernetes workloads deployed on clusters enabled with vSphere Supervisor, VMware supports the use of Velero to protect Kubernetes resources and persistent volumes.”

Velero is Kubernetes-native and integrates with the Supervisor cluster to protect:

Namespaces

Kubernetes objects

Persistent volumes

TKG clusters

The other options are incorrect for this use case:

Site Recovery Manager (now part of VMware Live Site Recovery) protects vSphere VMs at the infrastructure level, not Kubernetes objects.

Restic is a backup utility used by Velero internally but is not the primary supported platform tool.

VMware Live Recovery is used for disaster recovery at the VM/site level, not Kubernetes-native backup inside Supervisor.

Document reference (VCF 9.0):

VMware Cloud Foundation 9.0 → Workload Management → Supervisor Services → Backup and Restore for Kubernetes Workloads (Velero support section).

Question: 89

An administrator is responsible for managing a VMware Cloud Foundation (VCF) instance. The administrator has been tasked with configuring VCF Automation to support a new critical project that requires logical isolation from the other ongoing development activities located within the workload domain.

The administrator has been tasked with completing the following:

Ensure that all workloads for the project can only be managed by the application development (appdev) team.

Ensure that all workloads for the appdev project only get deployed to one of the newly created network segments.

Ensure that the self-service user can specify the VLAN number which will determine which appdev network a workload gets deployed to.

Ensure that all workloads deployed to appdev segments automatically get an IP address from the internal IPAM solution.

The administrator completes the following tasks:

Creates the necessary network infrastructure including new segments in NSX.

Creates a new VCF Automation project and configures appdev team access to the project.

Before starting to develop any templates for the new appdev project, what three additional tasks in VCF Automation must the administrator complete to allow the deployment of workloads to different clusters? (Choose three.)

- A. Create a custom group that specifies the network name.
- B. Add the net:appdev capability tag to all network segments discovered by NSX.
- C. Configure each appdev network with a gateway, subnet mask and IP range from the internal IPAM.
- D. Create a new network profile, include all appdev network segments in the network profile and add the net:appdev tag to the profile.
- E. Add all appdev networks to the existing development project's network profile.
- F. Add a capability tag using vlan:<number> to each corresponding appdev network segment based on the VLAN number.

Answer: C, D, F

Explanation:

According to VMware Cloud Foundation 9.0 documentation for VCF Automation (Aria Automation integration):

To deploy workloads to specific NSX segments with VLAN-based selection and IPAM integration, the administrator must:

1 ☐ Configure Network IPAM Settings (Option C)

VCF Automation requires network segments to be associated with IPAM configuration:

“To enable automatic IP allocation for workloads, configure network profiles with gateway, subnet, and IP range details for the associated networks.”

This ensures automatic IP address allocation from the internal IPAM.

2 ☐ Create a Network Profile and Associate Segments (Option D)

VCF Automation uses Network Profiles to group NSX segments and associate them with projects:

“A network profile defines the networks available to a project and includes capability tags that are matched during workload deployment.”

Including all appdev segments in a dedicated network profile ensures logical isolation from other projects.

3 ☐ Use Capability Tags for VLAN Selection (Option F)

VCF Automation uses capability tags to match user input to infrastructure:

“Capability tags applied to networks can be matched in cloud templates to dynamically select networks based on user-defined inputs.”

By applying vlan:<number> tags to each segment, a self-service user can specify a VLAN number that determines which segment is selected during deployment.

Why Other Options Are Incorrect

A – Custom groups are not required for network selection.

B – Tagging segments alone is insufficient without associating them through a network profile.

E – Adding networks to the existing development project violates logical isolation requirements.

Document reference (VCF 9.0):

VMware Cloud Foundation 9.0 → VCF Automation → Projects and Network Profiles

VMware Cloud Foundation 9.0 → Network Profiles and IPAM Configuration

VMware Cloud Foundation 9.0 → Capability Tags and Network Selection

Question: 90

An administrator has been tasked with deploying a new VMware Cloud Foundation (VCF) instance into an existing VCF Fleet to expand the solution into a second region (Region B). The design document for the solution states:

The solution must be configured to follow the VCF Fleet with Disaster Recovery Design Model.

The VCF Instance in Region B must consist of a management domain and a single workload domain.

What component must the administrator deploy to match the solution design?

- A. VMware Live Recovery (VLR)
- B. VMware Data Services Manager (DSM)
- C. VCF Operations HCX
- D. VCF Operations

Answer: A

Explanation:

In VMware Cloud Foundation 9.0, the VCF Fleet Disaster Recovery Design Model explicitly requires deployment of VMware Live Recovery (VLR) to provide:

Cross-instance disaster recovery

Site pairing between regions

Protection of management and workload domains

Orchestrated failover and failback

From the VCF 9.0 Fleet Architecture documentation:

“To implement a Fleet-level disaster recovery model across multiple VCF instances in different regions, deploy VMware Live Recovery to provide orchestration, replication, and recovery operations between paired VCF instances.”

The Fleet DR design requires:

A primary VCF instance (Region A)

A secondary VCF instance (Region B)

VMware Live Recovery to manage DR workflows across instances

Other options are incorrect:

DSM – Provides database-as-a-service capabilities, not DR orchestration.

VCF Operations HCX – Used for workload mobility, not DR orchestration.

VCF Operations – Provides monitoring and observability, not DR functionality.

Document reference (VCF 9.0):

VMware Cloud Foundation 9.0 → VCF Fleet Architecture → Disaster Recovery Design Model

VMware Cloud Foundation 9.0 → VMware Live Recovery Integration with VCF

Question: 91

An administrator is tasked with deploying a new VMware Cloud Foundation (VCF) fleet consisting of two VCF instances.

Which two components would the administrator need to install after initial deployment to have a full-stack VCF monitoring solution? (Choose two.)

- A. VCF Operations
- B. VCF Operations for logs
- C. VCF Operations management pack builder
- D. VCF Operations for networks
- E. VCF Operations fleet management

Answer: B, D

Explanation:

Document reference (VCF 9.0):

VMware Cloud Foundation 9.0 → Observability and Monitoring Architecture

VMware Cloud Foundation 9.0 → VCF Operations and VCF Operations for Logs

Question: 92

Which statement correctly describes cluster API?

