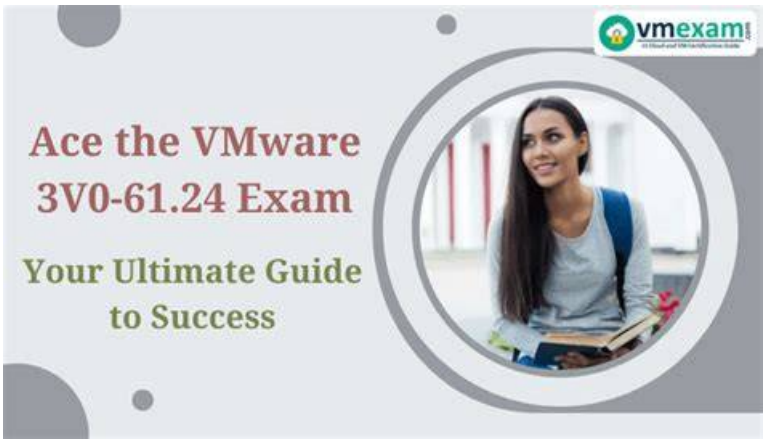
3V0-24.25 Valid Test Syllabus | 3V0-24.25 Vce Files



We provide you with two kinds of consulting channels if you are confused about some questions on our 3V0-24.25 study materials. You can email us or contact our online customer service. We will reply you as soon as possible. You are free to ask questions about 3V0-24.25 training prep at any time since that we are working 24/7 online. Our staff is really very patient and friendly. They are waiting to give you the most professional suggestions on our 3V0-24.25 exam questions.

VMware 3V0-24.25 Exam Syllabus Topics:

Section	Weight	Objectives
Security and Access Control	20%	- Network security and isolation - Compliance and hardening - Identity and access management • 1. Role-Based Access Control (RBAC) • 2. Integration with vCenter SSO - Security policies and workload protection
vSphere Kubernetes Architecture and Components	25%	- Core VKS components • 1. Container Network Interface (CNI) • 2. Cloud Provider Interface • 3. Container Storage Interface (CSI) - Supervisor Cluster design and functionality • 1. Single-zone and multi-zone architectures • 2. Integration with VMware Cloud Foundation
Resource Management and Operations	25%	- Backup and recovery with Velero Plugin - Monitoring, logging and troubleshooting - Compute, storage and network resource allocation - Cluster lifecycle management • 1. Upgrades and updates • 2. Scaling and maintenance
Deployment and Configuration	30%	- VKS deployment planning and prerequisites - Cluster creation and configuration • 1. Resource pool configuration • 2. Workload cluster provisioning - Integration with vCenter Server and NSX

>> 3V0-24.25 Valid Test Syllabus <<

First-grade 3V0-24.25 Valid Test Syllabus – Find Shortcut to Pass 3V0-24.25 Exam

According to our information there is a change for 3V0-24.25, I advise you to take a look at our latest VMware 3V0-24.25 reliable exam guide review rather than pay attention on old-version materials. You can regard old-version materials as practice questions to improve your basic knowledge. If you are searching the valid 3V0-24.25 Reliable Exam Guide review which includes questions and answer of the real test, our products will be your only choice.

VMware Advanced VMware Cloud Foundation 9.0 vSphere Kubernetes Service Sample Questions (Q71-Q76):

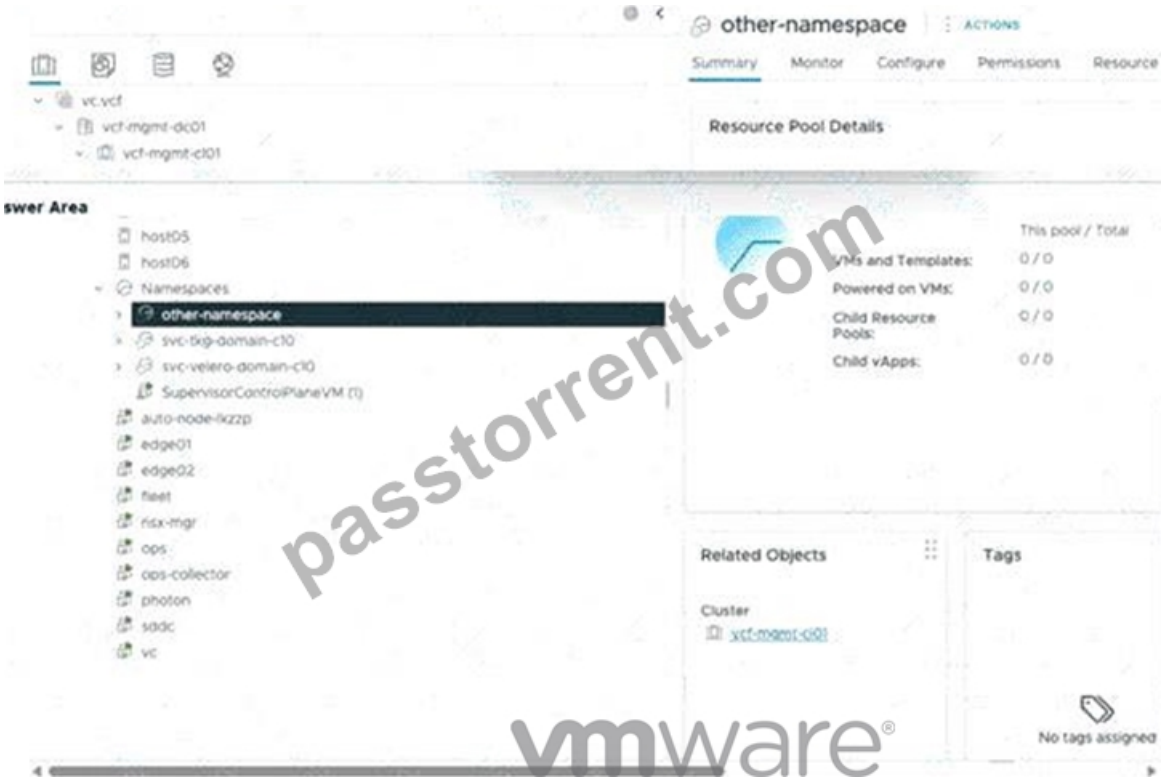
NEW QUESTION # 71
An administrator enabled cluster scaling by running kubectl edit deployment and updating the number of replicas from 5 to 10. When the cluster was redeployed with the number of replicas set to 5, what was the result?

