

VMware.3V0-21.25.v2026-06-20.q29

Exam Code:	3V0-21.25
Exam Name:	Advanced VMware Cloud Foundation 9.0 Automation
Certification Provider:	VMware
Free Question Number:	29
Version:	v2026-06-20
# of views:	122
# of Questions views:	290
https://www.freepdfdumps.com/VMware.3V0-21.25.v2026-06-20.q29.html	

NEW QUESTION: 1

A VMware Cloud Foundation (VCF) Automation administrator has been tasked with ensuring that all newly- deployed virtual machines (VMs) provisioned in the Finance Organization are automatically configured for disaster recovery protection using VMware Live Recovery (VLR). Finance is an AllApps Organization in VCFA.

Which statement meets this requirement?

- A. Configure an Event Subscription that triggers an Orchestrator workflow to protect the VMs in VLR.
- B. Create a catalog item that calls an ABX workflow to add the VMs to VLR.
- C. Create a Day 2 policy that adds the VMs to a VLR Protection Group. Attach the policy to all catalog items available in the Finance Organization.
- D. Create a Day 2 action, scoped to the Finance Organization, that assigns the appropriate VLR Protection Group to all deployments.

Answer: C (LEAVE A REPLY)

In VCF 9.0, Policies are the most scalable way to enforce compliance and operational standards across an organization without modifying individual blueprints. To ensure all VMs are automatically protected by VMware Live Recovery (VLR), the administrator should Create a Day 2 policy. This policy type can be configured to automatically apply a "VLR Protection Group" assignment as a post-provisioning step. By attaching the policy to all catalog items within the Finance Organization, the administrator guarantees that regardless of which blueprint a user chooses, the protection logic is consistently applied. This "Policy-as- Code" approach is superior to manual event subscriptions (Option A) or individual catalog items (Option B) because it centralizes governance; if the protection requirements change, the admin only needs to update the single policy rather than dozens of separate scripts or subscriptions. This ensures that the Finance team's workloads remain compliant with disaster recovery mandates from the moment they are deployed.

NEW QUESTION: 2

What are two prerequisites to enable provisioning VMs via kubectl against tenant resources? (Choose two.)

- A. Create a context via VCF CLI.
- B. Ask the Provider to generate a token via the system APIs.
- C. Generate an API token from the VCF Automation UI.
- D. Create a new extensibility Action.
- E. Create a context via kubectl.

Answer: (SHOW ANSWER)

NEW QUESTION: 3

An administrator is configuring RBAC policies in VMware Cloud Foundation (VCF) Automation to delegate access across multiple clusters. The administrator must ensure that:

* Cluster lifecycle operations (e.g., scaling) can only be performed by a designated operations group.

* Security policies at the NSX project level remain restricted to network administrators' group.

Which two role assignments meet these requirements? (Choose two.)

A. Assign the Organization Owner role to the network administrators group at the tenant organization level.

B. Assign the Security Administrator role in NSX to the network administrators group at the project scope.

C. Assign the Service Viewer role in VCF Automation to the operations group at the cluster scope.

D. Assign the Service User role in VCF Automation to the operations group at the cluster scope.

E. Assign the Cluster Administrator role in VCF Automation to the operations group at the cluster scope.

Answer: ([SHOW ANSWER](#))

VCF 9.0 introduces a more granular RBAC model to support complex operational requirements. To meet the first requirement regarding cluster lifecycle management, the administrator must assign the Cluster Administrator role to the operations group. This role provides the specific permissions needed to perform actions such as scaling, patching, and modifying the configuration of Supervisor or TKG clusters. By scoping this at the cluster level (or within the project containing those clusters), the operations group is empowered to maintain the resources without having broad administrative access to other organizational settings. For the second requirement, the Security Administrator role in NSX must be assigned to the network administrators group. By scoping this to the project, the network admins can manage distributed firewall rules, gateway policies, and security profiles specific to that project's VPCs while being prevented from interfering with the compute lifecycle managed by the operations team. This separation of duties is essential for large-scale enterprise deployments to prevent unauthorized security changes or accidental cluster disruptions.

NEW QUESTION: 4

An administrator is reviewing the network topology of an AllApps Organization. They notice that while each Virtual Private Cloud (VPC) has its own private address space, there is a common component that handles the routing between these VPCs and the corporate backbone.

What is this component?

A. NSX Tier-1 Gateway

B. NSX Edge Cluster

C. NSX Transit Gateway

D. Distributed Logical Router

Answer: **C** ([LEAVE A REPLY](#))

The NSX Transit Gateway (TGW) is the architectural cornerstone of regional networking in VCF 9.0. In previous versions, administrators had to manually manage complex Tier-0/Tier-1 relationships for each tenant; however, VCF 9.0 abstracts this through the TGW. When a Region is created, the system automatically instantiates the Transit Gateway to act as the high-speed "backplane" for the organization. Every VPC created within that region connects to this TGW, which then handles all East-West traffic between VPCs and North-South traffic toward the corporate WAN or Internet. This design ensures that the routing logic is consistent, automated, and isolated from the physical underlying fabric. The TGW works in conjunction with VPC Connectivity Profiles to determine if a VPC is completely isolated or has an external path, providing a scalable and secure way to manage hundreds of isolated network segments without manual intervention.

NEW QUESTION: 5

An administrator has been tasked with deploying an AllApps Organization within VMware Cloud Foundation (VCF) Automation.

During the regional networking creation step, which three NSX constructs will automatically be configured?

(Choose three.)