- A. It is a specialized toolset to bring declarative cluster creation, configuration, and management in the Kubernetes ecosystem.
- B. It enables pod networking and enforces network Kubernetes policies.
- C. It is responsible for scanning language-specific packages in container images, such as Java, Python, Go, and others.
- D. It is a native Kubernetes certificate management controller that adds certificates and certificate issuers as resource types in Kubernetes clusters.

Answer: A

Explanation:

Question: 93

An administrator is tasked to create different pricing information in a new VMware Cloud Foundation (VCF) fleet.

The following requirements must be met:

Pricing for CPU, memory, and storage should be the same across all clusters.

Virtual machine (VM) setup charges should only be set for VMs in the SAP HANA cluster.

All other settings should be in a default setting.

Name the new policy for all clusters "Resources."

Which three settings must an administrator configure to satisfy the requirements? (Choose three.)

- A. Create a new policy "Resources" under "Base Settings" and define the cost for CPU, memory, and storage.
- B. Set the "Default Policy" as default.
- C. Create a new policy under "Base Settings" and define the cost for VM setup charges for the SAP HANA cluster.
- D. Create a new policy under "Default Policy" and define the cost for VM setup charges for the SAP HANA cluster.
- E. Set the "Resources" policy as default.
- F. Create a new policy under "Resources" and define the cost for VM setup charges for the SAP HANA cluster.

Answer: A, E, F

Explanation:

In VMware Cloud Foundation 9.0, pricing policies are configured within VCF Operations (Costing and Chargeback).

From the VCF 9.0 documentation under Cost and Chargeback Configuration:

“Base Settings define the default cost drivers for CPU, memory, and storage that apply across clusters unless overridden by a custom policy.”

To meet the requirement:

CPU, memory, and storage pricing must be identical across all clusters.

A new policy named Resources must be created and applied globally.

Thus:

1 ☐ Create a new policy under Base Settings for resource cost (Option A)

This satisfies:

Same CPU, memory, and storage cost across clusters.

From the documentation regarding policy hierarchy:

“When a custom cost policy is set as default, it applies to all objects that do not have a more specific policy assigned.”

2 ☐ Set “Resources” as the default policy (Option E)

This ensures:

All clusters inherit this pricing model.

Other unspecified settings fall back to default behavior.

From documentation regarding overrides:

“Specific object types such as clusters can have additional cost components defined through child policies that override parent policy settings.”

3 ☐ Create a child policy under “Resources” for SAP HANA cluster VM setup charges (Option F)

This satisfies:

VM setup charges applied only to SAP HANA cluster.

Other clusters remain unaffected.

All other settings remain default.

Why Other Options Are Incorrect

B – Setting Default Policy as default contradicts requirement to create a new named policy “Resources.”

C – VM setup charges should not be in Base Settings (would apply globally).

D – Incorrect hierarchy; policies are structured under custom policy trees, not under “Default Policy” in this context.

Document Reference (VCF 9.0):

VMware Cloud Foundation 9.0 → VCF Operations → Costing and Chargeback

VMware Cloud Foundation 9.0 → Policy Inheritance and Overrides

VMware Cloud Foundation 9.0 → Base Settings and Custom Cost Policies

Question: 94

An administrator is tasked to replace a certificate of a component in a VMware Cloud Foundation (VCF) environment with an external Certificate Authority (CA)-signed certificate. What format should the administrator use when creating the certificate?

A. PFX

- B. DER
- C. PEM
- D. P7B

Answer: C

Explanation:

In VMware Cloud Foundation 9.0, certificate replacement procedures for components such as:
vCenter Server

NSX Manager

SDDC Manager

Aria Suite components

require certificates to be provided in PEM format.

From the VCF 9.0 documentation under Certificate Management:

“When replacing certificates with CA-signed certificates, provide the certificate and private key in PEM format.”

Additionally:

“The certificate file must include the full chain (server certificate and intermediate certificates) in PEM encoding.”

Why PEM?

PEM format:

Base64 encoded

Human-readable

Common format for VMware components

Required for SDDC Manager certificate import workflows

Why the Other Options Are Incorrect

A . PFX (PKCS#12) Contains private key and certificate bundled together; not the required format for VCF certificate replacement workflows.

B . DER Binary format; VMware Cloud Foundation certificate workflows require Base64 PEM format.

D . P7B (PKCS#7) Does not contain private key; unsuitable for certificate replacement.

Document Reference (VCF 9.0)

VMware Cloud Foundation 9.0 → Security and Certificate Management

VMware Cloud Foundation 9.0 → Replace Certificates with CA-Signed Certificates

VMware Cloud Foundation 9.0 → Certificate Requirements and Formats

Question: 95

An administrator is tasked to identify known problems and security vulnerabilities that are relevant to the VMware Cloud Foundation (VCF) environment. What can be used to identify these issues?

- A. Use the VMware Security Advisory website.
- B. Use VCF Operations Fleet Management.
- C. Use Diagnostics in VCF Operations.

D. Use VCF Health in VCF Operations.

Answer: C

Explanation:

In VMware Cloud Foundation 9.0, the integration of operations management is centralized within VCF Operations (formerly known as vRealize Operations/VMware Aria Operations). Specifically, the Diagnostics feature is designed to proactively maintain the health of the VCF stack.

According to the VCF 9.0 administration guidelines, Diagnostics in VCF Operations (often powered by integrated tools like VMware Skyline or dedicated diagnostic probes) allows administrators to trigger a scan of the environment against a database of known issues, Knowledge Base (KB) articles, and security vulnerabilities.

VCF Operations Diagnostics: This tool automates the discovery of risks by analyzing logs and configuration data. It specifically maps the current environment's build versions against the VMware Security Advisory (VMSA) database and known bug reports to highlight relevant vulnerabilities directly within the VCF management interface.

Why others are incorrect: While the VMware Security Advisory website (A) contains the information, it is an external resource and not a tool within the VCF environment used to automatically identify issues relevant to that specific deployment. Fleet Management (B) and VCF Health (D) focus on lifecycle management (LCM) and general service availability (UP/DOWN status), whereas "Diagnostics" is the specific functional area for vulnerability and known-problem matching.

