Exam Questions 3V0-22.25

Advanced VMware Cloud Foundation 9.0 Operation

https://www.2passeasy.com/dumps/3V0-22.25/

NEW QUESTION 1
An administrator is tasked with configuring the allocation model in the VCF Operations Policies. The allocation model must be enabled at the level of the datastore. The current disk space usage on datastore of an existing virtual machine must be used to determine how many virtual machines will fit on the datastore. What two settings must the administrator configure in the policy definition at the datastore level?(Choose two.)

A. Peak Utilization
B. The capacity buffer
C. The disk space allocation
D. The custom profile
E. The overcommit ratio

Answer: DE

Explanation:
The administrator must configure theovercommit ratioand activate the appropriatecustom profileat the datastore policy level. In VCF Operations, the Allocation Model is enabled from the policy Capacity card by unlockingAllocation Modeland setting the overcommit ratio for CPU, memory, or disk space. For aDatastore, the allocation model specifically allows the administrator to set the overcommit ratio for datastore disk space, which controls how allocated storage capacity is calculated rather than relying only on demand-based usage . The second requirement is to use the current disk space usage of an existing VM to determine how many similar VMs can fit on the datastore. That is handled by acustom profile. Custom profiles define a hypothetical VM configuration and calculate VM remaining for objects such as datastores, datastore clusters, and cluster compute resources . The custom profile wizard also allows metric values to be copied from an existing object, including by VM name, vCenter, VM tag, or custom group . Peak utilization and capacity buffer do not enable allocation modeling or define VM-fit profiles. Reference topic:Objective 4.2 - Manage VCF Capacity / Allocation Model / Custom Profiles / Policy Capacity Settings.

NEW QUESTION 2
An administrator uses the Rightsize feature within VCF Operations which identifies an oversized VM and provides a default recommendation of a 4 vCPU reduction. After speaking to the VM owner, the administrator agrees to limit the downsizing amount to 50% of the default recommendation and to schedule the reduction during the upcoming maintenance window. Which action does the administrator take to perform the vCPU reduction automatically during the maintenance window?

A. Create a Scheduled Action through VCF Operations Automation Central
B. Access the vSphere Client and create a Scheduled Task to reduce the VM vCPU
C. Resize the VM directly through the Reclaim feature within VCF Operations
D. Create a Scheduled Action through the Rightsize feature within VCF Operations

Answer: D

Explanation:
The administrator must create the scheduled action directly from theRightsizefeature. VCF Operations Rightsize is the capacity-optimization workflow used to adjust CPU and memory allocations for oversized and undersized virtual machines. For oversized VMs, the administrator selects the target VM, opens the resize workflow, reviews the recommended vCPU and memory reduction, and can use the edit controls to modify the recommendation before execution. In this scenario, the default recommendation is a 4 vCPU reduction, but the agreed action is only 50 percent of that value, so the administrator adjusts the reduction to2 vCPU. The Rightsize page also providesSCHEDULE ACTION, which opens a scheduling dialog so the resize action can run later during the maintenance window; scheduled jobs are then managed through Automation Central . Automation Central is used to manage scheduled jobs, but the rightsizing task is initiated from Rightsize. Reclaim is used for powered-off VMs, idle VMs, snapshots, and orphaned disks, not vCPU rightsizing. vSphere scheduled tasks bypass VCF Operations recommendations. Reference topic:Objective 4.2 - Manage VCF Capacity / Rightsize Workloads / Oversized VMs / Scheduled Actions.

