ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

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 dat a. 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.

Reference: VMware Cloud Foundation 9.0 – NSX Networking and VKS Deployment Guide (Tier-0 Gateway connectivity model).

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.

Reference: VMware Cloud Foundation 9.0 Automation Guide – Organizations for All Applications (unified management of VMs, Kubernetes, third-party integrations, and public cloud endpoints).

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.

Reference: vSphere 9.0 Resource Management Guide – Resource Pools section; VMware Cloud Foundation 9.0 Administration Guide (delegation of compute resources using 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).
Reference: VMware Cloud Foundation 9.0 Convergence and Migration Guide – Unsupported Configurations (ELM), Lifecycle Manager Requirements (Images only).

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. Reference: VMware Cloud Foundation 9.0 – Automation Guide (Custom Resources, Content Hub, Orchestrator integrations, AD plugin usage).

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 ES A. 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).

Reference: VMware Cloud Foundation 9.0 – Operations Guide, Access Control and Identity Broker sections (time-bound access policies and dashboard sharing).

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: D

Explanation:

The VCF 9.0 Operations Guide – Alerts and Policies explains how alert cycles are calculated:
Wait Cycle: The number of consecutive collection cycles that the symptom must remain true before the alert is triggered.
Cancel Cycle: The number of consecutive collection cycles that the symptom must not be true before the alert is canceled.
Default Collection Interval: VCF Operations collects data every 5 minutes by default.
Given the settings:
Wait cycle = 2 → The condition must persist for 2 × 5 minutes = 10 minutes before the alert triggers. Cancel cycle = 2 → The condition must clear for 2 × 5 minutes = 10 minutes before the alert cancels. Thus, the total elapsed time between the symptom being triggered and the alert being automatically canceled (if unresolved) is 10 minutes wait + 10 minutes cancel = 20 minutes.
Other options:
40 minutes (A) assumes a longer interval but is incorrect.
4 minutes (B) and 10 minutes (C) do not align with the default 5-minute cycle × 2 logic.
Therefore, the correct answer is 20 minutes.
Reference: VMware Cloud Foundation 9.0 Operations Guide – Alerts section (Wait Cycles, Cancel Cycles, and Collection Intervals).

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 ofline 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. Ofline 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.
Reference:
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: C

Explanation:

The VMware Cloud Foundation 9.0 NSX Projects and VPC Guide outlines the prerequisites for configuring external connectivity using a Transit Gateway (TGW). When VLAN-backed external connectivity is used, the documentation specifies:
"For VLAN-backed external connectivity, ensure that all hosts in the workload cluster where VPC workloads run have physical access to the VLAN(s) used by the Transit Gateway. This ensures end-to- end packet reachability between VPC segments and the physical router."
Analysis of options:
A (TWO BGP Peers): BGP can be configured later to enable dynamic routing but is not a prerequisite for establishing VLAN-backed connectivity.
B (TNP attached): A Transport Node Profile is required for NSX host preparation, but it is part of the general NSX setup, not the specific prerequisite for TGW VLAN external connectivity.
C (Access to VLANs): This is the critical prerequisite—hosts running workloads must have access to the external VLANs. Without this, connectivity to the physical routers will fail.
D (Access to Edge TEP network): TEP networks are used for overlay traffic (Geneve encapsulation), not for VLAN-backed TGW external connectivity.
Therefore, the correct prerequisite is ensuring all VPC workload hosts have access to the VLAN(s) used by the Distributed TGW.
Reference:
VMware Cloud Foundation 9.0 NSX Networking Guide – VPC External Connectivity (Transit Gateway VLAN-backed requirements).
NSX Project/VPC documentation: VLAN access prerequisites for external connectivity.

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.
Reference: VMware Cloud Foundation 9.0 – Automation Guide, Service Broker section (role in VM Apps tenant catalog services).

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.

Reference: VMware Cloud Foundation 9.0 – Kubernetes Services and Data Protection (Velero integration).

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.

Reference: VMware Cloud Foundation 9.0 – Automation Documentation (Property Groups for input and constant standardization).

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.

Reference: VMware Cloud Foundation 9.0 – Automation and Resource Policy Documentation (IaaS Resource Policies for Supervisor-based Kubernetes clusters).

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 selfservice 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.

Reference: VCF 9.0 Overview & Capabilities (What Is VCF), Organizations & Isolation, All Apps organizations.

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.

Reference: NSX Networking in VCF 9.0 – Transport Zones & VLAN Segment creation.

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.

Reference: VMware Cloud Foundation 9.0 – Operations Guide, Custom Groups and Policy Inheritance.

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.
Reference: vSphere 9.0 – Enhanced vMotion Compatibility (EVC) Overview and Configuration.

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.

Reference: VCF 9.0 Licensing – "Update Licenses in Connected Mode" and Licensing Overview (update cycle and consequences).

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.

Reference: VMware Cloud Foundation 9.0 – Operations Guide, "Working with Views" (List View supports tabular data and CSV export).

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.
Reference: VMware Cloud Foundation 9.0 – Operations Guide, Super Metrics section (aggregating and computing metrics across objects).

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. Install ESX using VCF Installer → Configure host settings → Perform hardware compatibility check → Create datastores

B. Hardware validation → Network configuration → ESX installation → Join vCenter

C. Boot from installation media → Select target disk → Configure management network → Set root password

D. Install vCenter Server → Configure cluster settings → Deploy ESX using VCF Installer → Create virtual machines

Answer: C

Explanation:

The VMware Cloud Foundation 9.0 Deployment Guide and the vSphere 9.0 Installation and Setup documentation describe the standard manual ESXi installation workflow. The steps are as follows: Boot from installation media: The host is started from the ESXi ISO image, either via physical media, virtual media through iLO/iDRAC, or PXE boot.

Select target disk: During setup, administrators select the disk or device where ESXi will be installed. Configure management network: After installation, the Direct Console User Interface (DCUI) is used to set up basic network parameters for the management interface (IP address, DNS, gateway).

Set root password: A secure root password is set to complete the initial setup of the host.

The documentation makes it clear that these steps form the foundation before the host can be discovered and commissioned by SDDC Manager in VMware Cloud Foundation.

Option A is incorrect because the VCF Installer is not used for installing ESXi; it is used for deploying management domains and workload domains.

Option B includes "Join vCenter," which happens after commissioning, not during installation.

Option D is incorrect since vCenter Server is installed later, not during the ESXi manual setup.

Therefore, the correct stages of manual ESXi installation are: Boot media → Select disk → Configure management network → Set root password.

Reference:

VMware Cloud Foundation 9.0 Deployment Guide – ESXi Host Preparation section.

VMware vSphere 9.0 Installation and Setup Guide – "Installing ESXi" and "Configuring the Direct Console User Interface (DCUI)."

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.

Reference: VMware Cloud Foundation 9.0 – Automation Guide, Content Hub and Content Sharing Policy sections.