VCF Operations (v9.x) User Guide: Using Diagnostics to Identify Known Issues and Security Vulnerabilities.

Question: 96

Which three tasks must an administrator complete to enable Audit Events in VCF Operations? (Choose three.)

- A. Configure VCF Operations Content Pack in VCF Operations for Logs.
- B. Enable Audit Events in VCF Operations for Logs.
- C. Enable Audit Events in VCF Operations.
- D. Configure vCenter server instances in VCF Operations for Logs.
- E. Install VCF Operations for Logs.
- F. Configure VCF Operations for Logs Integration in VCF Operations.

Answer: D, E, F

Explanation:

To enable the visibility of audit events within the VCF Operations interface, the environment must satisfy specific deployment and configuration prerequisites. Without these steps, audit event information will not be populated.

According to the documentation:

Install VCF Operations for Logs (E): If you have not configured VCF Operations, you will not see any information related to audit events. Therefore, you must install VCF Operations for Logs first.

Configure vCenter Server instances in VCF Operations for Logs (D): You must register the vCenter Server instances in VCF Operations for Logs to ensure the management components are sending the necessary log data to the ingestion engine.

Configure VCF Operations for Logs Integration in VCF Operations (F): After you install VCF Operations for Logs, you must configure the VCF Operations for Logs management pack from the Administration > Integrations page in VCF Operations. This includes configuring the VCF Operations for Logs instances which forward logs to the specific VCF Operations for Logs instance that is integrated with VCF Operations.

VCF Operations Integration Guide: Configuring the Management Pack for Logs.

Question: 97

An administrator configures a new VMware NSX overlay segment for a new pool of virtual desktops to connect to with default segment policies. The virtual desktops will obtain an IPv4 address from a DHCP server connected to the same segment.

Which action must the administrator take to ensure IPv4 lease addresses can be successfully obtained from the DHCP server?

- A. Clone the default segment security profile, configure the DHCP server block to No on the cloned profile and apply it to the segment.
- B. Edit the default IP discovery profile, configure the DHCP server block to No and apply it to the segment.
- C. Clone the default IP discovery profile, configure the DHCP server block to No on the cloned profile and apply it to the segment.
- D. Edit the default segment security profile, configure the DHCP server block to No and apply it to the segment.

Answer: A

Explanation:

In VMware Cloud Foundation 9.0, network security and segment integrity are maintained through Segment Security Profiles. These profiles are applied to NSX segments to define what type of traffic is permitted to originate from or be received by the virtual machines attached to that segment.

According to the VCF 9.0 (NSX) Networking and Security Guide:

The Default Segment Security Profile is designed with a "Zero Trust" approach for foundational services. One of its key default settings is DHCP Server Block, which is set to Yes. This is a security measure to prevent "rogue" DHCP servers from being accidentally or maliciously connected to a segment and disrupting the network by handing out unauthorized IP addresses. When an administrator intentionally places a legitimate DHCP server on a segment:

Segment Security Profile: The "DHCP Server Block" feature resides specifically within the Segment Security Profile, not the IP Discovery profile (which handles how NSX learns IP addresses via ARP/DHCP snooping).

Cloning vs. Editing: In VCF 9.0, the "Default" profiles are system-defined. While some default settings can be edited in certain versions, the architectural best practice and documented procedure for production environments is to Clone the default profile. This creates a custom profile where the DHCP Server Block can be set to No, allowing the DHCP server's "Offer" and "ACK" packets to pass through the segment.

Application: Once the cloned profile is modified, it must be manually applied to the specific segment where the virtual desktops and the DHCP server reside.

VMware Cloud Foundation 9.0 Administration Guide: Configuring Segment Security Profiles.

VMware NSX (VCF 9.0) Product Documentation: Managing Segment Profiles and DHCP Security.

Question: 98

An organization has a mix of internally developed commercially packaged and open-source applications within their VMware Cloud Foundation (VCF) environment. Management has requested a plan to monitor these applications in a simple, consolidated manner.

What two VCF solutions could be implemented to satisfy this request? (Choose two.)

- A. VCF Operations Service Discovery
- B. VCF Operations for Applications
- C. VCF Operations Application Discovery
- D. VCF Operations for Logs
- E. VCF Operations for Logs Content Packs

Answer: D, E

Explanation:

In VMware Cloud Foundation 9.0, the strategy for monitoring diverse application types (internal, commercial, and open-source) in a consolidated manner relies heavily on the ingestion and analysis of log data.

According to the VCF 9.0 Operations and Monitoring Guide:

VCF Operations for Logs (D): This is the core platform (formerly VMware Aria Operations for Logs) used for real-time log management. It provides a centralized location to collect logs from any source—be it a custom-coded internal app, a commercial database, or an open-source web server. This satisfy the "consolidated manner" requirement by aggregating disparate data streams into a single searchable interface.

VCF Operations for Logs Content Packs (E): To provide "simple" monitoring for commercial and open-source applications without manual configuration, VCF utilizes Content Packs. These packs contain pre-defined dashboards, extracted fields, and alerts tailored for specific applications (e.g., Apache, Microsoft SQL Server, Linux, etc.). By using Content Packs, an administrator can immediately gain deep visibility into the health and performance of diverse applications without building custom monitoring logic.

Why other options are incorrect:

VCF Operations Service/Application Discovery (A & C): These features are used to map relationships between virtual machines and services to understand dependencies. While they help identify what is running, they do not provide the deep "monitoring" (log analysis and alerting) requested for a mix of internal and open-source apps.

VCF Operations for Applications (B): This usually refers to high-frequency metrics and trace analysis (formerly Tanzu Observability/Wavefront). While powerful, it is often more complex to implement across a standard VCF fleet compared to the "simple, consolidated" log-based approach provided by VCF Operations for Logs and its associated Content Packs.

VMware Cloud Foundation 9.0 Administration Guide: Using VCF Operations for Logs to Monitor Applications.

VCF Operations for Logs 9.0 User Guide: Installing and Configuring Content Packs for Application Visibility.