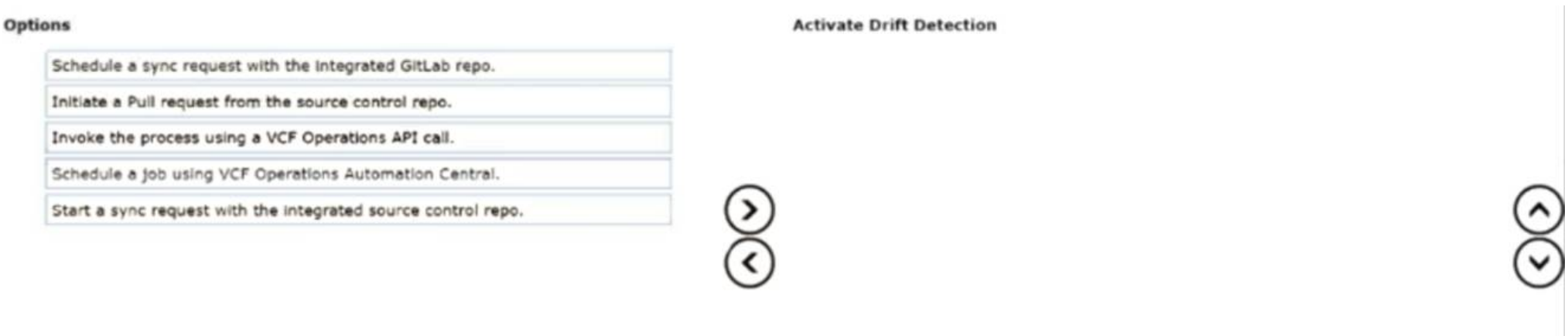
NEW QUESTION 3
An administrator has been tasked with enabling Service Discovery within VCF Operations. What steps must an administrator take to install and configure Service Discovery?

A. Service Discovery is enabled by default for all servers with VMware Tools installed, no action required
B. Within Administration, click Integrations and modify the properties of the vCenter by selecting the Service Discovery radio button to activate
C. Within Infrastructure Operations, click Configurations, select Service Discovery and click "Configure Service Discovery"
D. Within Workload Operations, click Manage SDMP Services and select Actions "Activate Service Monitoring"

Answer: C

Explanation:
The correct entry point isInfrastructure Operations>Configurations>Service Discovery>Configure Service Discovery. VCF Operations Service Discovery is not automatically enabled merely because VMware Tools is installed. VMware Tools is a dependency for discovery methods, but the vCenter adapter instance and Service Discovery configuration still must be enabled and associated with the relevant vCenter. The official workflow states that the administrator opensInfrastructure Operations>Configurations, selects theService Discoverytile, and clicksConfigure Service Discovery. From there, the administrator selects the vCenter instance, opens theService Discoverytab, and activates the Service Discovery option. Application Discovery and credential or credential-less discovery settings can also be enabled from the same workflow . Option B is incorrect because the documented navigation is not through an Administration menu, and the configuration is performed from the Service Discovery tile into the vCenter integration. Option D is used later to manage discovered services and monitoring state, not to initially configure the service discovery adapter. Reference topic:Objective 4.7 – Monitor Applications with VCF Operations / Service Discovery / Configure Service and Application Discovery.

NEW QUESTION 4
An administrator is tasked with using VMware Cloud Foundation Configuration Drift management in order to streamline an upcoming audit. Drag and drop the two options which can activate the properly configured Drift Detection into theActivate Drift Detectionlist on the right in any order.(Choose two.)



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Invoke the process using a VCF Operations API call.
Schedule a job using VCF Operations Automation Central.
The two valid activation methods are toinvoke Drift Detection through a VCF Operations API calland toschedule a job using VCF Operations Automation Central. VCF Operations Configuration Drift uses desired-state templates assigned through policy to compare vCenter and vSphere cluster configuration values against approved standards. The VCF 9.0 documentation states that unified configuration management supportsscheduled drift detectionfor vCenter and cluster objects and allows administrators to schedule drift detection through VCF Automation or the VCF Operations orchestrator . The scheduling workflow is performed fromFleet Management>Configuration Drifts>Schedule Drift Detection, where the administrator defines the scope, criteria, and schedule; after creation, VCF Operations creates a new job inAutomation Central. API invocation is also valid because VCF Operations exposes fleet and cloud proxy functionality through APIs for automation-driven operations . The GitLab or source-control sync options are not correct because source control synchronizes configuration templates, not the drift detection process itself. Pull requests govern template change review, not drift execution. Reference topic:Objective 4.16 – Monitor Security, Compliance and Configuration / Configuration Drift / Scheduled Drift Detection / Automation Central / API-driven operations

NEW QUESTION 5
An administrator is tasked with analyzing logs for esx.audit events related to firewall changes. The administrator chooses to review the logs using VCF Operations and enters two separate items into the search bar:
esx.audit
firewall
Based on the search criteria, which results will be displayed?

