Number: 2V0-11.24
Passing Score: 800
Time Limit: 120
File Version: 4.0

Exam Code: 2V0-11.24

Exam Name: VMware Cloud Foundation 5.2 Administrator

Exam A

QUESTION 1
An administrator has a requirement to share the contents of a Content Library across multiple vCenter instances.
What steps should the administrator perform to meet this requirement?

A. Create a Subscribed content library on a single vCenter instance and perform a synchronization
B. Create a Subscribed content library on each vCenter instance and enable publishing
C. Create a Local content library on each vCenter instance and perform a synchronization
D. Create a Local content library on a single vCenter instance and enable publishing

Correct Answer: D
Section:
Explanation:
To share the contents of a Content Library across multiple vCenter instances, you need to create a Local content library on one vCenter instance and enable publishing. This allows the library to be accessible by other vCenter instances, where they can subscribe to it, ensuring the content is shared.

QUESTION 2
When commissioning new hosts in VMware Cloud Foundation, which three parameters must be provided? (Choose three.)

A. Network Pool Name
B. Storage Type
C. Hardware Type
D. SSO Domain Name
E. ESXi Version
F. Username

Correct Answer: B, D, F
Section:
Explanation:
Storage Type: The storage type needs to be specified during the commissioning of new hosts in VMware Cloud Foundation, as it is important for the configuration of storage resources for the hosts.
SSO Domain Name: The Single Sign-On (SSO) domain is an essential parameter to associate the hosts with the existing authentication domain.
Username: The administrator needs to provide a username with appropriate permissions to configure the hosts during the commissioning process.

QUESTION 3
What are three prerequisites for deploying an NSX Edge cluster in a VMware Cloud Foundation solution? (Choose three.)

A. Verify that the NSX host overlay VLAN and NSX Edge overlay VLAN are routed to each other.
B. Set up vSAN storage policies for the Edge VMs.
C. Create DNS entries for the NSX Edge nodes.
D. Install Aria Operations and enable Edge Cluster monitoring.
E. Assign separate VLAN IDs and subnets for the NSX host overlay and NSX Edge overlay networks.

Correct Answer: A, C, E

Section:
Explanation:
The NSX host overlay VLAN and NSX Edge overlay VLAN need to be routed to each other to ensure proper communication between the host and NSX Edge clusters.
DNS entries for the NSX Edge nodes are required to enable name resolution, which is important for the proper functioning of the NSX Edge cluster.
Assigning separate VLAN IDs and subnets for the NSX host overlay and NSX Edge overlay networks is necessary to maintain network isolation and optimize traffic flow between components.

QUESTION 4
Which two SDDC Manager operations can be executed on an NSX Edge cluster after it has been deployed? (Choose two.)

A. Redeploy
B. |Sync
C. Expand
D. Delete
E. Shrink

Correct Answer: B, D
Section:
Explanation:
After an NSX Edge cluster has been deployed, you can perform a sync operation to ensure the NSX Edge cluster is in sync with the configuration in SDDC Manager.
Deleting an NSX Edge cluster can be done after it has been deployed if it is no longer required or needs to be removed from the environment.

QUESTION 5
While deploying a new VMware Cloud Foundation environment, a cloud administrator validates the information entered into the Deployment Parameter Workbook. The validation action results in an error and the VMware Cloud Builder GUI error message does not identify the cause.
Which logfile can the administrator use to identify the cause of the validation error?

A. VMware SDDC Manager appliance - vcf-deployment-debug.log
B. VMware Cloud Builder appliance - vcf-bringup-debug.log
C. VMware SDDC Manager appliance - vcf-bringup-debug.log
D. VMware Cloud Builder appliance - vcf-deployment-debug.log

Correct Answer: D
Section:
Explanation:
The vcf-deployment-debug.log file on the VMware Cloud Builder appliance contains detailed logs related to the deployment process, including any validation errors. This log will help identify the cause of the error during the deployment validation phase.

QUESTION 6
An organization is integrating VMware vCenter with Active Directory (AD) to streamline user authentication. As part of this process, the administrator needs to add AD as an identity source in vCenter.
Which three steps must be performed to successfully add AD as an identity source? (Choose three.)

A. Enter the Domain Name and the credentials of an AD user with domain join privileges
B. Configure DNS settings on all ESXi hosts to point to the AD DNS servers.
C. Select 'Add Identity Source' and choose 'Active Directory (Integrated Windows Authentication)'.
D. Reboot the vCenter Server to apply the identity source settings.
E. Navigate to the vCenter Single Sign-On configuration in the vSphere Client.