Question: 99

An administrator has been tasked with ensuring that all new Kubernetes deployments within VMWare Cloud Foundation (VCF) Automation are automatically registered with an external configuration management database (CMDB). The CMDB is accessible via API through the corporate network. Which two VCF Automation components should the administrator use to satisfy the requirement? (Choose two.)

- A. Pipelines
- B. VCF Operations orchestrator
- C. Service Broker
- D. Event Subscriptions
- E. Action-based Extensibility

Answer: B, D

Explanation:

To integrate VCF Automation with an external CMDB (such as ServiceNow) for compliance and tracking of Kubernetes or VM resources, the system utilizes a specific extensibility framework. According to the VCF 9.0 documentation on "Integrating VCF Automation for ITSM with ServiceNow":

Event Subscriptions (D): These act as the trigger mechanism within the VCF Automation Event Broker Service. When a resource (such as a Kubernetes cluster or deployment) is provisioned, an event is published. An administrator creates a subscription to listen for these specific lifecycle events (e.g., Compute.PostProvision or Kubernetes-specific topics) to initiate the registration process.

VCF Operations orchestrator (B): This is the orchestration engine (formerly known as VMware Aria Automation Orchestrator or vRO). Documentation specifies that for CMDB and ITSM compliance, VCF Automation is integrated with VCF Operations orchestrator workflows. These workflows contain the complex technical logic required to:

Separate objects and feed inputs into technical integration tasks.

Handle API tokens and authentication for the external CMDB.

Execute the REST API calls to the CMDB (e.g., to the `cmdb_ci_vmware_instance` table).
Update custom properties (like `serviceNowSysId`) back into the deployment for future decommissioning lifecycle events.

Extract from VCF 9.0 Documentation:

"Enterprise users commonly integrate their Cloud Management Platform with an IT Service Management (ITSM) and Configuration Management Database (CMDB) platform for compliance. Following this example, you can integrate VCF Automation with ServiceNow for CMDB and ITSM using VCF Operations Orchestrator Client... This integration uses Event Subscriptions to trigger VCF Operations Orchestrator workflows."

VCF Automation 9.0 Administration: Creating and Managing Event Subscriptions for External System Integration.

Question: 100

An Administrator has been tasked with deploying an Organization for All Applications within a new VMware Cloud Foundation (VCF) Automation. During the regional networking creation step, which four NSX constructs will automatically be configured? (Choose four.)

- A. An outbound Source Network Address Translation (SNAT) rule
- B. A Default Virtual Private Cloud (VPC)
- C. A Provider Tier-0 Gateway
- D. A Virtual Distributed Switch (VDS)
- E. An NSX Transit Gateway
- F. A Virtual Private Cloud (VPC) connectivity profile
- G. An outbound Destination Network Address Translation (DNAT) rule

Answer: A, B, C, F

Explanation:

In VMware Cloud Foundation 9.0, the introduction of the Virtual Private Cloud (VPC) model within VCF Automation (formerly Aria Automation) simplifies multi-tenancy. When an administrator creates an organization and configures regional networking, the system automates the deployment of several high-level NSX objects to provide isolated networking for that organization's applications.

According to the VCF 9.0 Automation and Networking Guide:

A Provider Tier-0 Gateway (C): This is the top-level logical router in the VCF environment. During the regional networking setup, the system identifies or configures the Provider T0 to act as the primary exit point for North-South traffic for the organization.

A Virtual Private Cloud (VPC) connectivity profile (F): This profile defines the networking "flavor" (such as IP blocks, DNS, and security settings) that will be applied to the organization's VPCs. It acts as the template for how the VPC interacts with the provider's physical and logical infrastructure.

A Default Virtual Private Cloud (VPC) (B): Upon completing the organization setup, VCF Automation provisions a default VPC for that organization. This VPC serves as the logical container for the tenant's subnets, security groups, and routing.

An outbound Source Network Address Translation (SNAT) rule (A): To allow virtual machines within the newly created VPC to access external resources (the internet or corporate network) while using private IP space, the system automatically creates an outbound SNAT rule on the gateway associated with the VPC or the Provider T0.

Why other options are incorrect:

A Virtual Distributed Switch (VDS) (D): The VDS is a foundational component of the VCF VI Workload Domain created during Day 1 operations. It is not "automatically configured" during the high-level regional networking step of a VCF Automation organization; it must already exist.

An NSX Transit Gateway (E): While NSX uses Tier-0 and Tier-1 gateways for transit, "Transit Gateway" is a specific term often associated with public cloud (AWS) integrations. In the context of VCF 9.0 regional networking for a VPC, the core constructs are the T0/T1 and VPC profiles.

An outbound Destination Network Address Translation (DNAT) rule (G): DNAT is typically used for inbound traffic (mapping a public IP to a private internal IP). Outbound traffic uses SNAT to mask the internal IP as it leaves the organization.

VMware Cloud Foundation 9.0 Administration Guide: Configuring Organizations and VPCs in VCF Automation.

VMware NSX (VCF 9.0) Guide: Automated VPC Provisioning and Connectivity Profiles.

Question: 101

An administrator has deployed a new VMware Cloud Foundation (VCF) fleet. The fleet is currently running in evaluation mode. Which three steps must the administrator complete to license the fleet? (Choose three.)

- A. Add the license file from the VCF Business Services console to VCF Operations.
- B. Register the VCF Operations instance with the VCF Business Services console.
- C. Assign licenses to vCenter instances and NSX Manager from VCF Operations.
- D. Generate license keys in the VCF Business Service console for every component.
- E. Add license keys from the VCF Business Service console to VCF Operations.
- F. Assign licenses to vCenter instances from VCF Operations.

Answer: A, B, F

Explanation:

In VMware Cloud Foundation (VCF) 9.0, the licensing architecture has undergone a fundamental shift to simplify the management of large-scale deployments. The legacy method of managing individual 25-character license keys for every component (ESXi, vCenter, NSX, etc.) has been replaced by a unified, subscription-based License File model managed through VCF Operations. According to the VCF 9.0 Licensing and Administration Guide:

Register the VCF Operations instance with the VCF Business Services console (B): This is the mandatory first step. VCF Operations must be linked to the cloud-based VCF Business Services console (vcf.broadcom.com). This registration allows the environment to sync entitlements and report usage.