A. vpxd OR firewall related events
B. esx.audit AND vdefend related events
C. esx.audit OR firewall related events
D. esx.audit AND firewall related events

Answer: D

Explanation:
VCF Operations log analysis uses the search bar underInfrastructure Operations>Analyze>Logsto refine log-event results by keyword, phrase, glob, regular expression, or field operation. In the main search text box, multiple keywords entered together are treated as a logicalAND, not an OR. The official guidance states that to find events containing specified keywords, the administrator enters complete keywords, globs, or phrases in the search text box, and thatentering a space in the main search field is a logical AND operator. Therefore, entering esx.audit and firewall returns only log events that contain both terms: events matching esx.audit and also matching firewall. This is the correct behavior when the administrator is searching for ESX audit events specifically related to firewall changes. Option C would apply to OR-style behavior, but that applies to multiple values inside a single filter row when entered as separate filter values, not to the main search bar keyword syntax . Options A and B introduce unrelated terms and do not match the provided search criteria. Reference topic:Objective 4.12 – Log Event Monitoring and Analysis in VCF Operations / Searching and Filtering Log Events / Search bar keyword logic.

NEW QUESTION 6
Which type of Plugin must the administrator configure to enable WLP Action-based notifications?

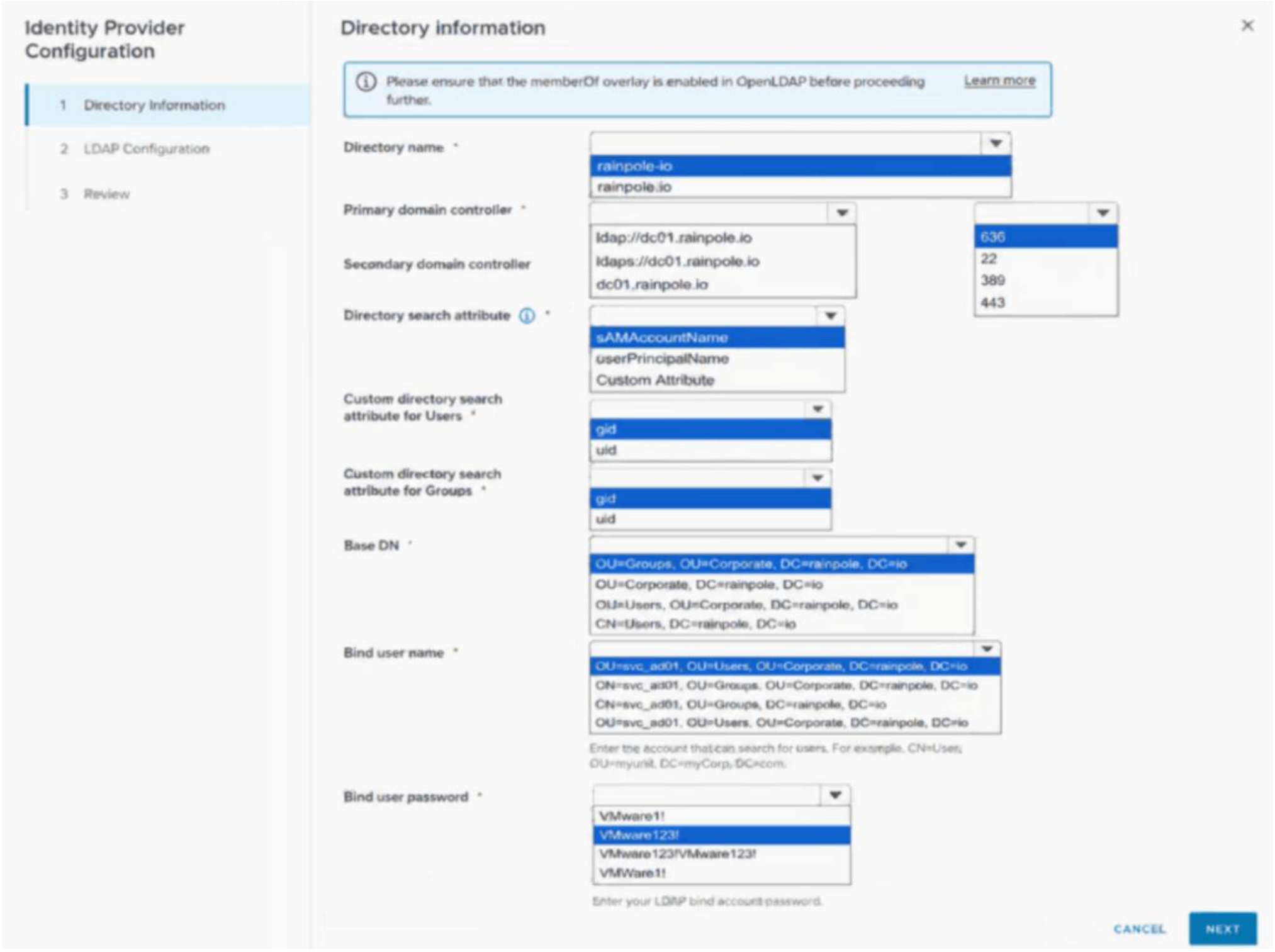
A. Network Share
B. SNMP Trap
C. Webhook Notification
D. Standard Email

