VMware

Exam Questions 3V0-22.25

Advanced VMware Cloud Foundation 9.0 Operation

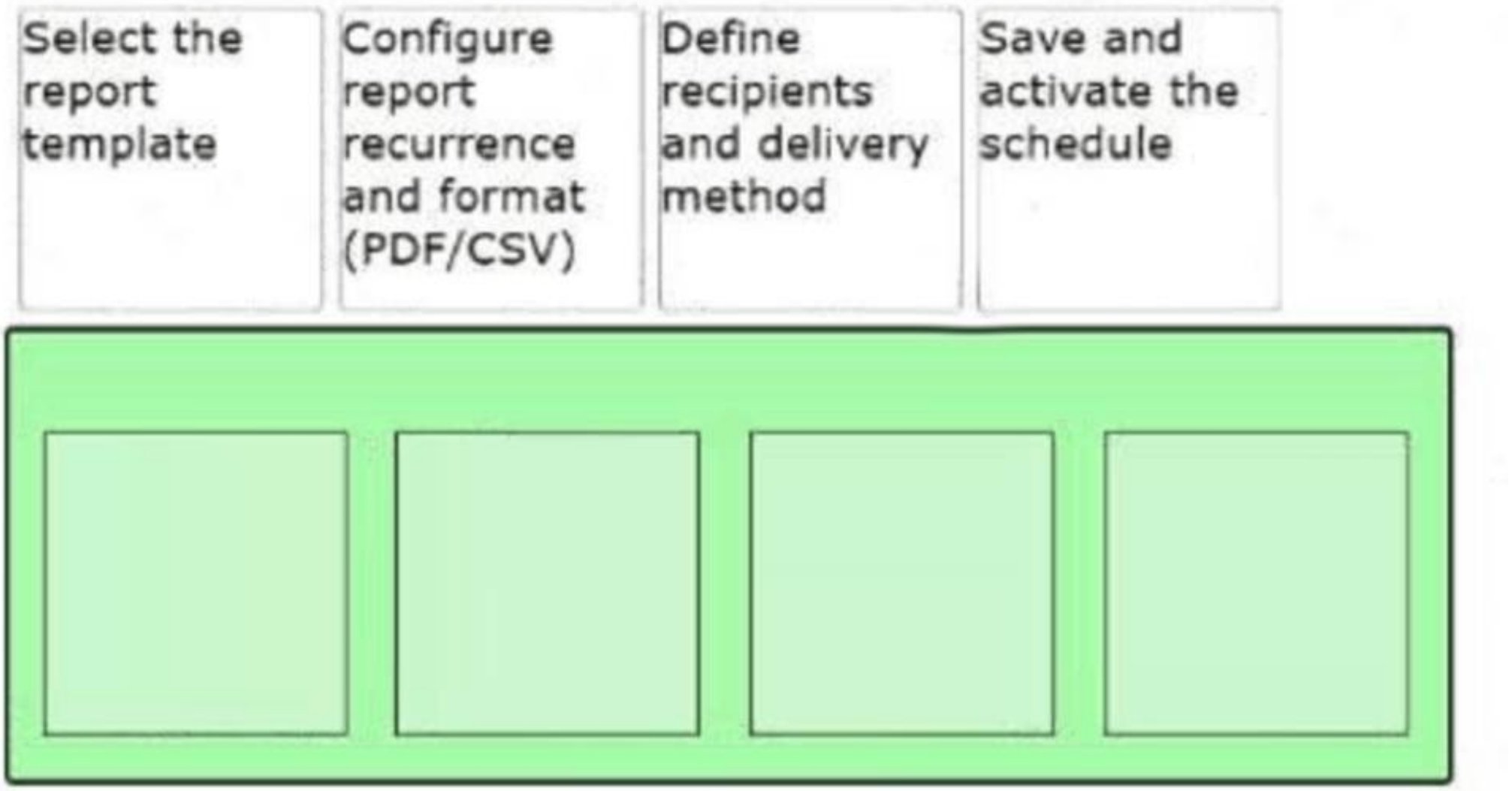
NEW QUESTION 1
An administrator successfully integrated VCF Operations Fleet Management with a Microsoft Certificate Authority and deployed certificates to vCenter, NSX, VCF Operations, and ESX hosts. VCF Operations now reports that all certificates are nearing expiration even though auto-renewal rotated certificates a week ago and the template allows certificates to last one year. What is the reason certificate warnings are still being generated?

