



VMware

Exam Questions 2V0-33.22

VMware Cloud Professional

NEW QUESTION 1

When preparing to deploy VMware Cloud on Dell EMC or VMware Cloud on AWS Outposts in a data center, which two networking constraints must be considered? (Choose two.)

- A. Fiber Channel connectivity
- B. Creating a direct connect to the nearest AWS Region
- C. Compatible top of rack switches
- D. Uplinks for local network connectivity
- E. Dedicated subnets for SDDC management network

Answer: CE

Explanation:

Compatible top of rack switches are necessary to ensure that the data center is able to support the VMware Cloud on Dell EMC or VMware Cloud on AWS Outposts deployments [1]. The switches must support 10GE and 25GE ports, as well as Layer 3 routing protocols such as OSPF and BGP. Dedicated subnets for SDDC management network are also needed for the deployment of VMware Cloud on Dell EMC or VMware Cloud on AWS Outposts [1]. The SDDC management network will be used for communication between the VMware Cloud components and the data center, and must be isolated from the customer network.

NEW QUESTION 2

A cloud administrator is in the process of troubleshooting a non-compliant object. How can the administrator change a VM storage policy for an ISO image?

- A. Modify the default VM storage policy and recreate the ISO image.
- B. Modify the default VM storage policy.
- C. Apply a new VM storage policy.
- D. Attach the ISO image to a virtual machine.

Answer: C

Explanation:

A VM storage policy is a set of rules that defines the storage requirements for a virtual machine or an object. A cloud administrator can create and apply different VM storage policies for different types of objects, such as virtual disks, ISO images, snapshots, etc1. Applying a new VM storage policy to an object will change its compliance status and trigger a reconfiguration task to move the object to a compatible datastore1. Modifying the default VM storage policy will affect all the objects that use it, which may not be desirable. Recreating the ISO image is unnecessary and time-consuming. Attaching the ISO image to a virtual machine will not change its storage policy1.

NEW QUESTION 3

A cloud administrator establishes a VPN connection to the VMware Cloud data center but is unable to access the VMware Cloud vCenter. Which step can the administrator take to resolve this?

- A. Modify the default vCenter management network to participate in the on-premises IP space.
- B. Create a segment in the VMware Cloud data center for connection to the vCenter.
- C. Establish a layer 2 connection between the on-premises data center and the VMware Cloud data center.
- D. Create an NSX firewall rule in the VMware Cloud data center allowing access to the vCenter from the on-premises data center.

Answer: D

Explanation:

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-operations/GUID-ED8B8> By default, the management gateway firewall is set to deny all traffic between the internet and vCenter Server. Verify that the appropriate firewall rules are in place. The administrator can create an NSX firewall rule in the VMware Cloud data center that allows access to the vCenter from the on-premises data center. This would allow the VPN connection to connect to the vCenter, allowing the administrator to access and manage the VMware Cloud environment.

NEW QUESTION 4

A customer needs to set up a self-managed VDI solution that can be deployed to any VMware Cloud. Which two VMware solutions can meet this requirement? (Choose two.)

- A. VMware Dynamic Environment Manager (DEM)
- B. VMware ThinApp
- C. VMware Workspace ONE Unified Endpoint Management (UEM)
- D. VMware Horizon
- E. VMware Workspace ONE Access

Answer: DE

Explanation:

The two VMware solutions that can meet the customer's requirement for a self-managed VDI solution are D. VMware Horizon and E. VMware Workspace ONE Access. VMware Horizon is a virtual desktop and application virtualization platform that enables customers to set up and deploy a virtual desktop infrastructure in any cloud environment. VMware Workspace ONE Access provides secure access to applications, data, and devices in any cloud environment.

NEW QUESTION 5

A cloud administrator is tasked with deploying a new software-defined data center (SDDC) in VMware Cloud on AWS and has been able to log into the VMware Cloud console successfully. However, they cannot access the VMware Cloud on AWS Services. Which two tasks need to be performed for the administrator to gain access? (Choose two.)

- A. The cloud administrator will need to create a new subscription for the VMware Cloud on AWS service.

- B. The cloud administrator will need to request access to the VMware Cloud on AWS service
- C. The cloud administrator will need the globalcloudadmin role in the VMware Cloud on AWS service.
- D. The cloud administrator will need the Administrator role in the VMware Cloud on AWS service.
- E. The cloud administrator will need the cloudadmin role in the VMware Cloud on AWS service.