A. A Default Virtual Private Cloud (VPC).

B. A Virtual Distributed Switch (VDS).

C. A Provider Tier-0 Gateway.

D. A Virtual Private Cloud (VPC) connectivity profile.

E. An NSX Transit Gateway.

Answer: **A,D,E** ([LEAVE A REPLY](#))

When creating a Region for an AllApps Organization in VCF 9.0, the automation engine orchestrates several critical NSX networking components to enable multi-tenancy. The NSX Transit Gateway is deployed to provide the underlying routing backbone that connects different VPCs and external services within the region. Simultaneously, a Default VPC is instantiated for the organization, providing an out-of-the- box isolated environment where developers can immediately begin deploying workloads. To govern how this VPC and others interact with the broader network, a VPC Connectivity Profile is created. This profile defines the "Guardrails" for the organization, such as whether VPCs are strictly isolated (Private - TGW) or have external access. Unlike manual networking setups, these steps are automated during the Region-to- Organization mapping process, ensuring that the necessary multi-tenant infrastructure is consistent and ready for use without manual Tier-1 gateway or segment configuration by the administrator.

NEW QUESTION: 6

An administrator clicks on Orchestrator to create a workflow in a VMApps organization as shown in the image. Where would the administrator go next to enable Orchestrator?

- A. Click Infrastructure.
- B. Click Connections.
- C. Click Integrations.
- D. Click Design.

Answer: A,B,C (LEAVE A REPLY)

In VCF 9.0 Automation, enabling the Operations Orchestrator (vRO) for a specific organization is an integration task performed within the portal's infrastructure settings. If the administrator sees a message stating "No VCF Operations Orchestrator integration available" under the Orchestrator tab, it indicates that the logical link between the Automation service and the Orchestrator engine has not been established for that tenant. To resolve this, the administrator must navigate through the following path: Infrastructure > Connections > Integrations. Under the Integrations menu, the administrator can select "Add Integration" and choose VCF Operations Orchestrator. They must provide the FQDN of the orchestrator server and the appropriate credentials. Once the integration is finalized and the "Collect Data" task completes, the Orchestrator tab will become functional, allowing the administrator to import, create, and manage workflows directly from the VCF Automation UI.

NEW QUESTION: 7

An administrator clicks on Orchestrator to create a workflow in a VM Apps organization as shown.

Where would the administrator go next to enable Orchestrator?



Answer:



Explanation:

To enable the Orchestrator integration, the administrator must navigate to:

* Infrastructure (tab)

In VMware Cloud Foundation (VCF) 9.0, the VCF Operations Orchestrator (formerly vRealize Orchestrator) is a separate functional engine that must be explicitly integrated into the automation framework.

When an administrator selects the Orchestrator tab and encounters the warning message "No VCF Operations Orchestrator integration available," it indicates that the logical link between the Automation service and the Orchestrator appliance has not yet been established for that specific organization.

The standard administrative workflow to resolve this and enable extensibility is to move from the consumption/design view into the foundational infrastructure configuration. By clicking on the Infrastructure tab, the administrator gains access to global settings. From there, the administrator must navigate to Connections and then Integrations. Within the Integrations menu, the administrator can select "Add Integration" and specifically choose VCF Operations Orchestrator. This process requires providing the FQDN of the orchestrator server and appropriate service account credentials.

Once the integration is finalized and a successful data collection occurs, the portal's Orchestrator interface becomes functional, allowing users to build, run, and manage multi-cloud automation workflows across the VCF 9.0 fleet.

NEW QUESTION: 8

An administrator needs to configure a connection between VMware Cloud Foundation (VCF) Automation and an external system to enable the exchange of data for extensibility purposes.

Which two integration types are supported for this purpose? (Choose two.)

- A. VCF Operations Orchestrator
- B. VMware Live Recovery
- C. Action-Based Extensibility (ABX)
- D. VMware Cloud Foundation SDDC Manager
- E. vSphere Lifecycle Manager

Answer: A,C (LEAVE A REPLY)

VCF 9.0 Automation provides two primary "engines" for extensibility and external system integration. VCF Operations Orchestrator is the robust, long-standing workflow engine designed for complex, multi-step orchestration across heterogeneous infrastructure. It supports extensive plugin libraries for third-party systems like ServiceNow, Infoblox, or custom REST/SOAP endpoints. Action-Based Extensibility (ABX) is the modern, serverless alternative that allows administrators to execute lightweight scripts (Python, Node.js, or PowerShell) directly within the VCF Automation framework. ABX is ideal for quick, specific tasks such as calling a web hook or performing a simple API transformation during the provisioning lifecycle. While SDDC Manager (Option D) and vSphere Lifecycle Manager (Option E) are core components of the VCF stack for management and patching, they are not used as extensibility "integrations" for data exchange in the context of automation workflows.

NEW QUESTION: 9

An administrator has been tasked with creating a workflow in VCF Operations orchestrator. The workflow will be used to take a snapshot before planned maintenance work is carried out within the virtual machine, and then automatically remove the snapshot at the end of the maintenance window. The following information has been provided for the workflow:

- . The workflow must allow a user to specify a virtual machine on which a snapshot should be taken.
- . The workflow must take a snapshot of the virtual machine specified by the user.
- . The workflow must name the snapshot based on the current date and time.
- . The workflow must delete all snapshots on the virtual machine after a cooling off period of 5 days has elapsed.
- . The workflow must stop running after the snapshot is created, a second workflow should automatically start when the 5 day cooling off period has elapsed.

The administrator creates a new workflow for this task and adds an input parameter to allow the user to specify the virtual machine.

Drag and drop the additional five steps the administrator should perform to continue configuring the workflow from the Possible Steps list on the left and place them into the Selected Steps list on the right in any order (Choose five.)

Possible Steps

Map the name input parameter to the currentDate output parameter to define the name of the snapshot.

Add an output parameter of type string to the workflow named currentDate for storing the current date and time value.

Add a Waiting timer element to the workflow and configure it to wait for 5 days.

Add a Workflow element to the schema and configure it to use the Create a Snapshot workflow provided by the orchestrator workflow library.

Map the name input parameter to the currentDate variable to define the name of the snapshot.

Add a Variable of type string to the workflow named currentDate for storing the current date and time value.