A. SDDC Manager has lost contact with the Microsoft CA
B. The certificate alert in VCF Operations has not been properly cleared
C. The Microsoft CA Root or Intermediate certificates are nearing expiration
D. The administrator must manually click "Renew Certificate" on desired items

Answer: C

Explanation:
The warnings persist because theissuing certificate chain, not the renewed leaf certificates, is approaching expiration. VCF Operations Fleet Management can view certificate details and certificate alerts across VCF Management and VCF Instance components, including vCenter, NSX Manager, SDDC Manager, ESX, and VCF Operations components . Auto-renewal only renews supported component TLS certificates and occurs 60 days before certificate expiration; it does not renew root certificates . When certificates are issued by an enterprise Microsoft CA, the validity of endpoint certificates is constrained by the validity of the issuing chain. vSphere documentation states that a certificate cannot be renewed with an expiration date beyond the expiration of the trusted root certificate . Therefore, even if the component certificates were recently rotated and the template is configured for one year, the generated certificates may still inherit a shorter effective validity period if the Microsoft CA root or intermediate certificate is expiring soon. The correct remediation is to renew or replace the CA chain, not repeatedly clear alerts or manually renew endpoint certificates. Reference topic:Objective 4.14 - Fleet Management / Certificate Management / Auto-Renewal / CA Chain Validity.

NEW QUESTION 2
Arrange the following steps in the correct order to schedule the delivery of a weekly report created in VCF Operations.