- A. The autoscaling YAML file was not updated.
- B. The Supervisor YAML file was not updated to enable autoscaling.
- C. The cluster YAML file was not updated to reflect the requested number of pods.
- D. The cluster did not have sufficient resources to deploy the requested number of pods.

Answer: C

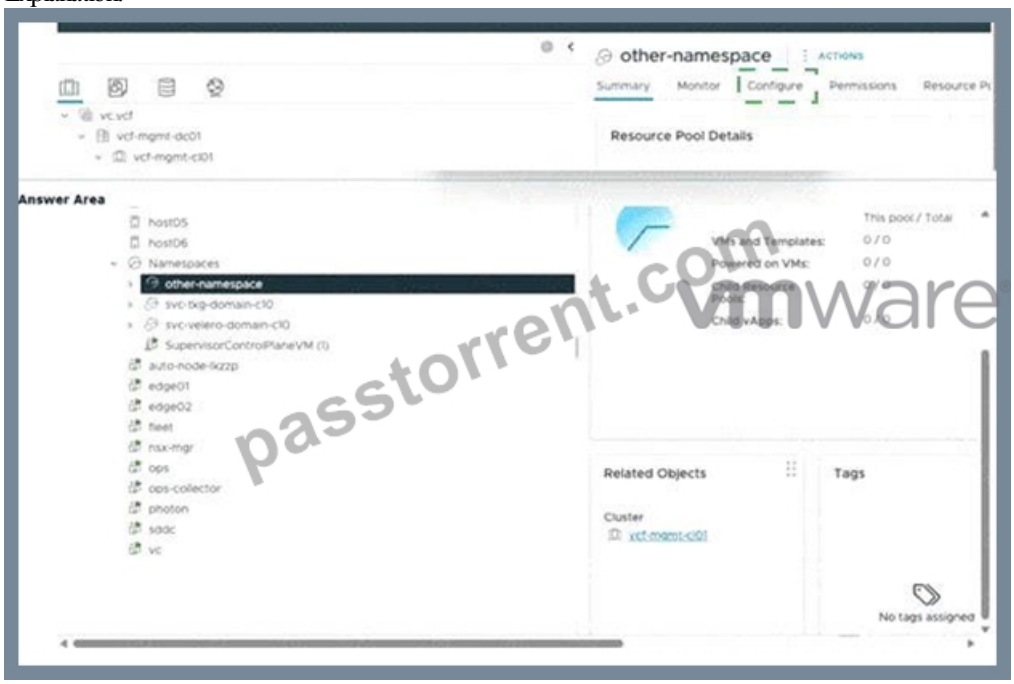
Explanation:
In a vSphere Kubernetes Service (VKS) environment, resource management follows aDeclarative Model.
When an administrator uses kubectl edit deployment to manually scale a running workload from 5 to 10 replicas, they are modifying thelive stateof the deployment. However, thesource of truthfor a Tanzu Kubernetes cluster in VCF 9.0 is theCluster YAML specificationmaintained by the Cluster API (CAPI) provider within the Supervisor.
If the administrator redeploys the cluster or if the Supervisor's controller performs a reconciliation loop, it refers back to the original configuration file. If that cluster YAML file still defines the replica count as 5, the Supervisor will terminate the 5 "extra" pods to match the desired state defined in the configuration. This is a common administrative pitfall; for changes to be persistent across redeployments or updates in VCF 9.0, the underlying manifest (the "Desired State") must be updated. Manually editing the live object only provides a temporary change that will be overwritten during the next synchronization or lifecycle event because the cluster YAML file was not updated to reflect the requested increase.

NEW QUESTION # 72
An administrator is tasked to create a new vSphere Zone for the highlighted namespace. Click the section of the interface where the administrator would navigate to start creating a new zone.