Add a Schedule workflow element to the schema and configure it to use the Remove all snapshots workflow.

Configure the Scheduled workflow to run 5 days from the value of the currentDate variable.

Add a Workflow element to the schema and configure it to use the Remove all snapshots workflow.

Selected Steps

vmware®

freepdfdumps.com

>

<

↑

↓

Answer:

Possible Steps

- Map the name input parameter to the currentDate output parameter to define the name of the snapshot.
- Add an output parameter of type string to the workflow named currentDate for storing the current date and time value.
- Add a Waiting timer element to the workflow and configure it to wait for 5 days.
- Add a Workflow element to the schema and configure it to use the Create a Snapshot workflow provided by the orchestrator workflow library.
- Map the name input parameter to the currentDate variable to define the name of the snapshot.
- Add a Variable of type string to the workflow named currentDate for storing the current date and time value.
- Add a Schedule workflow element to the schema and configure it to use the Remove all snapshots workflow.
- Configure the Scheduled workflow to run 5 days from the value of the currentDate variable.
- Add a Workflow element to the schema and configure it to use the Remove all snapshots workflow.

Selected Steps

- Add a Variable of type string to the workflow named currentDate for storing the current date and time value.
- Add a Workflow element to the schema and configure it to use the Create a Snapshot workflow provided by the orchestrator workflow library.
- Map the name input parameter to the currentDate variable to define the name of the snapshot.
- Add a Schedule workflow element to the schema and configure it to use the Remove all snapshots workflow.
- Configure the Scheduled workflow to run 5 days from the value of the currentDate variable.

Explanation:

- * Add a Variable of type string to the workflow named currentDate for storing the current date and time value.
- * Add a Workflow element to the schema and configure it to use the Create a Snapshot workflow provided by the orchestrator workflow library.
- * Map the name input parameter to the currentDate variable to define the name of the snapshot.
- * Add a Schedule workflow element to the schema and configure it to use the Remove all snapshots workflow.
- * Configure the Scheduled workflow to run 5 days from the value of the currentDate variable.

In VMware Cloud Foundation (VCF) 9.0, the Operations orchestrator (vRO) is used to build complex, state-aware automation. To satisfy the requirement that the main workflow stops running while a second cleanup task triggers later, the administrator must use the Schedule workflow element rather than a "Waiting Timer". A waiting timer keeps the workflow "Active," consuming system resources for the duration of the wait (5 days), whereas a scheduled task is handed off to the orchestrator's database to be triggered independently.

The configuration begins by defining a currentDate variable of type string. This variable captures the execution timestamp, which is then mapped to the Create a Snapshot library workflow to provide the required dynamic naming. To handle the automated cleanup, the administrator adds a Schedule workflow element. Unlike a standard workflow call, the scheduler allows for a specific execution offset.

By configuring the Remove all snapshots workflow to run 5 days from the currentDate value, the administrator ensures the snapshot exists for exactly the maintenance and cooling-off period before being programmatically removed. This approach is robust against orchestrator service restarts and provides a clean, asynchronous method for managing the temporary infrastructure lifecycle in a VCF 9.0 environment.

NEW QUESTION: 10

An organization uses VMware Cloud Foundation (VCF) and requires the following across the private cloud environment:

- * monitor IP space utilization.
- * detect network anomalies.
- * enforce consistent network policies.

What three capabilities are required? (Choose three.)

- A. NSX Traceflows
- B. Integrated Security with VCF Operations
- C. vDefend
- D. VCF Operations lifecycle management
- E. NSX Subnetting

Answer: (SHOW ANSWER)

To meet the comprehensive requirements of monitoring, anomaly detection, and policy enforcement in VCF

9.0, a combination of integrated networking and security tools is used. NSX Traceflows provide the deep visibility needed to monitor IP space utilization and troubleshoot connectivity at the packet level, allowing administrators to visualize the path traffic takes through the virtual and physical fabric. Integrated Security with VCF Operations (formerly part of the Aria suite) provides the management dashboard for detecting network anomalies by correlating flow data and identifying traffic patterns that deviate from established baselines. Finally, vDefend (the integrated NSX security stack) is essential for enforcing consistent network policies through distributed firewalls (DFW), gateway firewalls, and IDS/IPS capabilities. Together, these three capabilities ensure that the VCF environment remains secure, transparent, and compliant with corporate governance standards, providing the "closed-loop" operational model required for modern private clouds.

NEW QUESTION: 11

An administrator has been tasked with configuring tenant branding with the following requirements:

* Organization branding should only appear when a user has logged in to the organization portal.

Select the three steps involved in configuring branding. (Choose three.)

- A. Log into the Provider Management Portal.
- B. Log into the Organization Portal.
- C. Disable the Enable Login and Logout Page Branding setting.
- D. Navigate to Branding.
- E. Import a branding theme.
- F. Enable the Enable Login and Logout Page Branding setting.

Answer: B,C,D (LEAVE A REPLY)

In VMware Cloud Foundation 9.0, branding is managed within the Organization Portal to allow for tenant- specific customization. To meet the specific requirement that branding only appears after a user has authenticated, the administrator must navigate to the Branding section of the portal. The critical configuration step is to Disable the Enable Login and Logout Page Branding setting. By default, if this is enabled, the custom logos and colors are displayed on the public-facing login screen. Disabling it ensures that the generic VCF/Broadcom login page is presented to the public, and the custom tenant identity is only loaded into the browser session once the user's organization context is established through successful login. This is a common requirement for service providers who want to maintain a consistent entry point for all users while providing a personalized "white-labeled" experience once the user is inside their specific environment.

NEW QUESTION: 12

Which statement describes Virtual Private Clouds (VPCs)?

- A. Enables the provider administrator to create nested VCF instances with a private cloud.
- B. Enables multiple organizations to share the same physical Supervisor cluster while consuming logically isolated networks.
- C. Enables multiple organizations to share virtualized GPUs.
- D. Enables the provider administrator to create multiple VCF instances nested within public clouds (e.g., Amazon AWS, Microsoft Azure, Google GCP, etc.).