Add the license file from the VCF Business Services console to VCF Operations (A): Unlike previous versions that used keys, VCF 9.0 utilizes a "Secure License File" (or an activation code

that retrieves it). For environments without direct internet access (Disconnected Mode), the administrator must manually download this file from the Business Services console and upload it to the VCF Operations interface.

Assign licenses to vCenter instances from VCF Operations (F): Once the license file is added to VCF Operations, the "pool" of capacity (measured in Cores or TiBs) becomes available. The administrator then assigns the license specifically to the vCenter Server instances.

Documentation states: "License your vCenter, ESX hosts, NSX, VCF Operations, and other components by assigning the license to the vCenter instance." The vCenter then automatically handles the downstream entitlement for the hosts and integrated services.

Why other options are incorrect:

C: While NSX is licensed as part of the fleet, the administrative action in VCF 9.0 is to assign the license to the vCenter instance, which then licenses the "connected assets."

D & E: VCF 9.0 specifically "eliminates the need to manage multiple license keys" (except for certain legacy add-ons). The core fleet licensing uses a single License File rather than individual keys for every component.

VMware Cloud Foundation 9.0 Documentation: Licensing Overview and Registration.

VMware Cloud Foundation 9.0 Administration: Assigning Licenses to vCenter Server Instances.

Broadcom Technical Documents: VCF 9.0 Licensing and Compliance Guide.

Question: 102

As part of a new VMware Cloud Foundation (VCF) fleet, an administrator is tasked to deploy vSphere Supervisor utilizing VMware NSX networking. Which networking connectivity type should the administrator configure?

- A. Avi Load Balancer Controller IPs
- B. Data Network Subnet
- C. Distributed Gateway
- D. Centralized Gateway

Answer: C

Explanation:

In VMware Cloud Foundation 9.0, when deploying vSphere Supervisor (formerly part of Tanzu) specifically with VMware NSX as the networking provider, the architecture relies on the high-performance routing capabilities of the NSX fabric.

According to the VCF 9.0 Developer Ready Infrastructure Guide:

When NSX is selected as the networking stack for the Supervisor, the system utilizes Distributed Gateways (T1) to handle the routing for the supervisor's internal and external traffic.

Distributed Gateway (C): In an NSX-integrated Supervisor deployment, the East-West traffic and the localized routing for the Kubernetes Control Plane and Pod networking are handled by the Distributed Gateway. This ensures that routing occurs at the host level (kernel space) where possible, minimizing latency and "hairpinning" to a centralized edge node.

Why others are incorrect: * Avi Load Balancer (A): While Avi (NSX Advanced Load Balancer) is the preferred load balancer for VCF 9.0, the question asks for the "networking connectivity

type" for the Supervisor deployment itself. Avi provides the Load Balancing service (ingress/egress), but the underlying routing connectivity type is the Distributed Gateway.

Data Network Subnet (B): This is a general networking term and not a specific "connectivity type" construct within the NSX Supervisor deployment workflow.

Centralized Gateway (D): While a Tier-0/Tier-1 gateway can have centralized services (like NAT or Statefull Firewall), the standard connectivity model for Supervisor namespaces to maintain performance and scale across the VCF hosts is the Distributed Gateway.

VMware NSX 4.x/VCF 9.0 Integration Guide: Kubernetes Networking and Security with Distributed Gateways.

Question: 103

An administrator is responsible for managing a VMware Cloud Foundation (VCF) Automation organization within a VCF instance. The administrator has been tasked with updating an VMware NSX VPC by editing the NSX Connectivity profile for an NSX Project. The current profile was generated automatically when the NSX VPC was created.

What is the impact of the administrator making this change to the NSX VPC?

- A. All NSX VPCs associated with the VCF Automation organization will be updated with the new VPC connectivity profile.
- B. All NSX VPCs that use the default VPC connectivity profile will be updated with the new VPC connectivity profile.
- C. Only the selected NSX VPC will be updated with the new VPC connectivity profile.
- D. Only the NSX VPCs within the corresponding NSX Project will be updated with the new VPC connectivity profile.

Answer: C

Explanation:

In VMware Cloud Foundation (VCF) 9.0, the governance of Virtual Private Clouds (VPCs) allows for granular control over networking parameters. When a VPC is created in VCF 9.0, a VPC Connectivity Profile is automatically generated specifically for that instance if a pre-existing shared profile is not selected.

According to the VCF 9.0 Administration Guide (Networking Section):

VPC Isolation: Each NSX VPC serves as a distinct, isolated administrative and data plane boundary. While multiple VPCs can reside within a single NSX Project, their configurations—including the connectivity profiles—can be managed independently.

Profile Modification Impact: When an administrator edits the NSX Connectivity profile for a specific NSX Project and VPC, the system treats this as a targeted configuration update. Because the profile in this scenario was "generated automatically when the NSX VPC was created," it is uniquely associated with that specific VPC's lifecycle.

Scoped Changes: Modifying this specific profile does not trigger a global update across the entire VCF Automation organization, nor does it affect other VPCs within the project that may be using their own automatically generated or distinct profiles. This ensures that changes to one

tenant's or application's networking environment do not cause unintended disruptions to others.

VMware Cloud Foundation 9.0 Documentation: Editing VPC Connectivity Profiles in NSX Projects.
VMware NSX (VCF 9.0) Guide: Virtual Private Cloud (VPC) Lifecycle and Configuration Management.

Question: 104

An administrator is tasked to upgrade a VMware Cloud Foundation (VCF) environment from 5.2 to 9.0. During the preparation, the administrator can only see the SDDC Manager 9.0 bundle available to apply. Why are no other bundles available?

- A. SDDC Manager must be upgraded first.
- B. An offline repository was used for the upgrade bundles.
- C. A proxy server was used to download bundles.
- D. The ASYNC tool must be used to download all required upgrade bundles.

Answer: A

Explanation:

In VMware Cloud Foundation (VCF) 9.0, the Lifecycle Management (LCM) process follows a strict sequential upgrade path. The SDDC Manager (or the VCF Manager in version 9.0) acts as the central orchestrator for all metadata and bundle management for the entire Software-Defined Data Center (SDDC) stack.

