

VMware.2V0-17.25.v2026-07-14.q45

Exam Code:	2V0-17.25
Exam Name:	VMware Cloud Foundation 9.0 Administrator
Certification Provider:	VMware
Free Question Number:	45
Version:	v2026-07-14
# of views:	104
# of Questions views:	479
https://www.freecram.net/torrent/VMware.2V0-17.25.v2026-07-14.q45.html	

NEW QUESTION: 1

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: (SHOW ANSWER)

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 .

References: NSX Networking in VCF 9.0 - Transport Zones & VLAN Segment creation.

NEW QUESTION: 2

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: (SHOW ANSWER)

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.

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

NEW QUESTION: 3

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: (SHOW ANSWER)

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 .

NEW QUESTION: 4

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: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation:

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).

NEW QUESTION: 5

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: ([SHOW ANSWER](#))

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.

References: * VMware Cloud Foundation 9.0 Administration Guide: Monitoring and Troubleshooting the SDDC.

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

NEW QUESTION: 6

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: (SHOW ANSWER)

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 .

NEW QUESTION: 7

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: ([SHOW ANSWER](#))

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.

NEW QUESTION: 8

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 RAID-1 storage policy.
- D. Configure the twelve ESX hosts into six fault domains.

Answer: ([SHOW ANSWER](#))

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.

NEW QUESTION: 9

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: ([SHOW ANSWER](#))

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).

NEW QUESTION: 10

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: ([SHOW ANSWER](#))

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 .

NEW QUESTION: 11

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: ([SHOW ANSWER](#))

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.

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

NEW QUESTION: 12

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 (LEAVE A REPLY)

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) .

References: VMware Cloud Foundation 9.0 Convergence and Migration Guide - Unsupported Configurations (ELM), Lifecycle Manager Requirements (Images only).

NEW QUESTION: 13

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: (SHOW ANSWER)

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.

NEW QUESTION: 14

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: ([SHOW ANSWER](#))

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.

NEW QUESTION: 15

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: ([SHOW ANSWER](#))

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 .

NEW QUESTION: 16

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: (SHOW ANSWER)

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.

Valid 2V0-17.25 Dumps shared by EduDump.com for Helping Passing 2V0-17.25 Exam!

EduDump.com now offer the **newest 2V0-17.25 exam dumps**, the EduDump.com 2V0-17.25 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com 2V0-17.25 dumps with Test Engine here:

<https://www.edudump.com/exams/VMware/2V0-17.25/premium/> (**107** Q&As Dumps, **35%OFF**

Special Discount Code: freecram)

NEW QUESTION: 17

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: (SHOW ANSWER)

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).

NEW QUESTION: 18

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: ([SHOW ANSWER](#))

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).

NEW QUESTION: 19

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: (SHOW ANSWER)

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)

NEW QUESTION: 20

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: (SHOW ANSWER)

Comprehensive and Detailed Explanation:

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.

NEW QUESTION: 21

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: (SHOW ANSWER)

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.

References:

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

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

NEW QUESTION: 22

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: ([SHOW ANSWER](#))

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.

NEW QUESTION: 23

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: (SHOW ANSWER)

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.

References: VMware Cloud Foundation 9.0 - Automation Guide, Content Hub and Content Sharing Policy sections.

NEW QUESTION: 24

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: (SHOW ANSWER)

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.

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

NEW QUESTION: 25

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: (SHOW ANSWER)

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.

References: VMware Cloud Foundation 9.0 - Operations Guide (Configuration Management and Drift Detection), vSphere 8.0 U3 Configuration Profiles Documentation.

NEW QUESTION: 26

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

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 27

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. 4
- C. 3
- D. 6

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 28

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 ([LEAVE A REPLY](#))

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.

NEW QUESTION: 29

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: ([SHOW ANSWER](#))

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 .

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

NEW QUESTION: 30

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 ([LEAVE A REPLY](#))

<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>

NEW 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: (SHOW ANSWER)

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.

Valid 2V0-17.25 Dumps shared by EduDump.com for Helping Passing 2V0-17.25 Exam!

EduDump.com now offer the **newest 2V0-17.25 exam dumps**, the EduDump.com 2V0-17.25 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com 2V0-17.25 dumps with Test Engine here:

<https://www.edudump.com/exams/VMware/2V0-17.25/premium/> (**107** Q&As Dumps, **35%OFF**

Special Discount Code: freecram)

NEW QUESTION: 32

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: (SHOW ANSWER)

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.

NEW QUESTION: 33

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: (SHOW ANSWER)

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.

References: VMware Cloud Foundation 9.0 - Kubernetes Services and Data Protection (Velero integration).

NEW QUESTION: 34

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: ([SHOW ANSWER](#))

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.

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

NEW QUESTION: 35

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: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation:

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.

NEW QUESTION: 36

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: ([SHOW ANSWER](#))

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.

NEW QUESTION: 37

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: ([SHOW ANSWER](#))

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.

NEW QUESTION: 38

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 ([LEAVE A REPLY](#))

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.

NEW QUESTION: 39

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: (SHOW ANSWER)

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.

NEW QUESTION: 40

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: ([SHOW ANSWER](#))

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.

References: vSphere 9.0 Resource Management Guide - Resource Pools section; VMware Cloud Foundation

9.0 Administration Guide (delegation of compute resources using Resource Pools).

NEW QUESTION: 41

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: ([SHOW ANSWER](#))

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.

NEW QUESTION: 42

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: ([SHOW ANSWER](#))

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.

NEW QUESTION: 43

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: ([SHOW ANSWER](#))

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 .

NEW QUESTION: 44

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: ([SHOW ANSWER](#))

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.

NEW QUESTION: 45

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: ([SHOW ANSWER](#))

References: VMware Cloud Foundation 9.0 Deployment Guide - Core Components for VCF Instance Deployment and Fleet Architecture Overview.

Valid 2V0-17.25 Dumps shared by EduDump.com for Helping Passing 2V0-17.25 Exam!

EduDump.com now offer the **newest 2V0-17.25 exam dumps**, the EduDump.com 2V0-17.25 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com 2V0-17.25 dumps with Test Engine here:

<https://www.edudump.com/exams/VMware/2V0-17.25/premium/> (107 Q&As Dumps, **35%OFF**

Special Discount Code: freecram)