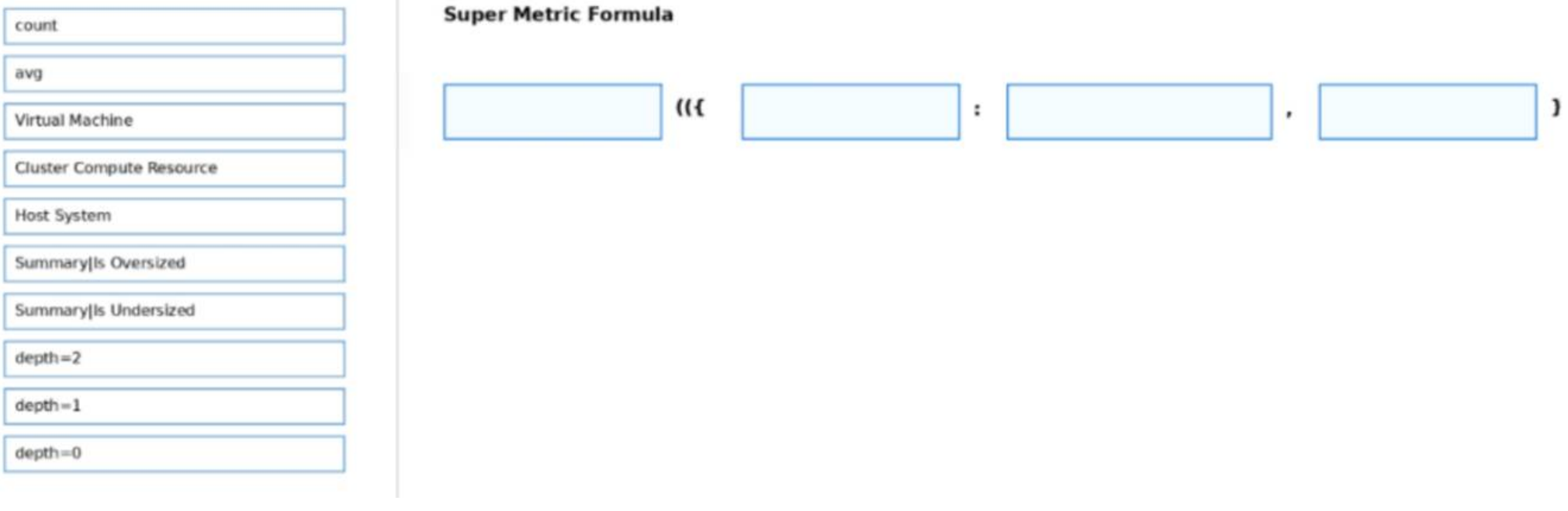
A. Mastered
B. Not Mastered

Answer: A

Explanation:
The correct sequence starts by selecting the relevantreport template, because VCF Operations schedules are created against an existing predefined or custom report template. The documented workflow is accessed fromInfrastructure Operations>Dashboards&Reports>Reports, where the administrator selects the required template from theReport Templatestab and choosesSchedulefrom the template actions . After the template and target object are selected, the administrator configures the schedule parameters, including time zone, start date, start time, andRecurrence. For a weekly report, the recurrence is set toWeekly. Report output is based on the template format, and VCF Operations supports bothPDFandCSVreport formats . The next step is to define delivery, such as enablingEmail report, entering recipients, and selecting the outbound rule, or saving the report to an external location such as a network share . Finally, the administrator saves the configuration to activate the schedule. Reference topic:Objective 4.10 - Creating Custom Dashboards, Views and Reports / Schedule a Report / Report Templates / Recurrence and Delivery Options.

NEW QUESTION 3
An administrator has been tasked with creating a new report in VCF Operations that details the total number of oversized virtual machines within a VMware Cloud Foundation workload domain cluster.
The following information has been provided:
Each VCF workload domain cluster has a separate VCF Operations policy assigned.

Only the metrics required for each object should be collected.
Drag and Drop the four components to complete the Super Metric formula required for the report.(Choose four.)



A. Mastered
B. Not Mastered

Answer: A

Explanation:

The report must count oversizedVirtual Machineobjects beneath the workload domain cluster. The correct aggregate function iscount, because the requirement is a total number, not an average. The correct object type isVirtual Machine, because the oversized state is a VM-level metric. The correct metric isSummary|Is Oversized, which maps to the VM metric key summary|oversized and returns whether the VM is oversized . The correct relationship depth isdepth=2, because the VCF Operations super metric guidance states that when a super metric is assigned to a cluster and calculates across virtual machines, the cluster is two levels above the VM in the relationship chain, so depth must be changed to 2

NEW QUESTION 4
An administrator was requested to define an Operational Intent that ensures the minimum number of clusters in the data center are used to host virtual machines, while still maintaining adequate performance. Currently, there are 10 clusters available within a single data center, each with 10 ESX hosts. Which feature should the administrator configure?

A. Admission Control based on slots
B. Workload Optimization - Consolidate
C. Distributed Resource Scheduler with Aggressive threshold
D. Cluster Headroom set to 10%

Answer: B

Explanation:
The administrator should configureWorkload Optimization - Consolidate. In VCF Operations, Operational Intent defines how workload placement and optimization should behave across clusters. TheConsolidatemode is specifically intended to minimize the number of clusters used by workloads while still maintaining acceptable performance. Broadcom's Workload Automation policy documentation describes Consolidate as the mode used to proactively minimize the number of clusters used by workloads, which directly aligns to the requirement to use the smallest possible number of clusters in the data center while continuing to meet performance goals. (TechDocs) Admission Control based on slots is a vSphere HA construct and does not provide VCF Operations workload-placement intent across multiple clusters. DRS aggressiveness affects balancing inside a cluster, not strategic placement across 10 clusters. Cluster Headroom reserves capacity buffer, but by itself it does not drive consolidation behavior. Reference topic:Objective 4.6 - Workload Optimization in VCF Operations / Operational Intent / Consolidate, Balance, and Moderate modes.

NEW QUESTION 5
A developer has created and successfully installed a new design using the VCF Operations Management Pack Builder. An administrator has observed that only some metrics are collected, relationships between two objects are not relayed correctly, and no alerts are generated when conditions exist in the target datasource. Which three data sources are available in VCF Operations to help troubleshoot the issue?(Choose three.)

A. Management Pack Builder Runtime Debug Interface
B. VCF Operations Integration Designer Controller log
C. VCF Operations Request Log
D. Management Pack Builder Adapter log
E. Management Pack Builder Design Screen
F. VCF Operations Observability Workbench

Answer: BCD

Explanation:
The correct troubleshooting sources are theRequest Log, theManagement Pack Builder Adapter log, and theIntegration Designer Controller log. Management Pack Builder troubleshooting is centered on validating the API requests, collection execution, adapter behavior, and server-side design processing. The VCF 9.0 documentation states that every test request or test collection in Management Pack Builder exposes request tabs showing the body, headers, and logs; these are used to diagnose response-code errors and request/response issues . For collection problems after installation, the administrator should reviewManagement Pack Builder Adapter logs, located under $VCOPS_BASE/user/log/adapters/MPBAdapter on the selected node or cloud proxy, because these logs show adapter-side warnings and errors during collection . If the issue appears to be with Management Pack Builder itself, the official guidance identifies /usr/lib/vmware-vcops/user/log/integration-designer-controller.log as the server-side log to review . The Design Screen is used to build and verify definitions, but it is not one of the listed troubleshooting data sources. Observability Workbench is for infrastructure troubleshooting, not Management Pack Builder design diagnostics. Reference topic:Objective 4.8 - Management Pack Builder / Troubleshooting a Design.