Answer: (SHOW ANSWER)

Virtual Private Clouds (VPCs) in VCF 9.0 represent a significant evolution in multi-tenant networking. A VPC is a logically isolated network partition that exists within a shared physical infrastructure, specifically a Supervisor cluster. This construct allows multiple distinct organizations to coexist on the same compute hardware while maintaining complete separation of their network traffic, IP address spaces, and security policies. Each VPC acts as a "mini-datacenter" for the tenant, providing automated services such as routing, DHCP, NAT, and distributed firewalls without the tenant ever needing to see or interact with the underlying NSX Tier-0 or Tier-1 gateway architecture. This "abstraction" is the key to scaling VCF 9.0 deployments, as it allows the provider to maximize host utilization across many small tenants while giving each tenant the

"look and feel" of a dedicated, private networking environment. It effectively removes the complexity of manual VLAN or segment management that characterized older private cloud architectures.

NEW QUESTION: 13

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 to the administrator for this task:

- * Two workload domains are configured and will integrate with the region.
- * All workload domains are configured to share a VMware NSX Manager.
- * All workload domains are configured with VMware vSAN storage.
- * All workload domain VMware vCenter instances have a Supervisor enabled.

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

- A. An AllApps Organization has been created.
- B. All Supervisors are configured with the same services across all vCenter instances.
- C. All required virtual machine (VM) classes are present and have the same names across all vCenter instances.
- D. A Region Quota has been created and associated with the Organization.
- E. All required storage classes are present and have the same names across all vCenter instances.

Answer: C,E (LEAVE A REPLY)

In VCF 9.0, a Region is a logical grouping of resources (typically spanning multiple vCenter/Supervisor instances) that is presented to an Organization for consumption. For the automation engine to treat multiple clusters or vCenter instances as a single, unified pool of capacity, there must be absolute naming parity for resource types. If a blueprint requests a "Large-Memory" VM Class or a "Gold-Storage" Storage Class, that specific name must exist and be configured identically on every Supervisor instance within the region. If naming differs-for example, "Gold-Tier" on one and "Gold-Storage" on another-the provisioning engine will fail to find a consistent placement target, leading to deployment errors. Validating that VM Classes and Storage Classes are synchronized in name and availability across all participating workload domains is a mandatory "Day 0" task before the logical Region construct can be finalized in the Provider Management Portal.

NEW QUESTION: 14

An administrator has been tasked with sharing a catalog item from the VMware Cloud Foundation (VCF) Automation Provider Consumption Org (PCO) to the FinTech organization.

The following information has been provided:

- * There are two catalog items, Linux VM and Windows VM
- * The Linux VM catalog item should be shared project called AppDev.

Drag and drop three steps from the Steps list to the Ordered Steps list on the right to complete the objective.

(Choose three.)

vmware®

Steps

Enable the **Show items without a project** option in the catalog.

Add the **Windows VM** catalog item to the **AppDev** project.

Add the **Linux VM** catalog item to the **AppDev** project.

Disable the **Show items without a project** option in the catalog.

Log into the **Provider Consumption** Organization.

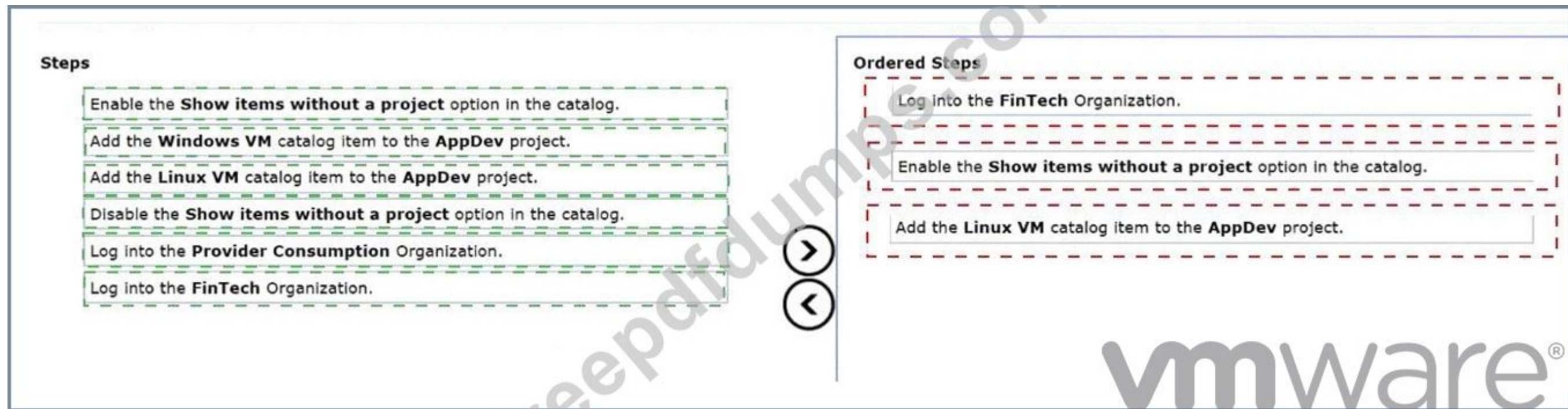
Log into the **FinTech** Organization.

Ordered Steps

>

<

Answer:



Explanation:

To share a specific catalog item from the Provider Consumption Org (PCO) to a tenant organization and project, follow these ordered steps:

Ordered Steps

Log Into the FinTech Organization.

Enable the Show items without a project option in the catalog.

Add the Linux VM catalog item to the AppDev project.