Answer:

Explanation:



Explanation:

Configure tab

In the context of VMware Cloud Foundation (VCF) 9.0 and vSphere with Tanzu, a vSphere Zone is a critical infrastructure object used to represent a failure domain. Specifically, it allows the vSphere Supervisor to span across multiple vSphere clusters (typically three) to provide high availability against a complete cluster failure. This " zoned " deployment model ensures that the Supervisor Control Plane and workload cluster nodes (VKS) are distributed across different physical racks or data centers.

To start the process of creating a new vSphere Zone, an administrator must navigate to the Configure tab.

While the provided screenshot highlights a specific namespace (other-namespace), the creation of the underlying infrastructure zones is an administrative task performed at the vCenter Server or Cluster level.

However, within any object's view in the vSphere Client, the Configure tab serves as the primary gateway for all lifecycle management and setup tasks. For a vCenter-level configuration, the path is vCenter Server > Configure > vSphere Zones . Once a zone is created and mapped to a vSphere cluster, it can then be associated with a Supervisor. In the namespace-specific view

shown, the Configure tab is also where the administrator would verify the placement of the namespace on a zoned Supervisor and manage the association with specific Supervisor Services. By clicking Configure , the administrator accesses the sub-menus required to define and modify these high-level SDDC constructs, bridging the gap between traditional vSphere resource management and the declarative Kubernetes environment provided by VKS.

NEW QUESTION # 73
A Security Operations Analyst is enforcing a policy that all container images used in TKG clusters must be pulled from an authenticated private registry (reg.secure.com). Anonymous pulls are blocked.
A developer's deployment is failing with ImagePullBackOff. The events show 401 Unauthorized.
Which steps must be taken to enable the TKG cluster to authenticate to the private registry? (Select all that apply.)

- A. Configure the Supervisor's "Image Registry" service with the credentials; the TKG cluster will inherit them automatically for all namespaces.
- B. Create a Kubernetes Secret of type docker-registry (or kubernetes.io/dockerconfigjson) in the developer's namespace, containing the valid username and password/token for reg.secure.com.
- C. The registry must be changed to allow anonymous access for the TKG nodes IP range.
- D. Reference the created Secret in the imagePullSecrets section of the Pod or Deployment YAML (or patch the default ServiceAccount to include it).
- E. Add the username and password to the TanzuKubernetesCluster spec under settings.network.registryAuth.

Answer: B,D

NEW QUESTION # 74
Which four capabilities are provided by a VMware Kubernetes Service (VKS) cluster?

- A. Authentication, backup services, VLAN segmentation, and DHCP.
- B. Identity federation, external storage, virtual machine networking, and DNS services.
- C. Identity federation, persistent logging, firewall services, and monitoring.
- D. Authentication, storage integration, pod networking, and load balancing.

Answer: D

Explanation:
The vSphere Kubernetes Service (VKS) in VMware Cloud Foundation (VCF) 9.0 is designed as an " enterprise-ready " Kubernetes distribution that is deeply integrated with the SDDC stack. It provides several core capabilities out-of-the-box that would otherwise require manual configuration in a generic Kubernetes installation. The four primary capabilities identified are Authentication , storage integration , pod networking , and load balancing .
First, Authentication is handled via integration with the vSphere Supervisor, which acts as an identity proxy (using Pinniped and OIDC) to allow users to log in using their vSphere or external identity provider credentials. Second, storage integration is achieved through the vSphere CSI (Container Storage Interface), which connects Kubernetes Persistent Volume Claims (PVCs) directly to vSphere datastores. Third, pod networking is provided by an integrated CNI (typically Antrea), ensuring secure and high-performance communication between containers. Finally, load balancing is managed through the vSphere distributed switch or NSX, allowing for the automatic creation of Layer 4 load balancers for Kubernetes services of type LoadBalancer. While VCF 9.0 supports add-on services for logging and monitoring (as mentioned in Option B), the core architectural pillars provided natively by the VKS cluster lifecycle manager are those that bridge the gap between container orchestration and the underlying vSphere infrastructure, ensuring that pods have the network, storage, and access control they require to run production workloads.

NEW QUESTION # 75
A VI Administrator is tasked with enabling the Harbor Image Registry on a Supervisor Cluster to provide a local, secure repository for developers. The "Harbor" Supervisor Service definition has already been uploaded to vCenter.
Review the configuration wizard requirements for enabling the service on a specific Supervisor:
1. Select Supervisor: Cluster-1
2. Service: Harbor
3. Configuration:
- Registry Storage Policy: [Select]
- Garbage Collection: [Select]
- Certificate: [Select]

Which prerequisite configuration must exist in the vSphere infrastructure to successfully complete this installation wizard and ensure the registry has persistence?

- A. A valid vSphere Storage Policy must be available and compatible with the Supervisor's datastores to back the Harbor PVCs (Persistent Volume Claims).
- B. A TKG Workload Cluster must already exist in the namespace to host the Harbor pods.
- C. The "VM Service" must be disabled on the Namespace.
- D. An NSX Load Balancer VIP must be manually pre-provisioned and entered into the wizard.

Answer: A

NEW QUESTION # 76
.....