NEW QUESTION 6
Match the VCF Operations for Logs feature with its description by dragging and dropping the correct item from the Feature list on the left and placing it onto the Description list on the right.

Feature		Description
Shared Dashboards		Custom defined filters that can be shared with all users to aid searching and aggregating log event data.
Regex		Individual elements within a dashboard used for displaying data and queries.
Widgets		Custom defined views of data from custom queries, accessible to other teams to aid troubleshooting.
Report		Format used to query the log data for specific patterns that are not associated with a predefined field.
Extracted Field		Copy of a dashboard over a defined time period that can be scheduled and emailed.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Feature	Correct Description
Shared Dashboards	Custom defined views of data from custom queries, accessible to other teams to aid troubleshooting.
Regex	Format used to query the log data for specific patterns that are not associated with a predefined field.
Widgets	Individual elements within a dashboard used for displaying data and queries.
Report	Copy of a dashboard over a defined time period that can be scheduled and emailed.
Extracted Field	Custom defined filters that can be shared with all users to aid searching and aggregating log event data.

VCF Operations for Logs usesqueriesmade from keywords, regular expressions, field operations, and aggregations. Regular expressions provide sophisticated pattern matching when keyword or glob searches are not sufficient.Extracted fieldsadd structure to unstructured logs and can be used in filters and aggregations. Dashboards are created from widgets and views, while reports are scheduled snapshots of dashboards or views that can be distributed for offline review.

NEW QUESTION 7
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 8
An administrator is tasked with collecting metrics from multiple VCF Private Clouds. The environment contains two VCF Fleets, each Fleet has two VCF instances, each VCF instance has one Management Domain and two Workload Domains, there must be no single point of failure, and each domain requires dedicated collectors. What is the minimum number of collectors the administrator must install?

A. 6
B. 4
C. 10
D. 12

Answer: D

Explanation:
The minimum count is12 collectors, because the requirement is stated at thedomainlevel and each VCF instance contains three domains: one Management Domain and two Workload Domains. The calculation is:2 Fleets ?? 2 VCF Instances per Fleet ?? 3 Domains per VCF Instance = 12 dedicated domain collectors. VCF 9.0 defines a VCF private cloud as containing one or more VCF fleets, a VCF fleet as containing one or more VCF instances, and a VCF instance as consisting of a management domain and optional workload domains . VCF Operations collector architecture also supports scaling collection by adding collector nodes and assigning them through collector groups; collector groups are used to increase resiliency when a collector becomes unavailable and redistribute collection work across remaining collectors . Because the question states that each domain requires dedicated collectors, the administrator cannot satisfy the design by sharing a single collector across multiple domains or counting only the VCF instances. Options 4, 6, and 10 undercount the total number of managed domains. Reference topic:Objective 4.1 – Day 2 Tasks / Unified Cloud Proxies / Collector Groups / Scaling VCF Operations Collection.

NEW QUESTION 9
An administrator is configuring an offline depot for a newly deployed VMware Cloud Foundation fleet. The VCF Download Tool is used to populate the depot because the installation is operating in a dark site environment. What does the VCF Download Tool require to authenticate with the Broadcom Business Portal and download the required software binaries?

A. A Download Token from the Broadcom Business Portal
B. A download SKU using the --sku option
C. The VCF or VVF bundleId to be downloaded
D. The target component using the component option

Answer: A

Explanation:
The VCF Download Tool requires adownload tokengenerated from the Broadcom portal to authenticate entitlement and download software binaries into an offline depot. In a dark-site deployment, the depot server is populated externally because the VCF environment cannot directly reach the online depot. The official VCF 9.0 documentation describes the VCF Download Tool as the CLI utility used to manage binaries and metadata for VMware Cloud Foundation lifecycle operations, including offline binary handling . The documented workflow for downloading binaries specifically instructs the administrator to obtain a download token from the Broadcom Support Portal, create a token file, and pass it to the tool using the depot download token file option . The SKU, bundle ID, and component parameters are selection or filtering inputs used to target what is downloaded; they do not authenticate the session. Authentication and entitlement validation are performed by the download token. Reference topic:Objective 4.14 – Fleet Management activities / offline depot / binary management / VCF Download Tool.