In VMware Cloud Foundation (VCF) 9.0, catalog items from the Provider Consumption Org (PCO) can be shared across multiple tenant organizations, such as the FinTech organization, to promote infrastructure standardization. To manage these shared items, the administrator must first Log into the FinTech Organization portal directly. Within this context, catalog items shared from the provider do not initially have a project association within the local tenant workspace.

Therefore, the administrator must Enable the "Show items without a project" option in the catalog view. This setting reveals global or provider-shared items that are available to the organization but have not yet been entitled to a specific local group. Once visible, the administrator can perform the entitlement task by selecting the specific Linux VM catalog item and adding it to the AppDev project. This step creates the final link in the role-based access control (RBAC) chain, ensuring that only users assigned to the AppDev project can request and deploy the Linux virtual machine according to the organization's governance policies. This workflow allows providers to maintain "golden" templates at the fleet level while granting tenants the flexibility to assign those resources to their own internal development teams.

NEW QUESTION: 15

A customer created a workflow to execute during machine provisioning in a VMApps Organization within VMware Cloud Foundation (VCF) Automation 9. The workflow includes inputs that interact with the provisioning-payload data. When a machine is requested, provisioning completes successfully, but the workflow does not run. What is the cause of the workflow-execution failure?

- A. The Event Broker Subscription is set to blocking.
- B. The workflow is not signed.
- C. The workflow is signed.
- D. The Event Broker Subscription is set to non-blocking.

Answer: (SHOW ANSWER)

VCF 9.0 introduces enhanced security requirements for Operations Orchestrator integration, specifically regarding the execution of custom extensibility logic. A common cause for a workflow failing to trigger, even when the provisioning process itself is successful, is that the workflow is not signed. By default, VCF 9.0 Automation enforces a security policy that requires all custom workflows to be digitally signed by a trusted certificate before the Event Broker Service (EBS) will execute them. This prevents unauthorized or malicious scripts from running within the management plane of the private cloud. If the workflow is not

signed, the EBS will silently ignore the trigger or log a security violation in the background, while the main VM provisioning-which is a separate process-continues to completion. The administrator must import the developer certificate into the Orchestrator and sign the workflow package to authorize its execution in the production environment.

NEW QUESTION: 16

An administrator is tasked to enable VMware Cloud Foundation (VCF) Automation to run ABX actions.

What must be configured?

- A. Create a project in an AllApps Organization.
- B. Create a cloud account in the Organization Portal.
- C. Create a region in an AllApps Organization.
- D. Create a cloud account in the Provider Management Portal.

Answer: D (LEAVE A REPLY)

Action-Based Extensibility (ABX) requires a functional management plane connection to execute scripts against the infrastructure. In VCF 9.0, the foundation for all automation tasks-including ABX-is the Cloud Account. The administrator must Create a cloud account in the Provider Management Portal to establish the primary connection between the VCF Automation appliance and the underlying vCenter/NSX endpoints.

While individual organizations can have their own accounts, the core extensibility engine (which runs the serverless containers for ABX) relies on the provider-level account to identify where and how to execute scripts across the fleet. Without a valid Cloud Account, the ABX service has no target for resource discovery or event-triggered logic, rendering the extensibility framework non-functional for both provider and tenant organizations.

Valid 3V0-21.25 Dumps shared by Actual4test.com for Helping Passing 3V0-21.25 Exam! Actual4test.com now offer the **newest 3V0-21.25 exam dumps**, the Actual4test.com 3V0-21.25 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 3V0-21.25 dumps with Test Engine here: https://www.actual4test.com/3V0-21.25_examcollection.html (**64** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 17

An administrator has been tasked with creating an action in VMware Cloud Foundation (VCF) Operations orchestrator. The action will be used within all custom created workflows and actions to print additional information into the logs to assist with troubleshooting. The following information has been provided for the action:

- * The action must be named standardLogging
- * The action must be stored in lab.vcf.logging
- * The action script will output a value that is in a JSON object format The action must accept an input with the following configuration:
 - o Name: sourceName
 - o Type: string

Drag and drop the five correct steps the administrator must perform as part of this task from the Possible Steps list on the left and place them into the Selected Steps list on the right in any order. (Choose five.)

Possible Steps

Set the Module field on the new Action to lab.vcf.logging.
Add a new Input named sourceName of type string.
Set the Runtime Environment field on the new Action to lab.vcf.logging.
Add a new Input named sourceName of type Any.
Add a new Output named logOutput of type Any.
Create a new module named lab.vcf.logging.
Create a new Action named standardLogging.
Create a new folder named lab.vcf.logging.
Set the Return type field to string.
Set the Return type field to Any.

Selected Steps

Answer:

Possible Steps

Set the Module field on the new Action to lab.vcf.logging.
Add a new Input named sourceName of type string.
Set the Runtime Environment field on the new Action to lab.vcf.logging.
Add a new Input named sourceName of type Any.
Add a new Output named logOutput of type Any.
Create a new module named lab.vcf.logging.
Create a new Action named standardLogging.
Create a new folder named lab.vcf.logging.
Set the Return type field to string.
Set the Return type field to Any.

Selected Steps

Create a new module named lab.vcf.logging.
Create a new Action named standardLogging.
Set the Module field on the new Action to lab.vcf.logging.
Add a new Input named sourceName of type string.
Set the Return type field to Any.

Explanation:

- * Create a new module named lab.vcf.logging.
- * Create a new Action named standardLogging.
- * Set the Module field on the new Action to lab.vcf.logging.
- * Add a new Input named sourceName of type string.
- * Set the Return type field to Any.

In VMware Cloud Foundation (VCF) 9.0, extensibility through the Operations orchestrator (formerly vRealize Orchestrator) requires a structured approach to modularity and data typing. To store an action in a specific path like lab.vcf.logging, an administrator must first create a new module with that name, as modules serve as the organizational namespaces for actions. Once the container exists, the administrator creates the Action named standardLogging and explicitly sets the Module field to the newly created namespace to ensure correct storage and accessibility across the orchestrator server.