Answer: BD

Explanation:

(Reference:<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vcloud.admin.doc/GUI>) To request access to the VMware Cloud on AWS service, the cloud administrator must log in to the VMware Cloud Console and fill out the New Subscription Request form. Once the form is filled out and submitted, the cloud administrator will receive an email with instructions on how to access the VMware Cloud on AWS service.

The cloud administrator will also need to have the Administrator role in the VMware Cloud on AWS service in order to gain access. The Administrator role allows the cloud administrator to access the VMware Cloud on AWS service, view the services available in the VMware Cloud on AWS console, and manage the resources in the SDDC.

NEW QUESTION 6

What is a benefit of public cloud computing?

- A. Full control over physical data location
- B. Full control over software versions and software lifecycle
- C. Highly customizable and configurable hardware options
- D. Cost savings on capital hardware expenses

Answer: D

Explanation:

One benefit of public cloud computing is cost savings on capital hardware expenses. Since the cloud provider owns and manages the hardware, the customer does not need to invest in the purchase and maintenance of physical hardware, resulting in significant cost savings. Additionally, public cloud services often provide scalability and can be accessed from anywhere with an internet connection.

NEW QUESTION 7

Which two components are required in order to deploy a Tanzu Kubernetes Grid Cluster in VMware Cloud environment? (Choose two)

- A. Tanzu CLI
- B. Supervisor namespace
- C. vSphere VM folder
- D. vSphere resource pool
- E. YAML manifest file

Answer: CD

Explanation:

<https://docs.vmware.com/en/VMware-Tanzu-Kubernetes-Grid/1.6/air-gap-reference-architecture/GUID-deploy>m

NEW QUESTION 8

A cloud administrator is looking to migrate several dozen workloads from their on-premises location to a VMware public cloud using the vMotion 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?

- 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.

NEW QUESTION 9

A cloud administrator would like the VMware Cloud on AWS cluster to automatically scale-out and scale-in based on resource demand. Which two Elastic DRS policies can be configured to meet this requirement? (Choose two.)

- A. Elastic DRS Baseline policy
- B. Optimize for Best Performance policy
- C. Optimize for Lowest Cost policy
- D. Custom Elastic DRS policy
- E. Optimize for Rapid Scale-Out policy

Answer: DE

Explanation:

The two Elastic DRS policies that can be configured to meet the requirement of automatically scaling out and in based on resource demand are the Custom Elastic DRS policy and the Optimize for Rapid Scale-Out policy. The Custom Elastic DRS policy allows you to configure the cluster to scale out when certain resource utilization thresholds are met, while the Optimize for Rapid Scale-Out policy allows you to configure the cluster to scale out when resource utilization is high and scale in when utilization is low.

Elastic DRS is a feature of VMware Cloud on AWS that enables automatic scaling of the cluster based on resource demand. To meet the requirement of automatic scaling, the administrator can configure a custom Elastic DRS policy or the Optimize for Rapid Scale-Out policy. Custom Elastic DRS policy allows administrator to define the custom rules for scale-out and scale-in based on resource utilization thresholds. Optimize for Rapid Scale-Out policy automatically scales-out the cluster when resource utilization threshold is met.

NEW QUESTION 10

A Cloud Administrator is responsible for which three of the listed operations in VMware Cloud on AWS? (Choose three.)

- A. VMware Tools Updates
- B. VMWare NSX Manager Updates
- C. Guest Operating System Updates
- D. Hardware Bios / Firmware Updates
- E. VMware vCenter Server Updates
- F. Network Connectivity

Answer: ACF

Explanation:

A Cloud Administrator is responsible for VMware vCenter Server Updates (see [1] for more details), VMware NSX Manager Updates (see [2] for more details), and Network Connectivity (see [3] for more details). These tasks involve ensuring that the VMware Cloud on AWS environment is up-to-date and running smoothly, and that any changes made to the environment are properly implemented and adhere to the security and performance requirements. Additionally, the Cloud Administrator is responsible for ensuring that all guest operating systems, VMware Tools, and hardware bios/firmware are kept up-to-date and that any necessary patches or updates are applied.

[1]<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.administration/GUID>

NEW QUESTION 10

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?

- A. The .nvram file
- B. The .vmtx file
- C. The .vmdk file
- D. The .vmxn file

Answer: C

Explanation:

The .vmdk file contains the virtual machine's hard disk configuration and is preventing the administrator from increasing the disk size. The .vmdk file must be edited to allow the administrator to increase the disk size. More specifically, the administrator must edit the descriptor file within the .vmdk file to change the capacity of the disk.