Correct Answer: A, C, E
Section:
Explanation:
When adding AD as an identity source, you need to enter the Domain Name and provide the credentials of an AD user with domain join privileges to authenticate and add the domain.
In the vSphere Client, you need to select 'Add Identity Source' and choose the appropriate method for AD integration, which is typically 'Active Directory (Integrated Windows Authentication)'.
The process to add AD as an identity source is performed under the vCenter Single Sign-On (SSO) configuration in the vSphere Client.

QUESTION 7
A newly added ESXi host is not able to communicate with the vCenter Server.
What three steps should an administrator take to diagnose and resolve this issue? (Choose three.)

A. Verify the network configuration on the ESXi host
B. Check the license on the ESXi host
C. Use the vSphere Client to review the host's network settings
D. Ensure that the management network is correctly configured and reachable
E. Restart the manaqement aqents on the ESXi host

Correct Answer: A, D, E
Section:
Explanation:
Verifying the network configuration on the ESXi host ensures that the host is correctly configured for network communication with the vCenter Server.
The management network must be properly configured and reachable from the ESXi host to communicate with the vCenter Server.
Restarting the management agents on the ESXi host can resolve issues related to communication between the ESXi host and vCenter Server, as sometimes the agents might become unresponsive.

QUESTION 8
Which feature of VMware Lifecycle Manager allows an administrator to manage the lifecycle of ESXi hosts by applying a consistent image across the hosts in a cluster?

A. Host Profiles
B. Lifecycle Manager Images
C. Update Manager Baselines
D. vSphere Auto Deploy

Correct Answer: B
Section:
Explanation:
VMware Lifecycle Manager (vLCM) enables administrators to manage the lifecycle of ESXi hosts by applying a consistent image across the hosts in a cluster. These images include the ESXi version, firmware, drivers, and settings, ensuring consistency and simplifying updates and patches across all hosts in a cluster.

QUESTION 9
After deploying the VMware Cloud Foundation management domain, an administrator needs to configure backup for the components within the domain.
Which two steps are involved in configuring the backup of VMware Cloud Foundation management components? (Choose two.)

A. Configure an external SFTP backup repository on the SDDC Manager.
B. Manually export the NSX configuration to the SDDC Manager.
C. Enable the vCenter Server snapshot manager on the SDDC Manager.
D. Install a third-party backup solution on each ESXi host.
E. Create a backup schedule on the SDDC manager to automate taking regular backups.

Correct Answer: A, E
Section:
Explanation:
To configure backups for the VMware Cloud Foundation management components, you must set up an external SFTP backup repository within the SDDC Manager. This repository will store the backup files for management components like vCenter, NSX Manager, and SDDC Manager itself.
Creating a backup schedule within the SDDC Manager ensures that regular, automated backups are taken, helping to maintain data integrity and recovery options for the management domain.

QUESTION 10
A cloud administrator recently deployed a new VI workload domain. As part of the initial VI domain creation, the administrator created a new SSO domain. However, they reconsidered and now want the domain to use the same SSO domain as the management domain.
How can the VI domain be changed from a dedicated SSO domain to sharing the SSO domain with the management domain?

A. From the SDDC Manager console, use the rsautil command to add the VI workload domain to the management domain SSO ring.
B. The vSphere SSO domain cannot be changed once it has been deployed and a new VI workload domain that is part of the Management SSO domain must be created, and workloads migrated.
C. From the VI Workload Domain vCenter Server instance, use the rsautil command to join the management domain SSO ring.
D. From the Management Domain vCenter Server instance, use the rsautil command to add the VI workload domain to the management domain SSO ring.

Correct Answer: B
Section:
Explanation:
Once the vSphere Single Sign-On (SSO) domain is set up for a workload domain, it cannot be changed. If you need the VI workload domain to use the same SSO domain as the management domain, you must create a new VI workload domain that is part of the management domain's SSO ring, and then migrate the workloads to the new domain.

QUESTION 11
Which command verifies the successful installation of the Tanzu CLI tools on a developer workstation?

A. vsphere -v
B. tanzu version
C. vicli version
D. vcli --check

Correct Answer: B
Section:
Explanation:
To verify the successful installation of the Tanzu CLI tools, you can use the tanzu version command. This command displays the version of the Tanzu CLI, confirming that the tools are properly installed on the developer workstation.