The configuration of inputs and outputs is critical for programmatic integration. By adding an input named `sourceName` of type `string`, the administrator ensures the action can receive metadata from calling workflows exactly as specified in the technical requirements. Regarding the output, the requirement states the script returns a JSON object format. In the orchestrator's JavaScript-based engine, while a string could technically hold JSON text, the "Any" return type is the standard and verified method for returning structured objects. This allows subsequent workflow elements to programmatically parse and interact with the JSON properties without manual conversion, fulfilling the requirement for sophisticated log data handling and troubleshooting within the VCF 9.0 framework.

NEW QUESTION: 18

An organization uses a centralized external Configuration Management Database (CMDB) to track all infrastructure assets. Currently, when a new virtual machine (VM) is provisioned through VMware Cloud Foundation (VCF) Automation, operations teams are required to manually input associated metadata into the CMDB.

An administrator is tasked with reducing the manual effort and increasing efficiency of this process using VCF Automation.

Which three of the following can VCF Automation perform? (Choose three.)

- A. Create a new event topic that creates a notification upon successful VM provisioning.
- B. Create a webhook endpoint on VCF with payload containing the required metadata.
- C. Call a webhook endpoint on the CMDB API with payload containing the required metadata.
- D. Configure a subscription that reacts to VM provisioning requests.
- E. Request additional metadata as input during the deployment of the blueprint.

Answer: C,D,E (LEAVE A REPLY)

To automate CMDB updates in VCF 9.0, administrators leverage the Event Broker Service (EBS) and Custom Forms. First, the administrator can Request additional metadata as input during the blueprint request. This ensures that unique information, such as "Cost Center" or "Application ID," is captured directly from the user at request time. Second, the admin must Configure a subscription that specifically listens for the "Post-Provisioning" event topic. This subscription acts as the trigger for the automation logic. Finally, the subscription invokes an ABX action or Orchestrator workflow that is programmed to Call a webhook endpoint on the CMDB API. This call sends a JSON payload containing both the system-generated metadata (e.g., VM UUID, IP address) and the user-provided inputs directly to the CMDB. This "closed-loop" automation eliminates manual data entry, reduces human error, and ensures that the asset repository is updated in real-time as soon as the infrastructure is live.

NEW QUESTION: 19

An administrator must initiate the deployment of a new 3-tier application architecture using the VMware Cloud Foundation (VCF) Automation portal. This application includes:

- * A web tier (stateless).
- * A business logic tier (some local caching).
- * A database tier (stateful, PostgreSQL).
- * An NSX load balancer fronting the web tier.
- * ~99.9% uptime requirement.
- * Moderate performance requirements.

Which requirement represents a risk inherent to single-zone deployments?

- A. A higher latency between application tiers.
- B. A split-brain isolation.
- C. A higher network complexity.
- D. A shared failure domain for all application tiers.

Answer: D (LEAVE A REPLY)

The primary architectural risk in any single-zone deployment within VCF 9.0 is the existence of a shared failure domain. In a single-zone Supervisor cluster or workload domain, all components-including the web, application, and database tiers-reside within the same logical and often physical infrastructure boundary (such as a single rack or data center room). If the underlying zone experiences a critical failure, such as a localized power outage, cooling failure, or a total top-of-rack switch collapse, the entire 3-tier application stack will go offline simultaneously. For mission-critical applications requiring high availability, VCF 9.0 recommends a multi-zone or stretched cluster architecture. In such designs, the failure of one zone does not compromise the entire application because the tiers can be distributed across different fault

domains, ensuring that the stateless web tier and stateful database remain operational elsewhere. In the context of the 99.9% uptime requirement mentioned, a single-zone design represents a significant risk because it lacks the redundancy needed to survive zone-level disruptions.

NEW QUESTION: 20

An administrator has been tasked with creating a Day 2 Operation which invokes vMotion migration on a virtual machine (VM). Which two steps are required? (Choose two.)

- A. Drag and drop the User Interaction schema element.
- B. Create a resource action.
- C. Call the pre-defined Orchestrator workflow named Migrate virtual machine with vMotion.
- D. Create an Orchestrator action.
- E. Create an ABX action named Migrate virtual machine with vMotion.

Answer: B,C ([LEAVE A REPLY](#))

In VCF 9.0 Automation, a Day 2 Operation is an extension of the platform's native capabilities, allowing users to perform lifecycle tasks on already deployed resources. To enable a vMotion migration through the automation portal, the administrator must first Create a resource action. This construct defines the UI element that will appear when a user selects a VM in their deployment list. The resource action must then be mapped to an execution logic; the most efficient and verified method is to Call the pre-defined Orchestrator workflow named Migrate virtual machine with vMotion. This workflow is part of the standard vCenter integration library in VCF Operations Orchestrator and contains all the necessary logic to handle destination host selection and validation. Once the action is created and mapped to the workflow, it must be added to a Service Broker Policy to entitle the appropriate users or projects to perform the migration task.

NEW QUESTION: 21

Which three types of profiles do Virtual Private Clouds (VPCs) in VMware Cloud Foundation (VCF) leverage? (Choose three.)

- A. Security Profile
- B. vGPU Profile
- C. Connectivity Profile
- D. QoS Profile
- E. Service Profile

Answer: (SHOW ANSWER)

In VMware Cloud Foundation 9.0, the Virtual Private Cloud (VPC) model utilizes a profile-based approach to standardize and automate network and security services for tenants. The Connectivity Profile is the primary construct used to define the "boundary" of the VPC, determining how the VPC connects to the regional Transit Gateway and whether it has access to external networks or remains isolated. The Security Profile allows administrators to define baseline security postures, such as distributed firewall (DFW) rules and group memberships, that are automatically applied to workloads within the VPC. Finally, the Service Profile is used to enable and configure additional network services, such as Load Balancing or NAT, within the VPC environment. By using these three profile types, the VCF Automation engine can provision consistent, "secure-by-default" network spaces for different organizations or projects, significantly reducing the manual configuration required compared to traditional NSX-T segment management.

