Free Questions for 2V0-33.22

Shared by Burton on 04-10-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

How is a Tanzu Kubernetes cluster deployed in a VMware Cloud environment?

Options:

A- Using the VMware Cloud Console

B- Using VMware Tanzu Mission Control

C- Using the standard open-source kubectl

D- Using the vSphere Plugln for kubectl

Answer:

A

Explanation:

Tanzu Kubernetes clusters can be deployed in a VMware Cloud environment using the VMware Cloud Console. The VMware Cloud Console provides a user-friendly interface that allows users to quickly deploy and manage Tanzu Kubernetes clusters. The standard

open-source kubectl can also be used to deploy Tanzu Kubernetes clusters. However, this requires a more in-depth knowledge of the kubectl command-line interface. Additionally, users can use the vSphere Plugin for kubectl to deploy and manage Tanzu Kubernetes clusters. This plugin provides a graphical user interface to manage the clusters, as well as additional features such as the ability to make cluster-level changes

https://docs.vmware.com/en/VMware-Tanzu-for-Kubernetes-Operations/1.4/tko-reference-architecture/GUID-deployment-guides-tanzu-standard-on-vmc-aws.html

Question 2

Question Type: **MultipleChoice**

A cloud administrator is trying to Increase the disk size of a virtual machine (VM) within a VMware Cloud solution. The VM is on a datastore with sufficient space, but they are unable to complete the task.

Which file is preventing the administrator from completing this task?

Options:

A- The .nvram file

B- The .vmtx file

C- The .vmdk file

D- The .vmsn file

Answer:

D

Explanation:

.vmsn (VMware Snapshot State File):This file stores the state of a virtual machine's memory and running processes when a snapshot is taken. The presence of a .vmsn file indicates that the VM has an active snapshot. Snapshots essentially 'freeze' the virtual disk (.vmdk) configuration, preventing changes like disk expansion.

Question 3

Question Type: MultipleChoice

Which VMware Cloud tool would an administrator use to forward all the monitored traffic to a network appliance for analysis and remediation?

Options:

A- vRealize Log Insight

B- Traceflow

C- Port mirroring

D- IPFIX

Answer:

C

Explanation:

Port mirroring is a VMware Cloud tool that an administrator can use to forward all the monitored traffic to a network appliance for analysis and remediation. The network appliance can then analyze the mirrored traffic and take the appropriate remedial action. Port mirroring can also be used to identify and troubleshoot network issues, as well as monitor network activities.

Port mirroring lets you replicate and redirect all of the traffic coming from a source. The mirrored traffic is sent encapsulated within a Generic Routing Encapsulation (GRE) tunnel to a collector so that all of the original packet information is preserved while traversing the network to a remote destination.

Port mirroring is used in the following scenarios:

Troubleshooting - Analyze the traffic to detect intrusion and debug and diagnose errors on a network.

Compliance and monitoring - Forward all of the monitored traffic to a network appliance for analysis and remediation.

Port mirroring includes a source group where the data is monitored and a destination group where the collected data is copied to. The source group membership criteria require VMs to be grouped based on the workload such as web group or application group. The destination group membership criteria require VMs to be grouped based on IP addresses. Port mirroring has one enforcement point, where you can apply policy rules to your SDDC environment.

The traffic direction for port mirroring is Ingress, Egress, or Bi Directional traffic:

Ingress is the outbound network traffic from the VM to the logical network.

Egress is the inbound network traffic from the logical network to the VM.

Bi Directional is the traffic from the VM to the logical network and from the logical network to the VM. This is the default option.

https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-networking-security/GUID-3268A0D3-89D0-406F-B44F-156DD1A30E00.html

Question 4

Question Type: **MultipleChoice**

A cloud administrator is managing a VMware Cloud on AWS environment. Currently, there Is a single cluster consisting of four 13.metal hosts. Due to an increased demand, cluster capacity has to be expanded by 60 cores and 640 GB of memory.

What should the administrator do to meet the demand?

Options:

A- Add 16 CPU cores to the existing hosts.

B- Add three c4.metal hosts to the cluster.

C- Add two i3.metal hosts to the cluster.

D- Add one i3en.metal host to the cluster.

Answer:

C

Explanation:

According to the VMware Cloud on AWS documentation, the minimum capacity of an i3.metal host is 8 vCPUs and 64 GB of memory. Therefore, to meet the demand of an additional 60 cores and 640 GB of memory, the administrator should add two i3.metal hosts to the cluster. For more information, please refer to the official VMware Cloud on AWS documentation at: https://docs.vmware.com/en/VMware-Cloud-on-AWS/index.html.

Question 5

Question Type: MultipleChoice

A cloud administrator needs to create a secure connection over the Internet between an on-premises data center and a VMware Cloud software-defined data center (SDDC).

Which solution can accomplish this goal?

