



Get Free VMware 2V0-17.25 Dumps PDF Questions

Why risk failure? Download updated VMware Cloud Foundation 9.0 Administrator exam PDF questions today. Practice with real 2V0-17.25 dumps and verified answers designed to help you ace your certification quickly using PrepBolt 2V0-17.25 exam pdf questions and answers.

Thank you for Downloading 2V0-17.25 exam PDF Demo

<https://prepbolt.com/2V0-17.25.html>

QUESTIONS & ANSWERS
DEMO VERSION
(LIMITED CONTENT)

Question 1

Question Type: MultipleChoice

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

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

Options:

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

Answer:

D, E

Explanation:

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

According to the VCF 9.0 Operations and Monitoring Guide:

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

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

Why other options are incorrect:

VCF Operations Service/Application Discovery (A & C): These features are used to map relationships

between virtual machines and services to understand dependencies. While they help identify what is running, they do not provide the deep 'monitoring' (log analysis and alerting) requested for a mix of internal and open-source apps.

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

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

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

Question 2

Question Type: MultipleChoice

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?

Options:

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

Answer:

A

Explanation:

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

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

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

When an administrator intentionally places a legitimate DHCP server on a segment:

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

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

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

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

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

Question 3

Question Type: MultipleChoice

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

Options:

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

Answer:

D, E, F

Explanation:

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

According to the documentation:

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

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

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

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

Question 4

Question Type: MultipleChoice

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?

Options:

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

Answer:

C

Explanation:

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

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

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

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

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

Question 5

Question Type: MultipleChoice

An administrator is tasked to replace a certificate of a component in a VMware Cloud Foundation (VCF) environment with an external Certificate Authority (CA)-signed certificate.

What format should the administrator use when creating the certificate?

Options:

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

Answer:

C

Explanation:

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

vCenter Server

NSX Manager

SDDC Manager

Aria Suite components

require certificates to be provided in PEM format.

From the VCF 9.0 documentation under Certificate Management:

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

Additionally:

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

Why PEM?

PEM format:

Base64 encoded

Human-readable

Common format for VMware components

Required for SDDC Manager certificate import workflows

Why the Other Options Are Incorrect

A . PFX (PKCS#12)

Contains private key and certificate bundled together; not the required format for VCF certificate replacement workflows.

B . DER

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

D . P7B (PKCS#7)

Does not contain private key; unsuitable for certificate replacement.

Question 6

Question Type: MultipleChoice

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

The following requirements must be met:

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

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

All other settings should be in a default setting.

Name the new policy for all clusters "Resources."

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

Options:

A- Create a new policy 'Resources' under 'Base Settings' and define the cost for CPU, memory, and storage.

B- Set the 'Default Policy' as default.

C- Create a new policy under 'Base Settings' and define the cost for VM setup charges for the SAP HANA cluster.

D- Create a new policy under 'Default Policy' and define the cost for VM setup charges for the SAP HANA cluster.

E- Set the 'Resources' policy as default.

F- Create a new policy under 'Resources' and define the cost for VM setup charges for the SAP HANA cluster.

Answer:

A, E, F

Explanation:

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

From the VCF 9.0 documentation under Cost and Chargeback Configuration:

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

To meet the requirement:

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

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

Thus:

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

This satisfies:

Same CPU, memory, and storage cost across clusters.

From the documentation regarding policy hierarchy:

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

2 Set "Resources" as the default policy (Option E)

This ensures:

All clusters inherit this pricing model.

Other unspecified settings fall back to default behavior.

From documentation regarding overrides:

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

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

This satisfies:

VM setup charges applied only to SAP HANA cluster.

Other clusters remain unaffected.

All other settings remain default.

Why Other Options Are Incorrect

B -- Setting Default Policy as default contradicts requirement to create a new named policy "Resources."

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

D -- Incorrect hierarchy; policies are structured under custom policy trees, not under "Default Policy" in this context.

Document Reference (VCF 9.0):

VMware Cloud Foundation 9.0 VCF Operations Costing and Chargeback

VMware Cloud Foundation 9.0 Policy Inheritance and Overrides

VMware Cloud Foundation 9.0 Base Settings and Custom Cost Policies

Question 7

Question Type: MultipleChoice

Which statement correctly describes cluster API?

Options:

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

Answer:

A

Question 8

Question Type: MultipleChoice

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?

Options:

A- 6

B- 2

C- 3

D- 4

Answer:

A

Thank You for trying 2V0-17.25 PDF Demo

To try our 2V0-17.25 practice exam software
visit link below

<https://prepbolt.com/2V0-17.25.html>

Start Your 2V0-17.25 Preparation

Use Coupon "SAVE50" for extra 50% discount on the purchase of Practice Test Software. Test your 2V0-17.25 preparation with actual exam questions.