Answer: C

Explanation:
The required plug-in type isWebhook Notification Plugin. Workload Placement Action-based notifications are a specific notification type used forWLP virtual machine movement tasks, not standard alert notifications. The VCF Operations documentation states that administrators can create and manage Workload Placement action-based notifications and configure actions for which notifications are sent when a WLP action succeeds, fails, or times out. It further specifies that notifications are sent after the WLP VM movement task completes, regardless of final status . Before such notification rules can be created, the administrator must configure theWebhook Notification Plugin. In the WLP Action notification workflow, the outbound method supported by default is the Webhook Notification Plugin, and the administrator selects or creates a Webhook plug-in instance before selecting the payload template . This is reinforced in the payload-template workflow, whereActionappears only whenWebhook Notification Pluginis selected as the outbound method; WLP Action notification payloads are configurable only for Webhook . Network Share does not support notification rules, and SNMP or Standard Email are used for alert-style notifications, not WLP Action notifications. Reference topic:Objective 4.9 – Notifications / Outbound Plugins / WLP Action-Based Notifications.

NEW QUESTION 7
An administrator has been tasked with configuringVCF Single Sign-On (SSO)in VCF Operations.

The following OpenLDAP Directory information has been provided:
The OpenLDAP server is calleddc01.rainpole.io.
All Users and Groups are located within an OU calledCorporate.
All Users are located within theUsersOU.
All Groups are located within theGroupsOU.
The bind user is calledsvc_ad01and has a password ofVMware123!.
The OpenLDAP domain does not support SSL/TLS certificates.
Thegiduniquely identifies Groups.
Theuiduniquely identifies Users.
Complete the Directory Information page of the Identity Provider Configuration wizard. Select the correct values from each of the nine drop-downs.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Directory name:rainpole-io
Primary domain controller:ldap://dc01.rainpole.io
Primary domain controller port:389
Directory search attribute:Custom Attribute
Custom directory search attribute for Users:uid
Custom directory search attribute for Groups:gid
Base DN:OU=Corporate, DC=rainpole, DC=io
Bind user name:CN=svc_ad01, OU=Users, OU=Corporate, DC=rainpole, DC=io
Bind user password:VMware123!
The configuration must match the OpenLDAP hierarchy and transport requirements. Because the directory does not support SSL/TLS, the primary domain controller must use the non-secure LDAP scheme,ldap://dc01.rainpole.io, with standard LDAP port389, not LDAPS port 636. The directory name should use the VCF SSO directory identifier format, thereforerainpole-iois selected. Since the environment uses OpenLDAP-specific attributes rather than Active Directory defaults, the directory search attribute must be set toCustom Attribute. The user identifier isuid, so the custom user search attribute is uid; the group identifier isgid, so the custom group search attribute is gid. The Base DN must cover both the Users and Groups OUs. Because both are insideOU=Corporate, the correct base scope isOU=Corporate, DC=rainpole, DC=io, not only Users or only Groups. The bind user resides in the Users OU, so the bind DN isCN=svc_ad01, OU=Users, OU=Corporate, DC=rainpole, DC=iowith passwordVMware123!. Reference topic:Objective 4.14 – Fleet Management / Identity and Access Management / VCF Single Sign-On / LDAP Identity Provider Configuration.