NEW QUESTION 10
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.

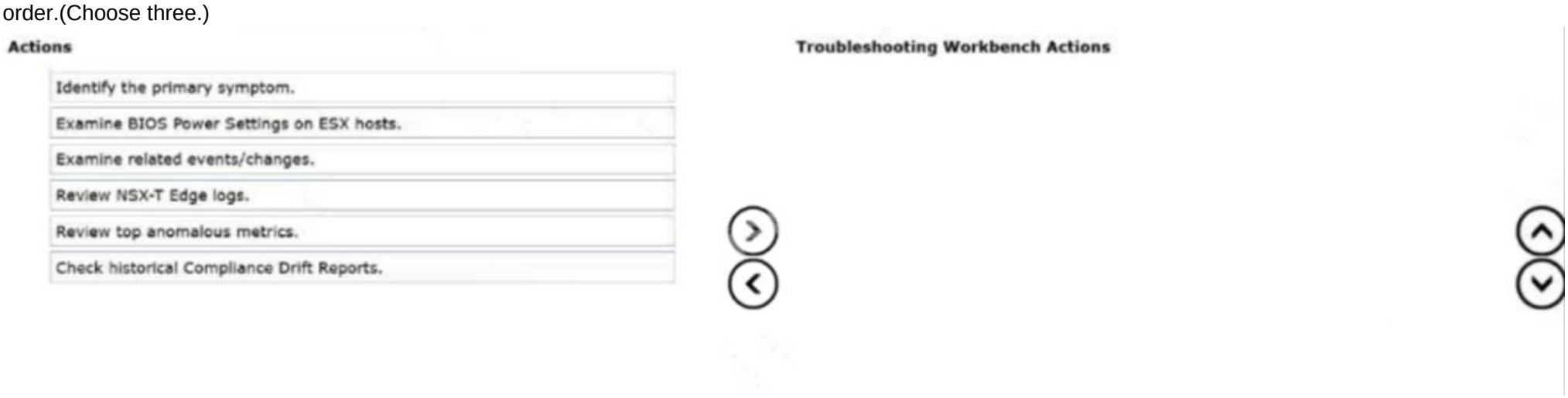
NEW QUESTION 10
Which type of Plugin must the administrator configure to enable WLP Action-based notifications?

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 11
An administrator has been tasked with investigating reports of degraded VM performance using theVCF Operations Troubleshooting Workbench.
Drag and drop the three correct actions from theActionslist on the left and place them into theTroubleshooting Workbench Actionslist on the right in any order.(Choose three.)



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Identify the primary symptom
Examine related events/changes
Review top anomalous metrics
The correct Troubleshooting Workbench actions are toidentify the primary symptom,examine related events or changes, andreview top anomalous metrics. VCF Operations Observability/Troubleshooting Workbench is designed to investigate known or unknown issues by focusing on a selected object, alert, or metric within a defined scope and time range. The documentation states that the workbench searches for potential evidence around the problem and displays evidence as cards based onEvents,Property Changes, andAnomalous Metrics. Events show metric-behavior changes and major events in the selected scope and time. Property Changes show important configuration changes that occurred in that same scope. Anomalous Metrics show metrics with drastic changes and rank them by the degree of change, giving the most relevant anomalies the highest weight . Therefore, reviewing anomalies and related changes is central to the workbench workflow. Identifying the primary symptom is the starting point for narrowing the investigation. BIOS power settings, NSX Edge logs, and historical Compliance Drift reports may support broader troubleshooting, but they are not core Troubleshooting Workbench actions. Reference topic:Objective 4.9 – Troubleshooting Workbench / Potential Evidence / Events, Property Changes, and Anomalous Metrics.