NEW QUESTION: 22

The administrator is tasked with configuring hard tenancy in VMware Cloud Foundation (VCF) Automation.

Which statement reflects how multi-tenancy is configured?

- A. VMApps organizations enable hard tenancy within VCF Automation.
- B. VCF Automation 9 does not support multi-tenancy. That's on the roadmap for VCFA 10.
- C. Namespaces enable hard tenancy within VCF Automation.
- D. Namespace Classes enable hard tenancy construct within VCF Automation.
- E. AllApps organizations enable hard tenancy within VCF Automation.

Answer: E ([LEAVE A REPLY](#))

In VMware Cloud Foundation 9.0, the "AllApps" (often noted as AllApps) organization model is the definitive architectural construct for implementing hard tenancy. While the platform supports several organization types, including the "classic" VMApps model, the AllApps organization leverages the deeper integration of the vSphere Supervisor and NSX Virtual Private Clouds (VPCs) to provide true logical and administrative isolation. This hard tenancy model allows a provider to carve out specific regions of infrastructure where the tenant has a completely isolated control plane, private networking via VPCs, and dedicated resource quotas. Unlike shared namespace models, an AllApps organization acts as a self-contained "cloud" for the consumer, ensuring that developer activities, network policies, and resource consumption in one organization cannot impact another. This is critical for regulated industries or large enterprises requiring strict segregation between business units. The configuration is managed through the Provider Management Portal, where the provider administrator maps physical infrastructure (via Regions) to these tenant organizations, establishing the "hard" boundary that defines the tenancy.

NEW QUESTION: 23

In VMware Cloud Foundation (VCF) Automation, which construct within an AllApps organization consists of one or more Supervisors and supplies compute, memory, storage, and network resources to the organization?

- A. Region
- B. Project
- C. Cloud Zone
- D. Cloud Account

Answer: A (LEAVE A REPLY)

In the architectural framework of VCF 9.0's AllApps (AllApps) organization, the Region is the fundamental resource provider construct. A Region represents a logical grouping of one or more vSphere Supervisor clusters that share a common NSX Manager instance. It is at the Region level that the cloud provider discovers and identifies the available infrastructure capacity-including Kubernetes namespaces, VM classes, and storage policies-that can then be allocated to a tenant organization. When an administrator creates a Region in the Provider Management Portal, they are effectively defining a "pool" of resources that spans physical workload domains, allowing the automation engine to intelligently place workloads across different Supervisors as needed. While a Project is used for user-level resource entitlement and a Cloud Zone is used in the older VMApps model, the Region is the mandatory infrastructure anchor for any modern AllApps organization seeking to consume Supervisor-based services in VCF 9.0.

NEW QUESTION: 24

An administrator is tasked with configuring an existing Organization to enable users to create namespaces with GPU resources on their assigned Projects.

The Organization is backed by a Region with a GPU-enabled supervisor on a single zone setup.

What needs to be configured for this requirement?

- A. Namespace Class with VM Class Reservations.
- B. NVIDIA grid_al00-40c profile.
- C. NVIDIA GPU Operator.
- D. GPU enabled VM Classes.

Answer: A (LEAVE A REPLY)

To deliver GPU resources to tenant users in VCF 9.0, the administrator must bridge the physical hardware to the logical project via a Namespace Class. Specifically, the administrator must create or modify a Namespace Class to include VM Class Reservations for GPU-enabled classes. In VCF 9.0, a "Namespace Class" defines the templates and limits for the Kubernetes namespaces that users can create. By adding a GPU-enabled VM Class (such as one utilizing NVIDIA vGPU profiles) to the reservation list within the Namespace Class, the administrator ensures that the Supervisor knows to prioritize and reserve those specific hardware resources for workloads deployed into that namespace. Once this Namespace Class is bound to the user's Project, the users can then select the GPU-enabled classes when deploying their containers or VMs, fulfilling the requirement for high-performance compute within the multi-tenant environment.

NEW QUESTION: 25

A system administrator is tasked to create a region for use within an AllApps organization. How would the administrator determine which vCenter Servers are available in the infrastructure?

- A. Verify connections in the Organization portal.

- B.** Verify connections in the Provider Management portal.
- C.** Manually look up the UUID of the vCenter Server(s) in the VMware Kubernetes Service (VKS).
- D.** Manually look up the UUID of the vCenter Server(s) in the vSphere Client.

Answer: ([SHOW ANSWER](#))

The Provider Management Portal in VCF 9.0 is the centralized interface where the cloud provider administrator manages all foundational infrastructure. When creating a Region, the administrator must select from the infrastructure already integrated into the VCF Automation appliance. By navigating to the infrastructure or "Cloud Accounts" section within the Provider Management Portal, the administrator can see the status of all vCenter Server and NSX Manager connections. This portal provides the "provider-view" of the entire fleet, allowing the admin to verify which vCenter instances are currently healthy, licensed for VCF 9.0, and have the Supervisor enabled. This step is critical because a Region cannot be successfully created if the underlying vCenter connection is down or the integration is incomplete. The Organization Portal, by contrast, is a tenant-facing interface and does not have the visibility into the global infrastructure required to perform these "Day 0" provider setup tasks.

NEW QUESTION: 26

An Organization Administrator for an AllApps Organization in VMware Cloud Foundation (VCF) Automation must determine which networks are used by deployed workloads. How does the administrator view the networks?

- A.** VPCs and connectivity profile assignments are visible in the Organization Portal, but the underlying NSX Tier-1 gateways and segments are not.
- B.** VPCs, connectivity profiles and the associated NSX segment and Tier-1 gateway details can be retrieved with `vcf-cli deployment get`.
- C.** The NSX Tier-1 gateway mappings for each workload in the Organization can be retrieved with `kubectl get vm`.
- D.** The NSX segments mapped to each workload are visible by expanding deployment details for each deployed workload in the Organization Portal.