QUESTION 12
An administrator has deployed a new VMware Cloud Builder appliance using the downloaded OVF file. While attempting to use the VMware Cloud Builder interface, the administrator discovers that no connection can be established to the appliance.
Which three configuration errors may have occurred? (Choose three.)

A. VLAN misconfiguration.
B. Incorrect DNS settings or inaccessible DNS servers.
C. Incorrect NTP settings or inaccessible NTP servers.
D. Incorrect Static IP configuration.
E. BGP routing misconfiguration.

F. Incorrect Dynamic IP configuration.

Correct Answer: A, B, D
Section:
Explanation:
A VLAN misconfiguration could prevent proper network connectivity, particularly if the appliance is not in the correct VLAN or if there is a misalignment in network segmentation.
Incorrect DNS settings or inaccessible DNS servers can prevent the VMware Cloud Builder appliance from being able to resolve hostnames, leading to connection issues.
Incorrect Static IP configuration would result in the appliance being unreachable because it won't have the correct IP address or network configuration to communicate with other components.

QUESTION 13
An administrator has been tasked with expanding an existing VMware Cloud Foundation environment by adding a new workload domain. The environment currently has one management domain and one VI workload domain.
What options are available to the administrator for deploying NSX in the second VI workload domain?

A. The new workload domain can have its own dedicated NSX Fabric or it can join the existing NSX Fabric configured in the existing VI domain.
B. The new workload domain can have a dedicated NSX Fabric or it can join the existing NSX Fabric configured in either the management domain or existing VI domain.
C. The new workload domain can have its own dedicated NSX Fabric or it can join the existing NSX Fabric configured in the management domain.
D. The new workload domain must have a dedicated NSX Fabric.

Correct Answer: B
Section:
Explanation:
When expanding a VMware Cloud Foundation environment with a new workload domain, you have the flexibility to either configure a dedicated NSX Fabric for the new domain or join an existing NSX Fabric from either the management domain or a previously established VI workload domain. This allows for consistent and scalable network virtualization across multiple domains in the environment.

QUESTION 14
An administrator is troubleshooting a high CPU usage issue in a VMware Cloud Foundation environment running IaaS Control Plane. Several namespaces are reporting degraded performance.
What two steps should the administrator take to diagnose and potentially resolve the issue? (Choose two.)

A. Reboot the supervisor cluster to clear any temporary issues.
B. Reconfigure the DRS settings to be more aggressive in load balancing.
C. Review the CPU usage of the ESXi hosts to identify any that are overcommitted.
D. Upgrade the vSphere version to the latest release.
E. Check the resource limits and reservations set on the Kubernetes namespaces.

Correct Answer: C, E
Section:
Explanation:
The administrator should review the CPU usage of the ESXi hosts to identify if any hosts are overcommitted. Overcommitted hosts can lead to performance degradation across workloads.
Checking the resource limits and reservations on Kubernetes namespaces is crucial. If the resource limits are too low or improperly configured, it could cause degraded performance for workloads running in those namespaces.

QUESTION 15
Which feature of VMware Data Services Manager enhances database security and compliance?

A. Automated workload migration
B. Database-Level Authentication
C. Network traffic optimization

D. Storage replication

Correct Answer: B
Section:
Explanation:
VMware Data Services Manager enhances database security and compliance by providing Database-Level Authentication, which ensures that access to databases is tightly controlled and that only authorized users can access sensitive database information. This is critical for maintaining security and compliance with industry standards and regulations.

QUESTION 16
An administrator successfully removed a host from a VMware vSphere cluster and decommissioned it in SDDC Manager.
What must be done before the host can be recommissioned and added back to the SDDC Manager inventory?

A. Loq in to the host console and select 'Reset System Configuration' from the ESXi DCUI.
B. Manually uninstall the NSX VIBs on the host.
C. From the host console, use the /sbin/qenerate-certifcates command to qenerate a new self-siqned certificate.
D. Reinstall ESXi on the host.

Correct Answer: A
Section:
Explanation:
Before the host can be recommissioned and added back to the SDDC Manager inventory, you must reset the system configuration. This can be done from the ESXi Direct Console User Interface (DCUI) by selecting the 'Reset System Configuration' option. This will remove any previous configuration and allow the host to be re-added to the environment.

QUESTION 17
An administrator needs to perform lifecycle management for their VMware Cloud Foundation components, including upgrading the SDDC Manager.
Which three steps should be followed to successfully upgrade VMware Cloud Foundation? (Choose three.)