NEW QUESTION 8
Given the scenario provided, which three statements should the administrator use to describe the way that the Capacity Models are configured within the VCF workload domain?(Choose three.)

A. The most constrained resource in CL-01 is CPU Allocation
B. The Allocation model has not been enabled on CL-02
C. The Allocation model for CPU in CL-01 has been configured with a 4:1 vCPU:Core ratio
D. The most constrained resource in CL-02 is Memory Allocation
E. The Allocation model has not been enabled on CL-01
F. The Allocation model for CPU in CL-01 has been configured with a 5:1 vCPU:Core ratio

Answer: ABF

Explanation:
CL-01 is using both Demand and Allocation capacity models. The Demand model is shown by GHz and physical memory capacity remaining, while the Allocation model is shown by allocated capacity values such asvCPUsand expanded memory capacity. VCF Operations states that the Allocation model is enabled in policy by setting overcommit ratios for Cluster Compute Resource CPU, memory, and disk space, and that the Capacity tab displays Demand by default and Allocation values when configured . CL-01 has 60 physical cores. It reports 300 vCPUs as the allocation basis, so the CPU allocation ratio is300 ?? 60 = 5:1, not 4:1. This aligns with the documented allocation calculation where the vCPU count is derived from physical cores multiplied by the overcommit ratio . CL-01??s most constrained resource is CPU Allocation because only 30% of vCPU capacity remains, compared with 80% GHz remaining and 80% memory remaining. CL-02 shows only GHz and physical memory values, with no vCPU or allocation-expanded memory values, so the Allocation model is not enabled for CL-02. Reference topic:Objective 4.2 – Capacity Models / Allocation vs Demand / Overcommit Ratios / Capacity Remaining.

NEW QUESTION 9
An administrator has been tasked with configuring a VCF Operations policy to enable a more conservative capacity modelling. When setting the Risk Level Configuration, what is the time remaining metric based on?

A. Actual Projection of Available Capacity Mean
B. Actual Projection of Capacity Utilization Mean
C. Lower Bounds Projection of Capacity Utilization
D. Upper Bounds Projection of Capacity Utilization

Answer: D

Explanation:
For conservative capacity modelling, theTime Remainingcalculation is based on theupper bound projection of capacity utilization. VCF Operations uses its capacity engine to analyze historical utilization and forecast future workload. The engine projects future workload as a range, consisting of an upper-bound projection and a lower-bound projection. The documentation states that capacity calculations are based ontime remaining and risk level, and that the capacity engine uses theupper bound projectionfor a conservative risk level, while an aggressive risk level uses the mean between the upper and lower projections . This behavior is intentionally cautious: conservative modelling assumes the higher side of projected utilization, making resource exhaustion appear sooner and reducing the chance of underestimating future demand. The Time Remaining metric itself represents the number of days until projected utilization crosses the threshold for usable capacity . Therefore, the answer is not based on available-capacity mean, utilization mean, or lower-bound utilization. Those would produce less conservative or different planning outcomes. Reference topic:Objective 4.2 – Manage VCF Capacity / Policy Capacity Settings / Risk Level Configuration / Time Remaining.