According to the VCF 9.0 Upgrade and Migration Guide:

Sequential Bundle Availability: The SDDC Manager UI is designed to only display bundles that are compatible with its current running version. Because an SDDC Manager at version 5.2 does not possess the metadata or orchestration logic required to manage version 9.0 components (such as vCenter 9.0 or ESXi 9.0), those bundles are hidden from the "Available Bundles" list.

Orchestration Logic: To unlock the remaining components of the VCF 9.0 release, the SDDC Manager must be upgraded first. Once the SDDC Manager reaches version 9.0, it retrieves the new manifest from the VMware/Broadcom Depot. This manifest informs the SDDC Manager of the compatible versions for vCenter Server, NSX, and ESXi that constitute the 9.0 Bill of Materials (BOM).

Upgrade Order: The documented upgrade order for VCF 9.0 is:

Step 1: SDDC Manager

Step 2: vCenter Server (Management Domain)

Step 3: NSX (Management Domain)

Step 4: ESXi (Management Domain)

Step 5: Workload Domains (vCenter, NSX, then ESXi)

Why other options are incorrect:

B & C: While an offline repository or a proxy might affect the ability to download bundles, it would not selectively hide everything except for the SDDC Manager bundle if the repository was properly configured.

D: The Async Patch Tool (ASYNC tool) is used for applying individual patches or "out-of-band" updates that are not yet part of an official VCF release. It is not the standard tool for a major version upgrade from 5.2 to 9.0.

VMware Cloud Foundation 9.0 Lifecycle Management Guide: Sequential Upgrade Procedures.

VMware Cloud Foundation 9.0 Release Notes: Upgrade Path and Bill of Materials (BOM).

VCF 9.0 Administration Guide: Managing Software Bundles and SDDC Manager Updates.

Question: 105

An administrator is tasked with configuring a storage solution within a VMware Cloud Foundation (VCF) environment. The storage must be accessible to both client workstations and virtual machines.

Which VCF feature should an administrator configure to satisfy the requirement?

- A. vSAN Storage Cluster
- B. Local VMFS Datastore
- C. vSAN Stretched Cluster
- D. vSAN File Services

Answer: D

Explanation:

vSAN File Services is the appropriate feature because it provides file-sharing capabilities from a vSAN cluster and makes file shares accessible over standard file protocols. This allows file-based storage to be consumed by workloads such as virtual machines and external client systems.

vSAN File Services extends the functionality of a vSAN datastore by providing file shares rather than limiting storage consumption to virtual disks used by VMs. This makes it suitable when the requirement is for storage that needs to be accessible to systems outside the traditional VM datastore model.

The other options do not meet the stated requirement. A vSAN Storage Cluster provides distributed storage primarily as a datastore for virtual infrastructure but does not by itself provide client-accessible file shares. A local VMFS datastore provides block-based storage local to an ESX host and is not intended to provide shared file access to client workstations. A vSAN Stretched Cluster provides site-level availability and resiliency but does not itself address file-sharing requirements.

Therefore, the feature that satisfies the requirement for storage accessible to both client workstations and virtual machines is vSAN File Services.

Question: 106

An administrator plans to deploy a workload domain with VMware Virtual Machine File System on Fibre Channel (VMFS-FC) as principal storage. What must be completed before the hosts can be commissioned?

- A. Configure two 10 Gbps NICs for the storage network.
- B. Mount the VMFS datastore(s) on all the hosts.
- C. Enable pass-through mode on the storage controller.
- D. Create a network pool for the storage network.

Answer: B

Explanation:

For hosts that will be commissioned for a workload domain using VMFS on Fibre Channel as principal storage, the Fibre Channel storage must already be accessible to every ESX host before commissioning begins. VMware Cloud Foundation 9.0 explicitly states: "The VMFS datastore must be mounted on all the hosts before commissioning."

VCF also requires supported Fibre Channel HBAs and drivers, and the hosts must be able to access the FC array. Fibre Channel does not require a dedicated Ethernet storage network because FC traffic uses Fibre Channel HBAs and the SAN fabric rather than VMkernel-based IP storage networking.

A network pool must exist before host commissioning, but for VMFS-FC it is used for VCF host networking such as management and vMotion; it is not a dedicated Fibre Channel storage network. Therefore, option D is not the specific storage prerequisite asked here. Pass-through mode is also unrelated to FC principal storage.

=====

Question: 107

What is a valid use case for VMware Cloud Foundation (VCF) Operations for networks?

- A. Generating network reports.
- B. Configuring network automation jobs.
- C. Performing Crown Jewel Analysis.
- D. Providing logs from NSX components.

Answer: C

Explanation:

A documented use case of VCF Operations for networks is Crown Jewel Analysis. VMware Cloud Foundation 9.0 states that administrators can use Crown Jewel Analysis to identify possible lateral movement opportunities for an adversary based on existing network flow paths. Administrators can mark critical VMs or physical IP addresses as crown jewels and then analyze their connectivity, incoming flows, relationships, and potential exposure.

The documentation specifically provides the workflow Plan & Assess > Crown Jewel Analysis, where administrators can analyze reachability scores and determine how many lateral movements might be required to reach critical assets. It can also suggest firewall rules to improve security.

While VCF Operations for networks can generate various reports, option A is too generic. Network automation jobs are a VCF Operations automation capability, not a primary VCF Operations for networks use case. NSX log collection is handled by VCF Operations for Logs rather than Operations for networks.

=====

Question: 108

An administrator has been tasked with configuring regions in VMware Cloud Foundation (VCF) Automation to provide resources reflecting different service classes to VCF Automation Organizations.

The following information has been provided:

Regions should provide Gold, Silver, and Bronze service classes.

Gold should use VMware vSAN storage.

Silver should use NFS storage.

Bronze should use VMFS on Fibre Channel storage.

A new VCF fleet will contain one VCF instance with three workload domains.

Which two items should the administrator validate as part of the VCF deployment to allow creation of the three regions? (Choose two.)