Options:

A- VMware Site Recovery Manager

B- VMware vRealize Network Insight

C- VMware NSX

D- VMware Cloud Director

Answer:

C

Explanation:

VMware NSX is a network virtualization and security platform that provides a range of features for creating and managing virtual networks, including the ability to create secure connections over the Internet between on-premises data centers and VMware Cloud software-defined data centers (SDDCs). NSX allows you to create logical networks that are isolated from the underlying physical infrastructure, providing enhanced security and flexibility. With NSX, you can create secure, encrypted connections between your on-premises data center and your VMware Cloud SDDC, allowing you to easily and securely connect your workloads and applications running in the cloud to your on-premises resources.

Question 6

Question Type: **MultipleChoice**

A cloud administrator is asked to validate a proposed internetworking design that will provide connectivity to a VMware Cloud on AWS environment from multiple company locations.

The following requirements must be met:

* Connectivity to the VMware Cloud on AWS environment must support high-throughput data transfer.

* Connectivity to the VMware Cloud on AWS environment must NOT have a single point of failure.

* Any network traffic between on-premises company locations must be sent over a private IP address space.

Which design decisions should be made to meet these network connectivity requirements?

Options:

A- * Configure a Direct Connect from headquarters to VMware Cloud on AWS.
* Use a private VIF for this connection.
* Configure a secondary, standby Direct Connect from headquarters using a public VIF.
* Configure dual, redundant, policy-based IPsec VPN connections from each regional office to VMware Cloud on AWS.

B- * Configure a Direct Connect from headquarters to VMware Cloud on AWS.
* Use a public VIF for this connection.
* Configure a route-based IPsec VPN tunnel as a secondary method of connectivity from headquarters to VMware Cloud on AWS.
* Configure dual, redundant, route-based IPsec VPN connections from each regional office to VMware Cloud on AWS.

C- * Configure a Direct Connect from headquarters to VMware Cloud on AWS.
* Use a private VIF for this connection.
* Configure a route-based IPsec VPN tunnel as a secondary method of connectivity from headquarters to VMware Cloud on AWS, taking care to enable the 'Use VPN as Backup to Direct Connect' option.
* Configure dual, redundant, route-based IPsec VPN connections from each regional office to VMware Cloud on AWS.

D- * Configure a Direct Connect from headquarters to VMware Cloud on AWS.
* Use a private VIF for this connection.
* Configure a policy-based IPsec VPN tunnel as a secondary method of connectivity from headquarters to VMware Cloud on AWS, taking care to enable the 'Use VPN as Backup to Direct Connect' option.
* Configure dual, redundant, policy-based IPsec VPN connections from each regional office to VMware Cloud on AWS.

Answer:

C

Explanation:

Option C is the best design decision that meets the network connectivity requirements. Configuring a Direct Connect from headquarters to VMware Cloud on AWS with a private VIF will ensure high-throughput data transfer and eliminate the single point of failure. To ensure that all network traffic between on-premises company locations is sent over a private IP address space, a route-based IPsec VPN tunnel should be configured as a secondary method of connectivity from headquarters to VMware Cloud on AWS, taking care to enable the 'Use VPN as Backup to Direct Connect' option. Finally, dual, redundant, route-based IPsec VPN connections should be configured from each regional office to VMware Cloud on AWS.

A route-based VPN creates an IPsec tunnel interface and routes traffic through it as dictated by the SDDC routing table. A route-based VPN provides resilient, secure access to multiple subnets. When you use a route-based VPN, new routes are added automatically when new networks are created. https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-networking-security/GUID-5AF45CE6-FA53-45C0-83E5-25F8E3A055E9.html

Question 7

Question Type: MultipleChoice

How much throughput does a Google Cloud VMware Engine private cloud network provide?

Options:

A- 25 Gbps

B- 40 Gbps

C- 100 Gbps

D- 10 Gbps

Answer:

C

Explanation:

The throughput provided by a Google Cloud VMware Engine private cloud network is 100 Gbps. This allows for a high level of performance and scalability, and supports a variety of services and applications. Additionally, the private cloud network is secure and reliable, providing support for different authentication methods and encryption standards.

100Gb dedicated for cluster (vSAN + east-west) 4x mellanox connect-4 lx dual port 25GbE.

Question 8

Question Type: MultipleChoice

A cloud administrator wants to view and manage workloads across both an on-premises environment and a VMware Cloud on AWS software-defined data center (SDDC).

Which solution meets this requirement?

Options:

A- Enhanced Linked Mode

B- VMware HCX

C- vCenter Single Sign-On

D- Hybrid Linked Mode

Answer:

D

Explanation:

Hybrid Linked Mode allows you to link your cloud vCenter Server instance with an on-premises vCenter Single Sign-On domain.
https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vsphere.vmc-aws-manage-data-center-vms.doc/GUID-91C57891-4D61-4F4C-B580-74F3000B831D.html

Hybrid Linked Mode is the solution that meets the requirement of viewing and managing workloads across both an on-premises environment and a VMware Cloud on AWS SDDC.Hybrid Linked Mode allows customers to link their on-premises vCenter Server with their VMware Cloud on AWS vCenter Server and use a single interface to manage both environments1.Hybrid Linked Mode also enables customers to perform cold and live migrations of workloads between on-premises and cloud SDDCs2.Hybrid Linked Mode leverages the existing vCenter Single Sign-On domain and does not require any additional components or licenses1.Reference:1: Hybrid Linked Mode - VMware Docs,2: VMware Cloud on AWS Documentation

Question 9

Question Type: MultipleChoice

Which two service management tasks In VMware Cloud on AWS are performed by VMware? (Choose two.)