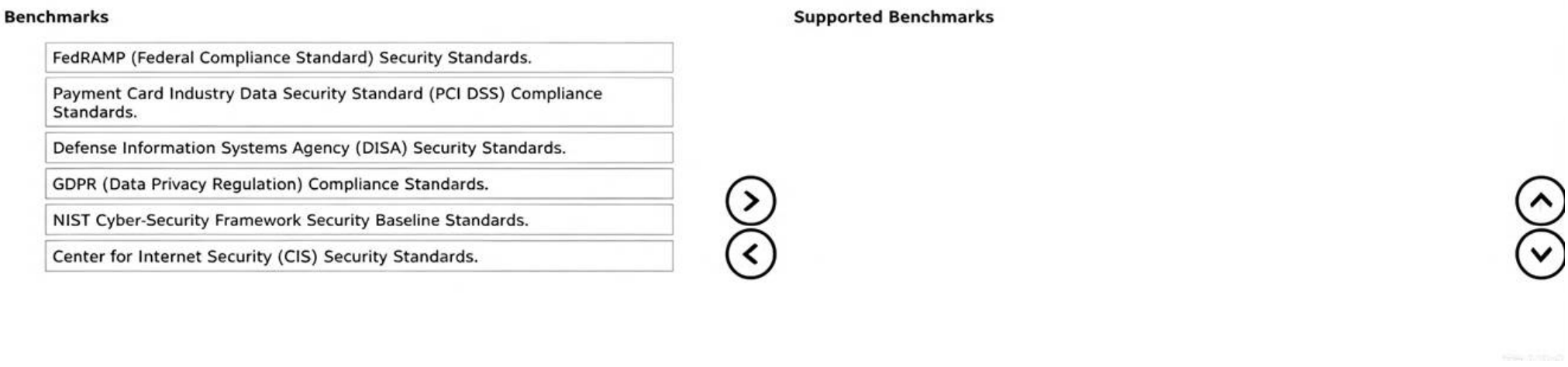
NEW QUESTION 10
An administrator has been tasked with scaling an existing VCF instance that consists of one workload domain that uses vSAN as its principal storage. The requirements are to add an additional workload domain and manage the new workload domain from the existing vCenter. Which two actions must the administrator take?(Choose two.)

A. Ensure the new hosts are commissioned with the valid storage type and mapped to a network pool prior to domain creation
B. Ensure the existing workload domain uses the same NSX Manager as the management domain
C. Create a vCenter Linking Group to link the two workload domain vCenters
D. Ensure the new workload domain uses the same SSO domain as the existing workload domains
E. Configure vCenter Enhanced Link-mode to link the two workload domain vCenters
F. Ensure the new workload domain is configured using vSAN storage with compatible disks installed

Answer: AC

Explanation:
The administrator must first ensure that the new ESX hosts are properly prepared for workload-domain creation. In VCF, adding a new workload domain requires commissioned hosts that match the intended principal storage type and have the necessary network-pool resources available. Since the existing environment uses vSAN, the hosts used for the new domain must be suitable for the selected storage model and have the required networking in place before domain creation. Creating a workload domain adds a logical pool of compute, network, and storage resources to the VCF instance (TechDocs). The second requirement is management visibility from the existing vCenter. In VCF 9.0, this is achieved throughvCenter Linking Groups, not Enhanced Linked Mode. vCenter linking in VCF Operations provides a single-pane-of-glass view of linked vCenter instances from one vSphere Client (TechDocs). Option B is incorrect because workload domains cannot use the management domain NSX Manager. Option D reflects older SSO-domain thinking and is not the VCF 9.0 linking model. Option E is incorrect because Enhanced Linked Mode is not the preferred VCF 9.0 mechanism. Reference topic:Objective 4.1 / 4.14 – Day 2 administration, workload-domain scaling, vCenter Linking Groups, and host preparation.

NEW QUESTION 10
An administrator has been tasked with identifying the built-in regulatory benchmarks supported in VCF Operations.
Drag and drop the three correct benchmarks from theBenchmarkslist on the left and place them into theSupported Benchmarkslist on the right in any order.(Choose three.)