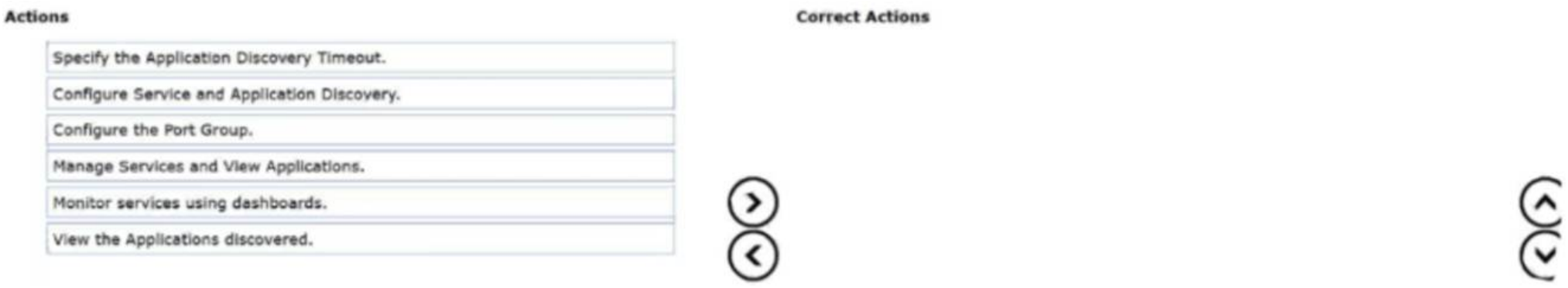
NEW QUESTION 13
An administrator deploys the company's first two VCF instances within a single VCF Fleet and connects both VCF Instances to a VCF Operations Fleet Management Single Sign-On configuration managed by the first VCF instance using an LDAP Identity Provider. The second VCF instance must now be connected to a new SAML 2.0 Identity Provider and Single Sign-On configuration. What action must the administrator take to begin configuring the second VCF instance to use a new VCF Single Sign-On configuration?

A. Reset the VCF Single Sign-On that is associated with the second VCF Instance
B. Deregister the second VCF Instance from the Single Sign-On configuration
C. Deregister the first VCF Instance from the Single Sign-On configuration
D. Reset the VCF Single Sign-On that is associated with the first VCF Instance

Answer: B

Explanation:
The administrator mustderegister the second VCF Instance from the existing Single Sign-On configuration. In this scenario, the second VCF Instance is currently attached to an SSO configuration whose identity source is managed by the first VCF Instance. The requirement is not merely to change the LDAP provider on the existing shared configuration; it is to connect the second instance to anew SAML 2.0 Identity Provider and a new VCF Single Sign-On configuration. The VCF 9.0 documentation provides a specific workflow for this condition: when a VCF Instance must be removed from an existing SSO configuration, the administrator navigates to the VCF Instance, opensComponent Configuration, filters configured components, selects all configured components, and clicksDeregister Component. After all registered components are deregistered, the page reloads and allows the administrator to either connect to an existing SSO configuration or create a new SSO configuration for that VCF Instance . Resetting the first instance would disrupt the controlling SSO configuration. Resetting the second instance is used for changing identity-source details within its own SSO lifecycle, not for detaching it from an SSO configuration managed by another instance. Reference topic:Objective 4.14 – Fleet Management / Identity and Access Management / VCF Single Sign-On / Deregister VCF Instance from SSO.

NEW QUESTION 14
An administrator can discover and monitor services using VCF Operations.
Which three actions should administrators take in VCF Operations to discover and monitor services and add and view applications?(Choose three.)



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Configure Service and Application Discovery
Manage Services and View Applications
Monitor services using dashboards
The three correct actions areConfigure Service and Application Discovery,Manage Services and View Applications, andMonitor services using dashboards. VCF Operations uses the Service Discovery adapter to discover services running inside virtual machines and to build service relationships or dependencies between services running on different VMs. The official workflow states that, to discover and monitor services and add and view applications, administrators should configure Service and Application Discovery, manage services and view applications, monitor services using dashboards, and view discovered services . Configuration starts fromInfrastructure Operations>Configurations>Service Discovery, where the administrator enables Service Discovery and Application Discovery on the vCenter integration . Service monitoring is then managed fromWorkload Operations>Applications>Manage SDMP Services, where administrators can provide credentials, activate service monitoring, and view service discovery status . Applications are viewed fromWorkload Operations>Applications, where VCF Operations shows application resources, connected VMs, service relationships, graphs, lists, and links . Application Discovery Timeout and Port Group configuration are not required actions in this workflow. Reference topic:Objective 4.7 – Monitor Applications with VCF Operations / Service Discovery / Manage Services / View Applications / Service Discovery Dashboards.

NEW QUESTION 18
An administrator is tasked with creating an alert definition that will send a notification when the following condition is met: for any NSX Edge Node that has a CPU Utilization > 95%. Which base object-type must the administrator use?