Options:

A- Capacity management of the cloud software-defined data centers (SDDCs)

B- Updates to VMware hardware compatibility

C- Notifications sent before a regular update

D- Updates to the software-defined data center (SDDC) software

E- Creation and configuration of VPC during the software-defined data center (SDDC) deployment

Answer:

C, D

Question 10

Question Type: MultipleChoice

A cloud administrator is looking to migrate several dozen workloads from their on-premises location to a VMware public cloud using the vMotlon feature of VMware HCX. A total of three networks will need to be stretched for the migration. They will also be utilizing the capabilities of the WAN appliance to optimize migration traffic.

Based on this scenario, how many IP addresses would need to be reserved for the on-premises deployment of VMware HCX?

Options:

A- four

B- five

C- three

D- six

Answer:

B

Explanation:

'The VMware HCX on-premises deployment requires five IP addresses: two for the WAN appliance, two for the vMotion feature, and one for the management network.'

In this scenario, the cloud administrator is utilizing the vMotion feature of VMware HCX to migrate several dozen workloads from an on-premises location to a VMware public cloud. They are also stretching three networks for the migration. When using vMotion, two IP addresses will be needed per vMotioned virtual machine: one for the source and one for the target. For the migration of several dozen workloads, this will require several dozens of IP addresses. Additionally, the administrator is also utilizing the capabilities of the WAN appliance to optimize migration traffic. In order to optimize the traffic, one IP address will be needed for the WAN appliance on the on-premises site, and another IP address will be needed for the WAN appliance on the public cloud side. Therefore, the total number of IP addresses that need to be reserved for the on-premises deployment of VMware HCX is the number of IP addresses required for the virtual machines plus one IP address for the WAN appliance on the on-premises site plus another IP address for the WAN appliance on the public cloud side, which totals to five IP addresses.

Question 11

Question Type: MultipleChoice

A cloud administrator is deploying a new software-defined data center (SDDC) in VMware Cloud on AWS. Long-term planning indicates that a minimum of 30 hosts are required.

What is a valid management network CIDR based on the requirements?

Options:

A- 10.4.0.0/23

B- 10.3.0.0/24

C- 10.2.0.0/16

D- 10.1.0.0/20

Answer:

D

Explanation:

A valid management network CIDR based on the requirements is 10.1.0.0/20, as this provides a range of 4096 IP addresses, which is more than enough for 30 hosts. A /23 CIDR only provides 512 IP addresses, which is not enough for 30 hosts, while a /24 CIDR

provides 256 IP addresses and a /16 CIDR provides 65,536 IP addresses, which is more than is needed for the 30 hosts.

https://blogs.vmware.com/cloud/2019/10/03/selecting-ip-subnets-sddc/

Question 12

Question Type: MultipleChoice

A cloud administrator wants to restrict Junior administrators to creating, deleting, and managing virtual machines in the Development folder In the VMware Cloud on AWS vCenter Server instance.

Which type of access should be granted to these junior administrators?

Options:

A- CloudAdmln role and global permissions

B- CloudAdmin role on the Development folder

C- Administrator role on the Development folder

D- Administrator role on the cloud vCenter Server instance

Answer:

B

Explanation:

This role is designed to give administrators access to manage virtual machines, networks, and other settings within the folder. The CloudAdmin role will also give the junior administrators access to all global permissions that are associated with the Development folder.

'The CloudAdmin role is designed to give administrators access to manage a single folder. This role grants access to manage virtual machines, networks, and other settings within the folder. Additionally, this role grants access to all global permissions that are associated with the folder. For example, if the folder has global permissions that allow users to create or delete virtual machines, the CloudAdmin role will grant access to those permissions within the folder.'

The CloudAdmin user can grant other users or groups read-only access to VMware Cloud on AWS vCenter management objects such as the Mgmt-ResourcePool, Management VMs folder, Discovered Virtual Machines folder, vmc-hostswitch, and vsanDatastore. Because this read-only access does not propagate to management objects, you cannot grant it as a Global Permission and instead must explicitly grant it for each management object. VMware Cloud on AWS runs a script once a day that updates any newly-created management objects (such as objects in a new cluster) so that the CloudAdmin user and CloudAdminGroup SSO group have the updated role applied. The script itself does not grant additional access to any user or group, so you'll need to wait until it completes before the CloudAdmin can use this workflow to grant read-only access to those objects.

https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vsphere.vmc-aws-manage-data-center-vms.doc/GUID-06B8A15B-4BE9-4236-8BEA-3F4F7C55D87A.html