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Payment Card Industry Data Security Standard, PCI DSS, Compliance Standards
Defense Information Systems Agency, DISA, Security Standards
Center for Internet Security, CIS, Security Standards
The supported benchmarks from the provided list arePCI DSS,DISA, andCIS. VCF Operations compliance monitoring is accessed fromSecurity>Compliance, where compliance scorecards are based on alert definitions with theCompliancesubtype. The official VCF 9.0 documentation states thatRegulatory Benchmarksdisplay benchmarks for industry-standard regulatory compliance requirements and explicitly listsDefense Information Systems Agency (DISA) Security Standards,Payment Card Industry Data Security Standard (PCI DSS) Compliance Standards, andCIS Security Standardsas supported regulatory benchmark options. DISA is available as a native pack, PCI DSS is listed as a regulatory compliance standard, and CIS is supported through a compliance pack from VMware Marketplace . FedRAMP and GDPR are not listed in the VCF Operations regulatory benchmark set shown in the guide. NIST is supported only as specificNIST SP 800-171andNIST SP 800-53 R5packs, not as the generic ??NIST CyberSecurity Framework Security Baseline Standards?? option shown in the question . Reference topic:Objective 4.16 – Monitor Security, Compliance and Configuration / Compliance Benchmarks / Regulatory Benchmarks.

NEW QUESTION 15
An administrator is responsible for a VCF Private Cloud. VCF Operations has identified a VM that violated the CIS Security Standards Benchmark. Which three actions will allow the administrator to determine which symptom(s) triggered the compliance alert?(Choose three.)

A. Open the compliance alert and expand Potential Evidence to review the triggered symptoms.
B. Open the compliance alert and expand Related Alerts to review the triggered symptoms.
C. In the VM's Alerts view, set Alert Subtype = Compliance to locate the correct compliance alert.
D. In the VM's Alerts Actions, click Go to Alert Definition.
E. In the VM's Alerts view, set Object Type = Compliance to locate the correct compliance alert.
F. Open the compliance alert and expand Alert Basis to review the triggered symptoms.

Answer: ACF

Explanation:
The administrator should first locate the relevant VM compliance alert by filtering the VM??s alert list usingAlert Subtype = Compliance. Compliance benchmark violations are implemented as alert definitions and symptoms, so filtering by compliance subtype narrows the alert list to the correct class of benchmark findings. After opening the alert, the administrator should inspect the alert evidence and specifically expandAlert Basis. Broadcom documents thatAlert Basisshows the active symptoms or conditions that were met for the alert whenActive Onlyis enabled, which directly identifies the symptom or symptoms that triggered the compliance violation (TechDocs). ThePotential Evidenceview is also part of the alert investigation workflow and exposes supporting evidence around the alert, including the basis used to explain why the alert fired (TechDocs).Related Alertsis not the correct place to identify the triggering symptom; it shows other correlated alerts.Object Type = Complianceis invalid because compliance is an alert subtype, not a VM object type.Go to Alert Definitionshows the configured definition, but not necessarily which symptoms were active on that VM at trigger time. Reference topic:Objective 4.16 – Compliance Benchmarks / CIS Security Standards / Alert Basis and Triggered Symptoms.

NEW QUESTION 16
An administrator has been tasked with creating a custom group for NSX edges. The first two NSX Edges have been tagged with the tag nsx:edge. The custom group has Object Type = Edge Cluster and membership criteria Tag Category = nsx, Tag Value = edge. After 60 minutes the group still has no members. What action must the administrator take?

A. B.Change the Tag Value to nsx:edge C.Change the Tag Category to edge D.Change the object type to Virtual Machine

Answer: A

NEW QUESTION 17
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 3V0-22.25 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 3V0-22.25 Product From:

https://www.2passeasy.com/dumps/3V0-22.25/

Money Back Guarantee

3V0-22.25 Practice Exam Features:

* 3V0-22.25 Questions and Answers Updated Frequently

* 3V0-22.25 Practice Questions Verified by Expert Senior Certified Staff

* 3V0-22.25 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 3V0-22.25 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year