A. NSX: Edge Cluster
B. NSX: Transport Node
C. vCenter: Virtual Machine
D. vCenter: Entity Status

Answer: B

Explanation:
The correct base object type isNSX: Transport Node. In VCF Operations, an NSX Edge Node is modeled operationally as anNSX Edge Transport Node, not simply as a vCenter virtual machine. The alert definition must therefore be built against the NSX object type that owns the relevant NSX system-resource metrics. The VCF Operations documentation identifies Edge Node health monitoring as includingEdge Resource Utilization, which summarizes CPU, memory, and disk storage utilization for the node . The metrics reference also states that VCF Operations for Networks collects metrics forNSX-T Transport Node, and under Node Metrics includesCPU Usage (%), described as the percentage of CPU used out of total capacity during the interval . This aligns directly with an alert condition such as CPU Utilization > 95%.NSX: Edge Clusteris a higher-level grouping object and would not be the correct base for per-node CPU utilization.vCenter: Virtual Machinewould monitor the appliance as a VM, but not the NSX transport-node metric model.vCenter: Entity Statusis not appropriate for CPU thresholding. Reference topic:Objective 4.9 – Configure a Custom Alert / NSX Transport Node Metrics / Edge Node Resource Utilization.

NEW QUESTION 23
Which four steps should the administrator perform within VCF Operations to determine whether there is sufficient capacity within the cluster to complete all planned migration phases?(Choose four.)

A. Create a single What-If Analysis scenario that represents all migration phases together
B. Persist each scenario configuration without performing analysis
C. Add virtual machine workloads to each What-If Analysis scenario for the corresponding migration phase
D. Import Application Profiles from the source vCenter environment
E. Run all What-If Analysis scenarios together to evaluate the combined impact on the target cluster
F. Create a separate What-If Analysis scenario for each migration phase
G. Configure an Application Profile in each scenario to represent the VM t-shirt sizing

Answer: CEFG

Explanation:
The administrator should model the phased migration by usingWhat-If Analysisworkload planning, not migration execution workflows. Because the target workload domain usesvSAN, the correct planning model is the hyperconverged workload-planning workflow, where VCF Operations lets the administrator add or remove VM workloads in a vSAN environment and evaluate the capacity effect on the selected cluster . Each migration phase should be represented as a separate scenario: small VMs, medium VMs, and large VMs. In each scenario, the administrator configures anApplication Profileto represent the t-shirt size by defining vCPU, memory, and disk space, then adds the corresponding number of VM workloads for that phase . Since the source vCenter is unmanaged, importing profiles or VM templates directly from the source environment is not the correct method. After the scenarios are created, VCF Operations allows compatible saved scenarios that target the same object to be selected and run together, so the administrator can evaluate the cumulative impact of all planned phases on the target cluster . Reference topic:Objective 4.3 – Forecast VCF Capacity Growth / What-If Analysis / Add VM Workloads / Run Multiple Scenarios Cumulatively.

NEW QUESTION 27

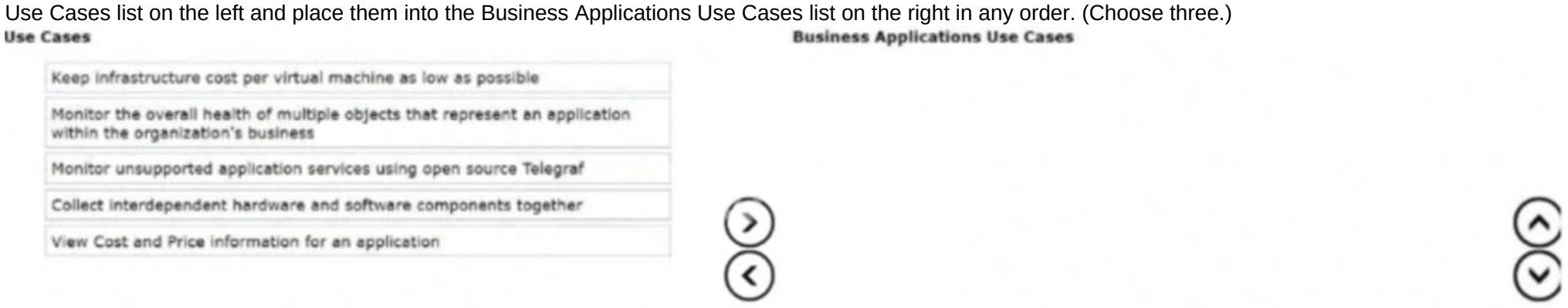
An administrator has been tasked with configuring VCF Operations to set the pricing for Virtual Machines deployed by customers using VCF Automation. The administrator edits the Default Policy and enables the pricing engine. Which three additional steps must the administrator perform to complete this task?(Choose three.)