A. Backup all VMware Cloud Foundation components before starting the upgrade.
B. Disable DRS and HA on all clusters before initiating the upgrade.
C. Manually download the update bundles with a secure browser from the VMware website.
D. Perform a pre-check to ensure that all components are compatible with the new version.
E. Use the SDDC Manager Ul to initiate the upgrade process.

Correct Answer: A, D, E
Section:
Explanation:
Backing up all VMware Cloud Foundation components ensures that data is protected in case the upgrade process encounters issues.
Performing a pre-check is important to verify that all components are compatible with the new version to avoid compatibility issues during the upgrade process.
The SDDC Manager UI is used to initiate the upgrade process, providing a guided and consistent method for upgrading the VMware Cloud Foundation environment.

QUESTION 18
While preparing to enable Application Virtual Networks (AVNs) and deploying Aria Suite components, an administrator plans to deploy an NSX Edge cluster.
What is a requirement for deploying the NSX Edge cluster?

A. The Edge transport nodes must be configured with an MTU of 1500.
B. The Edge cluster must be deployed in the management domain.
C. The Edge transport nodes must be deployed using the 'large' form factor.
D. The Edge cluster must be configured for NSX Federation.

Correct Answer: B
Section:
Explanation:
When deploying an NSX Edge cluster in a VMware Cloud Foundation (VCF) environment, it must be deployed in the management domain. The management domain is responsible for managing and orchestrating various resources, including the NSX Edge cluster, which is crucial for network virtualization and security within the environment.

QUESTION 19
An administrator is tasked with performing password rotation for VMware Cloud Foundation components managed by SDDC Manager.
Which action must be taken to complete this task?

A. Use the Async Patch CLI Tool to rotate passwords for all components.
B. Schedule a maintenance window to rotate the passwords to minimize disruption.
C. Manually update the passwords in vCenter Server and NSX Manager.
D. Access the SDDC Manager UI and navigate to the password management section.

Correct Answer: D
Section:
Explanation:
Password rotation for VMware Cloud Foundation components is managed via the SDDC Manager UI. In the password management section of the SDDC Manager, administrators can rotate the passwords for various components like vCenter Server, NSX Manager, and other management components.

QUESTION 20
An administrator is tasked with deploying a new application that requires both virtual machines and containers.
Which two components of VMware Cloud Foundation would be utilized to provide a unified platform for managing these workloads? (Choose two.)

A. Aria Operations
B. IaaS Control Plane
C. HCX
D. NSX
E. Aria Suite Lifecycle

Correct Answer: A, D
Section:
Explanation:
Aria Operations: Aria Operations (formerly vRealize Operations) provides a unified platform for managing both virtual machines (VMs) and containers, offering monitoring, analytics, and performance management for the entire environment.
NSX: NSX provides network virtualization and security, which can be used to manage network traffic for both VMs and containers, offering a consistent networking model for both workloads.

QUESTION 21
An organization is planning to manage a diverse set of databases across multiple VMware Cloud Foundation environments.
Which three capabilities of Data Services Manager would help in managing these databases efficiently? (Choose three.)

A. Centralized monitoring and alerting for all managed databases.
B. Policy-based backup and recovery for databases.
C. Automated VM migration between on-premises and cloud environments.
D. Automated database provisioning and deployment.
E. Integration with vSAN for optimized storage management

Correct Answer: A, B, D
Section:
Explanation:
Centralized monitoring and alerting for all managed databases: Data Services Manager enables centralized monitoring and alerting for databases across multiple environments, providing visibility and proactive management.
Policy-based backup and recovery for databases: Data Services Manager allows for the implementation of backup and recovery policies to ensure the safety and availability of databases.
Automated database provisioning and deployment: With Data Services Manager, administrators can automate the deployment and provisioning of databases, streamlining the management process.

QUESTION 22
An administrator is responsible for monitoring the logs of multiple vSphere components using VMware Aria Operations for Logs. They notice an increase in error logs for a specific ESXi host.
Which two steps should be taken to pinpoint the issue? (Choose two.)

A. Restart the ESXi host to resolve the issue immediately
B. Filter the loos by the ESXi host name and error severity.
C. Correlate the error logs with recent configuration changes on the ESXi host.
D. Check for patterns or repeated error messages over a specific time frame.
E. Delete all old logs to free up space and generate new logs.

Correct Answer: B, D
Section:
Explanation:
Filtering the logs by the ESXi host name and error severity helps narrow down the logs to those relevant to the specific host and allows for easier identification of significant errors.
Checking for patterns or repeated error messages over a specific time frame helps identify the root cause of the issue and determine if the errors are linked to a specific event or condition.