Answer: **A** ([LEAVE A REPLY](#))

The AllApps (AllApps) organization model in VCF 9.0 is built on the principle of high-level abstraction to simplify the developer experience. In this model, the Organization Portal presents networking through the lens of Virtual Private Clouds (VPCs) and Connectivity Profiles. The Organization Administrator can easily view which VPC a workload belongs to and what connectivity policies (such as public access or isolation) are applied. However, the underlying NSX implementation details-such as the specific Tier-1 gateways and segments automatically created by the Supervisor-are intentionally abstracted away from the organization-level view. This "cloud-style" visibility ensures that tenants can manage their application networking without being burdened by the complexity of the provider's physical or logical NSX fabric, which remains the exclusive domain of the Provider Administrator.

NEW QUESTION: 27

In VMware Cloud Foundation (VCF) Automation, which two statements identify the relationship between a storage policy and a region? (Choose two.)

- A.** Regions can only use the default vSphere storage policy.
- B.** Storage policies determine which datastores are available in a region.
- C.** Regions automatically create storage policies based on cluster configuration.
- D.** Storage policies must be replicated across all regions using the VCF Automation REST API.
- E.** A storage policy can be associated with one or more regions.

Answer: **B,E** ([LEAVE A REPLY](#))

In VCF 9.0, the Region construct acts as the bridge between physical vSphere infrastructure and the logical automation consumption layer. Storage policies (SPBM) are used to abstract the underlying physical datastores (such as vSAN, VMFS, or vVOLS). A region identifies which storage policies are available for consumption by the tenant organizations mapped to it. Consequently, storage policies determine which datastores are available within a region; if a datastore is not associated with a policy selected during region configuration, it cannot be used for workload placement. Furthermore, a storage policy can be associated with one or more regions. This allows a provider to offer standardized "Gold," "Silver," or "Bronze" storage tiers across different geographic or logical regions of the VCF fleet, ensuring a consistent consumption experience for developers regardless of which physical workload domain their virtual machines or Kubernetes pods are deployed into.

NEW QUESTION: 28

An administrator has been tasked with creating a provider content library. The following requirements must be satisfied:

- * The content library must be configured as a local content library.

* The content library must be associated with the region called West.
Select the four steps involved in configuring the provider content library. (Choose four.)

Action Options

Log into the Provider Management Portal.

Ensure **Subscribe to an external library** is enabled.

Ensure **Subscribe to an external library** is disabled.

Specify the region called West.

Log into the Organization Portal.

Click **CREATE CONTENT LIBRARY**.

Action List

>

<

Answer:

Action Options

Log into the Provider Management Portal.

Ensure **Subscribe to an external library** is enabled.

Ensure **Subscribe to an external library** is disabled.

Specify the region called West.

Log into the Organization Portal.

Click **CREATE CONTENT LIBRARY**.

Action List

>

<

Explanation:

- * Log into the Provider Management Portal.
- * Click CREATE CONTENT LIBRARY.
- * Specify the region called West.

* Ensure Subscribe to an external library is disabled.

In VMware Cloud Foundation (VCF) 9.0, the Provider Management Portal is the centralized interface used by cloud providers to manage global infrastructure and shared resources across the entire fleet.

To satisfy the requirements:

* Administrative Context: The task of creating global resources like a provider-level content library is a

"Day 0/1" infrastructure task, which must be performed in the Provider Management Portal rather than a tenant-specific Organization Portal.

* Regional Association: VCF 9.0 uses Regions to logically group underlying vSphere and NSX resources. Associating the library with the West region ensures that the templates and ISOs within that library are specifically available for workloads deployed into that regional infrastructure.

* Local vs. Subscribed: A Local Content Library is one where the provider directly uploads and manages the content. The requirement specifies a local configuration; therefore, the option to Subscribe to an external library must be disabled. If it were enabled, the library would instead attempt to synchronize content from a remote URL (such as a public VMware repository or another VCF instance).

Once created, this library acts as a "golden repository" that the provider can then share with multiple tenant organizations, ensuring consistency across the private cloud fleet.

NEW QUESTION: 29

An administrator is deploying a Supervisor cluster in VMware Cloud Foundation (VCF) Automation and notices that only one vSphere zone is configured in the deployment workflow.

Which statement best describes the capabilities of the Supervisor cluster being deployed?

- A.** The cluster enables the use of a single control plane across multiple vCenter instances.
- B.** The cluster will automatically upgrade to multi-zone when additional zones are provided.
- C.** The cluster will span multiple vSphere clusters for high availability.
- D.** The cluster will not have zone-level fault isolation.

Answer: D (LEAVE A REPLY)

VCF 9.0 supports both Single-Zone and Multi-Zone Supervisor cluster deployments. In a single-zone deployment, all Supervisor control plane VMs and worker nodes reside within a single logical and physical fault domain (a single vSphere cluster). Consequently, the cluster will not have zone-level fault isolation. If the underlying hardware, power, or top-of-rack switch for that specific zone fails, the entire Supervisor instance and all hosted workloads (VMs and Pods) will go offline. Multi-zone clusters, by contrast, distribute nodes across three distinct zones to ensure that the control plane and workloads can survive the complete loss of one zone. While a single-zone cluster is suitable for non-critical development or testing, it represents a significant risk for production environments that require the high-availability and fault-tolerance features inherent to the VCF 9.0 multi-zone architecture.

Valid 3V0-21.25 Dumps shared by Actual4test.com for Helping Passing 3V0-21.25 Exam! Actual4test.com now offer the **newest 3V0-21.25 exam dumps**, the Actual4test.com 3V0-21.25 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 3V0-21.25 dumps with Test Engine here: https://www.actual4test.com/3V0-21.25_examcollection.html (64 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)