A. Configure the Provider Pricing settings.
B. Add Recurring Charges for each VM tag.
C. Configure the VC Pricing settings.
D. Add a slab for each of the predefined VM sizes.
E. Set the CPU Rate to vCPU Count Based.
F. Apply a tag to each VM based on their size.

Answer: ADE

Explanation:
The requirement is provider-side pricing for VMs consumed throughVCF Automation Organizations, with charging based on assigned vCPU count and different rates by VM size. In VCF Operations, this maps toProvider Pricing, not vCenter pricing or tag-based additional charges. The official workflow states that Provider Pricing is configured fromInfrastructure Operations>Configurations>Policy Definition>Edit Policy>Provider Pricing, where the administrator activates the pricing engine and configures Region Quota settings . For CPU charging, the Compute Rate section provides the optionCPU GHz Based / vCPU Count Based, and the administrator must selectvCPU Count Basedbecause the business rule is based on assigned vCPUs, not GHz consumption . The same section supportsBase Rate Slabs, which allow different base rates depending on the number of CPUs used; each slab uses a ??greater than or equal?? threshold and a base rate . Therefore, slabs should be created for Small, Medium, and Large VM ranges. Tags and recurring tag charges are unnecessary because VM size is determined directly from vCPU count. Reference topic:Objective 4.4 – Cost Management in VCF Operations / Provider Pricing / Rate Cards / Chargeback.

NEW QUESTION 29
An administrator has been tasked with explaining the benefits of Business Applications within VCF Operations. Drag and drop the three correct use cases from the Use Cases list on the left and place them into the Business Applications Use Cases list on the right in any order. (Choose three.)



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Business Applications in VCF Operations are application-centric container objects used to model and monitor the services that support the business. The documentation defines a Business Application as a set of interconnected applications, services, and hosts configured to offer a service to the organization, and also as a collection of interdependent hardware and software components that deliver a specific business capability . Therefore, monitoring the overall health of multiple objects that represent an application and collecting interdependent components together are direct use cases. The Business Applications page displays health in a sortable table, with the application health determined by the aggregated health of underlying objects . VCF Operations also states that after adding a Business Application, administrators can track object health and optimize capacity, cost, and run What-If Analysis on Business Applications . Cost and price analysis also supports container objects such as Business Apps and Custom Groups . Keeping VM cost as low as possible is a general FinOps goal, and unsupported service monitoring with open source Telegraf is an application-monitoring function, not a Business Application use case. Reference topic:Objective 4.7 – Monitor Applications with VCF Operations / Business Applications / Application Health, Cost, and Capacity.

NEW QUESTION 34
An administrator has been tasked with assigning a policy to a group of VMs. The group should update automatically when the application owner adds or deletes VMs. The VMs do not use the same naming convention and are deployed on different subnets. What three actions must the administrator take?(Choose three.)

A. Add all VMs to the same subnet
B. Select tag as the criteria for group membership
C. Add each VM as an object to the custom group
D. Add the same tag to the selected virtual machines
E. Create a custom group
F. Add virtual machines to a dedicated folder

Answer: BDE

Explanation:
The administrator should create acustom group, assign a commontagto the target VMs, and define the group membership criteria based on that tag. This satisfies the requirement for automatic updates because the group must be dynamic rather than manually maintained. VCF Operations supports custom object groups with either manual or dynamic membership. For dynamic groups, VCF Operations discovers objects that match the defined rules and keeps membership current as objects are added, removed, or changed . The custom group workspace allows the administrator to define membership criteria using object type, metrics, relationships, properties, object name, ortag. The documentation specifically identifies tag-based membership criteria as a supported method for creating dynamic custom groups . Because the VMs do not share a naming convention and are on different subnets, object name and network criteria are unsuitable. Adding each VM manually would create a static group, which would not automatically update when the application owner adds or removes VMs. Reference topic:Objective 4.5 – Managing VCF Operations with VCF Policy / Custom Groups / Dynamic Membership / Policy Assignment.

NEW QUESTION 36
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 37
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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