QUESTION 23
An administrator needs to deploy a Kubernetes cluster on a vSphere IaaS control plane (formerly vSphere with Tanzu) to host a new application.
Which three steps should be followed to successfully deploy the Kubernetes cluster? (Choose three.)

A. Configure a Load Balancer for the Kubernetes control plane nodes.
B. Create a new VM template for the Kubernetes nodes.
C. Configure a vSphere Namespace and assign resource quotas.
D. Enable Workload Management on the vSphere Cluster.
E. , Deploy a vSphere Pod Service.

Correct Answer: A, C, D
Section:
Explanation:
A Load Balancer is needed for the Kubernetes control plane nodes to distribute traffic across the control plane and ensure high availability for the Kubernetes management layer.
A vSphere Namespace must be configured to define a logical boundary for Kubernetes workloads, and resource quotas help ensure that resources are allocated appropriately for the workloads.
Enabling Workload Management on the vSphere Cluster is necessary to integrate Kubernetes with vSphere and manage the lifecycle of Kubernetes clusters using vSphere with Tanzu.

QUESTION 24
Which is the appropriate first action to take to resolve dropped network packets on an ESXi host?

A. Check physical network switch configuration
B. Enable Storage I/O Control
C. Increase the CPU and memory allocation for VMs
D. Migrate VMs to another data store

Correct Answer: A
Section:
Explanation:
Dropped network packets are often caused by misconfigurations or issues at the physical network layer. Checking the physical network switch configuration is the first step to ensure that the network settings, such as VLANs, uplinks, and port configurations, are correctly set up. This ensures proper connectivity and traffic flow for the ESXi host and the VMs.

QUESTION 25
An administrator needs to ensure that their VMware Cloud Foundation-based private cloud solution can support multi-tenancy for different departments within their organization.
What two configurations and components are necessary to achieve this? (Choose two.)

A. Configure vSAN storage policies for each department.
B. Use vSphere Resource Pools to allocate resources to different departments.
C. Deploy Aria Automation to enable self-service provisioning for tenants.
D. Use NSX to create isolated network segments for each tenant.

Correct Answer: B, D
Section:
Explanation:
vSphere Resource Pools allow for the allocation of CPU, memory, and storage resources to different departments (tenants) within the VMware Cloud Foundation environment. This ensures that each department has its own dedicated resources, preventing resource contention between them.
NSX can be used to create isolated network segments (logical networks) for each tenant, ensuring network security and segmentation between departments. Each department can have its own isolated network environment.

QUESTION 26
What is the primary benefit of using VMware vCenter Content Libraries?

A. They enable centralized management and distribution of VM templates, ISO images, and scripts.
B. They facilitate the creation of virtual networks.
C. They allow for the automation of VM snapshots.
D. They provide enhanced security for vCenter Server.

Correct Answer: A
Section:
Explanation:
VMware vCenter Content Libraries provide a centralized location for storing and managing virtual machine templates, ISO images, and scripts, making it easier to distribute these resources across multiple vCenter instances. This helps streamline the deployment process, ensuring consistency and reducing the overhead of managing these resources manually.

QUESTION 27
A disk failure has occurred in a vSAN cluster.
What four steps should be taken to recover from this disk failure? (Choose four.)

A. Use the vSohere Client to check the vSAN Health Service
B. Disable disk group encryption
C. Rebuild the affected disk group
D. Perform a full resync of the vSAN objects
E. Replace the failed disk with a new one
F. Ensure the new disk is claimed by the vSAN cluster

Correct Answer: A, C, E, F
Section:
Explanation:
Checking the vSAN Health Service in the vSphere Client is the first step in diagnosing the issue and verifying the status of the vSAN components after the disk failure.
Rebuilding the affected disk group is necessary to ensure that data is re-optimized and replicated in accordance with the vSAN policy.
Replacing the failed disk with a new one ensures that the storage capacity is restored.
Ensuring that the new disk is claimed by the vSAN cluster is important to ensure that it is recognized and integrated into the vSAN disk group.

QUESTION 28
Which tool is most appropriate for analyzing detailed network performance metrics in a vSphere environment?

A. vSphere CLI
B. vSphere Client
C. vSAN Health Service
D. Aria Operations

Correct Answer: D
Section:
Explanation:
Aria Operations (formerly vRealize Operations) is the most appropriate tool for analyzing detailed network performance metrics in a vSphere environment. It provides comprehensive monitoring, analytics, and performance management, including network performance metrics across the vSphere infrastructure.