- A. All required VM classes are present and have the same names across all VMware vCenter instances.
- B. The vSphere Supervisor is enabled on each workload domain vCenter instance.
- C. Each workload domain vCenter is integrated with a VMware NSX Manager instance.
- D. A Region Quota is created for each region.
- E. All required Storage classes are present and have the same names across all VMware vCenter instances.

Answer: B, C

Explanation:

A VCF Automation region is built from one or more vSphere Supervisors, and the participating vCenter instances must be integrated with an NSX Manager. VMware Cloud Foundation 9.0 states that before creating a region, administrators must verify that the vCenter instance has a Supervisor enabled.

The documentation also states that VCF Automation creates a region by grouping Supervisors from one or more vCenter instances, provided those vCenter instances are configured with the same NSX instance. A single NSX Manager must therefore integrate with all vCenters participating in a particular region.

Options A and E apply when multiple Supervisors/vCenters are combined into one region because VM classes and storage classes must then be identical across those participating

instances. In this scenario, the design is for three separate service-class regions backed by three workload domains, so identical classes across all vCenters are not inherently required. Region quotas are created after regions exist and are assigned to Organizations; they are not prerequisites for creating the regions themselves.

Question: 109

An administrator wants to implement a solution that will centrally manage and distribute Virtual Machine (VM) templates, ISO images, and other files across multiple physical locations and VMware Cloud Foundation (VCF) instances. Which solution should the administrator implement?

- A. vSAN Storage Cluster
- B. Shared VMFS datastore
- C. Content Library
- D. Network File Copy

Answer: C

Explanation:

The correct solution is Content Library. VMware vSphere and VCF documentation define content libraries as container objects for storing and sharing VM templates, vApp templates, ISO images, text files, and other content. The documentation specifically states that content libraries can be used to “share content across vCenter instances in the same or different locations,” which directly matches the requirement to centrally distribute content across multiple physical sites and VCF instances.

VCF 9.0 further explains that content libraries can distribute VM and vApp templates, ISO images, and other files across vCenter instances, promoting “consistency, compliance, efficiency, and automation in deploying workloads at scale.” Local libraries can be published, while subscribed libraries synchronize content from a publisher.

A vSAN Storage Cluster and shared VMFS datastore provide storage capacity but are not content-distribution mechanisms. Network File Copy is a file-transfer operation rather than a centralized management and synchronization service.

=====

Question: 110

An administrator is tasked with deploying a new VMware vSAN-backed vSphere cluster.

The existing VMware Cloud Foundation (VCF) instance has two workload domains.

Each workload domain has one VMware vSphere cluster.

The administrator is required to lifecycle and scale the components related to the new vSphere cluster separately from the existing clusters.

Which action must the administrator take when deploying the new cluster?

- A. Deploy the new vSphere cluster as a new workload domain with shared NSX within the existing VCF instance.
- B. Deploy the new vSphere cluster on one of the non-management workload domains within the existing VCF instance.
- C. Deploy the new vSphere cluster as a new workload domain with a new NSX instance within the existing VCF instance.
- D. Deploy the new vSphere cluster on one of the existing workload domains within the existing VCF instance.

Answer: A

Explanation:

A workload domain is the appropriate lifecycle boundary when components must be managed independently. VCF 9.0 defines a workload domain as a logical pool containing its own vCenter and one or more vSphere clusters, while NSX Manager can be shared with other workload domains.

The VCF architecture documentation also identifies independent lifecycle management as a benefit of workload domains. A separate workload domain provides its own vCenter management boundary, allowing the new cluster and its associated components to be scaled and lifecycle-managed separately from existing domains.

A new NSX instance is not required simply to obtain independent lifecycle and scaling. VCF explicitly supports sharing an NSX Manager among workload domains, and VCF 9.0 describes shared NSX as a supported cross-workload-domain architecture. Therefore, creating a new workload domain while sharing the existing NSX instance satisfies the requirement with less management overhead than deploying another NSX stack.

=====

Question: 111

An administrator is responsible for managing a VMware Cloud Foundation (VCF) fleet. The administrator has been tasked with the following:

Ensure that newly deployed Virtual Machines create a DNS A and DNS PTR record in DNS.

Create the DNS records before each Virtual Machine is deployed.

If a deployment fails, ensure that the created DNS record is deleted.

Only remove the DNS records for each Virtual Machine after it is destroyed.

Every workflow must be allowed to complete before starting any additional workflow for the same event topic.

The administrator has already created the required VCF Operations Orchestrator workflows, Event Subscriptions, and blueprint properties for hostname and domainName.

What must the administrator configure within the Event subscription to ensure that the DNS record is only created when the domain name is provided?

- A. Add the Delete DNS Records workflow as the Recovery Workflow of the Add DNS Records subscription.
- B. Enable the Block execution of events in topic option in the Add DNS Records and Delete DNS Records subscriptions.
- C. Add the event.data.customProperties['hostname'] != null condition to the Add DNS Records and Delete DNS Records subscriptions.
- D. Add the event.data.customProperties['domainName'] != null condition to the Add DNS Records and Delete DNS Records subscriptions.

Answer: D

Explanation:

VCF Automation event subscriptions support Boolean conditions that determine whether the associated workflow runs. VCF 9.0 states that filters can be applied to subscriptions so that “the event and workflow only triggers if the Boolean expression is ‘true’.” Conditions can access event payload values through event.data, and the != operator is explicitly supported.

Because the stated requirement is specifically to create DNS records only when domainName has been provided, the subscription must test the corresponding custom property:
event.data.customProperties['domainName'] != null

Option C checks hostname, which does not satisfy the stated condition. Option B addresses execution ordering: blocking subscriptions prevent another matching subscription from receiving the event until the current runnable item finishes. Option A is relevant to cleanup if the primary workflow fails because VCF supports recovery runnable items for blocking subscriptions, but it does not determine whether the DNS workflow should run based on the presence of the domain name.

Question: 112

A private cloud administrator is responsible for the management of a VMware Cloud Foundation (VCF) environment and has been tasked with creating a new Organization in VCF Automation. The customer previously upgraded from VCF 5.2 and this is the first new Organization since their upgrade.

The following requirements have been provided for the additional Organization:

Support Kubernetes deployment using VMware Kubernetes Service (VKS).

Use third-party integrations, including GitHub and GitLab.

Support virtual machine (VM) deployments.

What action should the administrator take to complete the objective?

- A. Create the new Organization for All Applications within the VCF Automation Provider Management Portal.
- B. Create the new Organization for VM Applications using the VCF Automation Provider Management Portal.
- C. Create the new Organization for VM Applications within the VCF Operations Fleet Management API.
- D. Create the new Organization for VM Applications using the VCF Automation API.

Answer: A

Explanation:

VCF Automation 9.0 defines Organizations for All Applications as the primary multi-tenancy model for environments that need both traditional VM workloads and modern Kubernetes-based workloads. The documentation states that an All Apps organization can run “a wide variety of applications, including virtual machines (VMs), Kubernetes, data services, and so on.” The same documentation specifies that these organizations are created from the VCF Automation Provider Management Portal and use underlying vSphere Supervisor infrastructure. This directly satisfies the requirements for VKS and VM deployment.

By contrast, a VM Apps organization is primarily intended for customers continuing legacy Aria Automation-style VM application provisioning. The documentation states that it is most suitable for customers who want to continue “VM-based applications” without disrupting existing operations. It is not the correct choice when Kubernetes and modern integrations are required.

=====

Question: 113

An administrator is responsible for managing a VMware Cloud Foundation (VCF) solution. A 3-node vSAN Express Storage Architecture (ESA) cluster currently runs workloads using a storage policy configured with RAID-5. The administrator has been tasked with enabling auto-policy management in vSAN ESA.

Given the scenario, what is the minimum number of hosts required for running workloads with RAID-5?

- A. 2
- B. 3
- C. 4
- D. 6

Answer: C

Explanation:

VCF 9.0 documents an important distinction between manually configured RAID-5 and RAID-5 when auto-policy management is enabled. The documentation explicitly states: “RAID-5 in vSAN ESA supports three ESX host clusters. If you enable auto-policy management, the cluster must have four ESX hosts to use RAID-5.”

Therefore, although the existing three-node ESA cluster can support RAID-5 under a manually configured policy, enabling auto-policy management changes the minimum cluster size requirement to four hosts.

Auto-policy management automatically generates an optimal datastore policy based on the cluster topology and the number of ESX hosts. VCF design guidance also recommends at least

four nodes for vSAN ESA clusters because this allows vSAN to create a capacity-optimized default policy and provides better ability to re-protect objects following a host failure. Six hosts are required for RAID-6, not RAID-5.

=====

Question: 114

An administrator is responsible for the management of a VMware Cloud Foundation (VCF) environment that consists of two VCF Automation tenants, Production and Development.

The administrator has been tasked with the following:

Configure a new project within the Development tenant to support the creation of a new Kubernetes-based application.

Ensure that, as the development team onboards new members, the ongoing management overhead of the project membership is minimized.

Which four of the following steps should the administrator take to meet the objective? (Choose four.)

- A. Log in to the Development tenant as an Organization Administrator.
- B. Assign at least one Namespace to the Project.
- C. Assign both Project Administrators and Project Members to the Project using Active Directory Users.
- D. Log in to the Development tenant as a Project Administrator.
- E. Create a new Project.
- F. Assign both Project Administrators and Project Members to the Project using Active Directory Groups.
- G. Assign at least one Cloud Zone to the Project.

Answer: A, B, E, F

Explanation:

Because this project must support a Kubernetes-based application, the applicable VCF Automation model is All Apps, where projects consume resources through vSphere Namespaces, not legacy VM Apps cloud zones. VCF 9.0 states that an Organization Administrator can create and delete projects, whereas the Project Administrator manages an existing project but does not create new projects.

The administrator therefore logs in as the Organization Administrator and creates the new project. The documentation states that when configuring a project, the administrator adds at least one namespace so users can start provisioning resources. Namespaces provide the resource envelope for workloads including VKS clusters.

To minimize ongoing membership administration, VCF explicitly recommends assigning roles using groups. The documentation explains that group-based roles allow users to “come and go from your identity provider rather than requiring the project administrator to constantly update the individual users.” Therefore, Active Directory groups should be assigned rather than individual users.

Question: 115

An administrator has been tasked with the deployment of a new VMware Cloud Foundation (VCF) solution. The design for the solution states:

There will be a single VCF Instance within the new VCF Fleet.

The VCF instance will consist of a management domain and three workload domains.

VCF Operations will be deployed in Continuous Availability Mode within the new VCF instance.

Which three steps must the administrator perform to complete the deployment of the VCF solution to meet the stated design requirements? (Choose three.)

- A. In the VCF Installer Deployment Wizard, select the option to connect to an existing VCF Operations instance.
- B. Manually deploy a new VCF Operations Continuous Availability cluster into the new VCF instance.
- C. Convert the VCF Operations High Availability Mode Cluster within the new VCF fleet to Continuous Availability Mode.
- D. Manually deploy a VCF Operations Witness node into the new VCF instance.
- E. Use a JSON Specification file to deploy the VCF Fleet without a VCF Operations instance.
- F. Use the VCF Installer Deployment Wizard to deploy the VCF fleet with VCF Operations in High Availability Mode.

Answer: C, D, F

Explanation:

For a new VCF fleet in which VCF Operations ultimately needs to operate in Continuous Availability (CA) mode, the initial deployment is performed using the supported VCF Installer workflow with VCF Operations in High Availability (HA) mode. Therefore, F is required as the starting deployment configuration.

After the VCF Operations HA deployment is operational, the cluster is converted from High Availability mode to Continuous Availability mode, making C the second required action.

Continuous Availability uses a dual-site architecture and requires a witness node to participate in determining cluster availability and prevent split-brain conditions. Consequently, the administrator must also deploy the required VCF Operations Witness node, making D the third required step.

Option A applies when an existing VCF Operations deployment is available to connect to, which contradicts the scenario of deploying a new VCF fleet. Option B incorrectly suggests deploying a separate CA cluster rather than converting the deployed HA cluster. Option E would omit VCF Operations during initial fleet deployment and does not follow the required deployment sequence.

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

**Check our Customer Testimonials and ratings
available on every product page.**

Visit our website.

<https://examsempire.com/>