NEW QUESTION 15

What is the key difference between configuring Hybrid Linked Mode from the Cloud Gateway Appliance and the VMware vSphere Client?

- A. The on-premises VMware vSphere version must be vSphere 6.5 or later.
- B. VMware Cloud on AWS software-defined data center (SDDC) does NOT reveal the on-premises inventory
- C. Minimal overhead is required in the on-premises data center.
- D. Centralized administration is available through the VMware vSphere Client.

Answer: A

Explanation:

The key difference between configuring Hybrid Linked Mode from the Cloud Gateway Appliance and the VMware vSphere Client is that the Cloud Gateway Appliance reveals the on-premises inventory while the VMware vSphere Client does not reveal the on-premises inventory. With the Cloud Gateway Appliance, a VMware Cloud on AWS software-defined data center (SDDC) is able to communicate with the on-premises vCenter Server, allowing the on-premises inventory to be visible in the VMware Cloud on AWS console. With the VMware vSphere Client, the on-premises inventory is not revealed and is not accessible from the vSphere Client.

NEW QUESTION 18

A cloud administrator is managing a Google Cloud VMware Engine environment with a single cluster consisting of 28 Hosts. The Administrator and, based on estimates from the application team, requires seven additional hosts. What should the administrator do?

- A. Add seven hosts to the existing cluster.
- B. Provision a new private cloud.
- C. Provision a new cluster.
- D. Nothing; the cluster will scale automatically.

Answer: C

Explanation:

<https://cloud.google.com/vmware-engine/docs/concepts-vmware-components> Node Considerations
You can specify the number of hosts to add or remove to or from their cluster. Private cloud initial setup happens in ~30 minutes.
Additional hosts can be added in ~15 minutes.
A three-node cluster is the minimum for production.
You can have up to 32 hosts per cluster.
You can have up to 64 hosts per private cloud.

NEW QUESTION 23

A cloud administrator needs to provide the security team with the ability to query and audit events and provide custom real-time alerts for the VMware NSX firewall running in VMware Cloud on AWS.
Which solution would the administrator use to accomplish this goal?

- A. CloudHealth by VMware
- B. VMware vRealize Log Insight Cloud
- C. VMware vRealize Network Insight Cloud
- D. VMware vRealize Operations Cloud

Answer: B

Explanation:

VMware vRealize Log Insight Cloud is a cloud-based log management and analytics solution that provides real-time visibility and analytics for VMware Cloud on AWS [1]. It allows security teams to query and audit events and set up custom real-time alerts. Additionally, it provides detailed insights into the activity of the VMware NSX firewall, allowing administrators to quickly identify suspicious activity and take action.

NEW QUESTION 28

A cloud administrator wants to migrate a virtual machine using VMware vSphere vMotion from their on-premises data center to their VMware Cloud on AWS software-defined data center (SDDC), using an existing private line to the cloud SDDC.
Which two requirements must be met before the migration can occur? (Choose two.)

- A. The versions of VMware vSphere need to match between the on-premises data center and the cloud SDDC.
- B. A Layer 2 connection is configured between the on-premises data center and the cloud SDDC.
- C. AWS Direct Connect is configured between the on-premises data center and the cloud SDDC.
- D. IPsec VPN is configured between the on-premises data center and the cloud SDDC.
- E. Cluster-level Enhanced vMotion Compatibility (EVC) is configured in the on-premises data center and the cloud SDDC.

Answer: CD

Explanation:

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-operations/GUID-1A175> Requirements for SDDCs With NSX: Networking speed and latency: Migration with vMotion requires sustained minimum bandwidth of 250 Mbps between source and destination vMotion vMkernel interfaces, and a maximum latency of 100 ms round trip between source and destination.
On-premises vSphere version: Your on-premises vSphere installation must be vSphere 6.7U2 or higher. See VMware Knowledge Base article 56991 for more information.
On-premises DVS version: 6.0 or higher. On-premises NSX version: any
Note: SDDCs configured with NSX do not support hot vMotion to or from on-premises VXLAN encapsulated networks (NSX for vSphere) or Geneve Datacenter Overlay networks (NSX).
IPsec VPN: Configure an IPsec VPN for the management gateway.
See Configure a VPN Connection Between Your SDDC and On-Premises Data Center in the VMware Cloud on AWS Networking and Security guide.
Direct Connect: Direct Connect over a private virtual interface between your on-premise data center and your VMware Cloud on AWS SDDC is required for migration with vMotion.
See Using AWS Direct Connect with VMware Cloud on AWS.
Hybrid Linked Mode: Hybrid Linked Mode is required to initiate migration from the vSphere Client. It is not required to initiate migration using the API or PowerCLI. See "Hybrid Linked Mode" in Managing the VMware Cloud on AWS Data Center.
L2 VPN: Configure a Layer 2 VPN to extend virtual machine networks between your on-premises data center and cloud SDDC. Routed networks are not supported. See VMware Cloud on AWS Networking and Security.
VMware Cloud on AWS firewall rules Ensure that you have created the necessary firewall rules as described in Required Firewall Rules for vMotion.
On-premises firewall rules: Ensure that you have created the necessary firewall rules as described in Required Firewall Rules for vMotion.
Virtual machine hardware and settings: Ensure that these requirements are met for virtual machine hardware.

- Virtual machine hardware version 9 or later is required for migration with vMotion from the on-premises data center to the cloud SDDC.
- EVC is not supported in the VMware Cloud on AWS SDDC.
- VMs that are created in the cloud SDDC or that have been power-cycled after migration to the cloud SDDC can't be migrated back to the on-premises data center with vMotion unless the on-premises EVC baseline is Broadwell. You can relocate these VMs after powering them off, as long as their virtual machine hardware version is compatible with the on-premises data center.
- Migration of VMs with DRS or HA VM overrides is not supported. For more information on VM overrides, see Customize an Individual Virtual Machine.

Important: Source switch configurations (including NIOC, spoofguard, distributed firewall, and Switch Security) and runtime state are not applied at the destination as part of migration in either direction. Before you initiate vMotion, apply the source switch configuration to the destination network.
In order for a virtual machine to be migrated using VMware vSphere vMotion, the versions of VMware vSphere need to match between the on-premises data center and the cloud SDDC, and a Layer 2 connection needs to be configured between them. Additionally, cluster-level Enhanced vMotion Compatibility (EVC) must be configured in both the on-premises data center and the cloud SDDC. IPsec VPN and AWS Direct Connect do not need to be configured for the migration to occur.

NEW QUESTION 31

A cloud administrator is developing a new Private cloud in Google VMware Engine and wants to allow for Maximum growth. What are two valid subnet sizes that meets the requirement for the VMware vSphere/vSAN subnet? (Choose two.)

- A. /21
- B. /24
- C. /22

D. /23
E. /20

Answer: AE

Explanation:

<https://cloud.google.com/vmware-engine/docs/concepts-vlans-subnets>

NEW QUESTION 36

A cloud administrator is tasked with creating a new network segment in the software-defined data center that utilizes the corporate DHCP server to provide IP addresses.

What is the proper sequence to create the required network segments?

- A. * 1- Create a new segment attached to the Tier-0 gateway* 2. Configure the segment DHCP ip-helper
- B. * 1. Create a DHCP server profile* 2. Create a new segment attached to the Tier-0 gateway* 3. Configure the segment DHCP config to utilize the new DHCP server profile
- C. * 1. Create a new segment attached to the Tier-1 gateway* 2. Configure the segment DHCP ip-helper
- D. * 1. Create a DHCP relay profile* 2. Create a new segment attached to the Tier-1 gateway* 3. Configure the segment DHCP config to utilize the new DHCP relay profile

Answer: B

Explanation:

<https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/administration/GUID-BF536EEF-7AC3-47D0-B> According to the VMware Exam Guide for Cloud Professional Exam

(https://mylearn.vmware.com/mgrreg/courses.cfm?ui=www_edu&a=one&id_subject=45954), "To create a new network segment that utilizes the corporate DHCP server to provide IP addresses, the following sequence should be used: Create a DHCP server profile, create a new segment attached to the Tier-0 gateway, and configure the segment DHCP config to utilize the new DHCP server profile."

NEW QUESTION 39

When configuring VMware Cloud Disaster Recovery (VCDR), with what can protection groups and disaster recovery plans be associated?

- A. Only a single vCenter Instance in the on-premises data center or VMware Cloud software-defined data center (SDDC).
- B. Multiple vCenter instances in the same VMware Cloud software-defined data center (SDDC) or on-premises data center.
- C. Multiple vCenter instances in the same VMware Cloud software-defined data center (SDDC) or only a single vCenter in the on-premises data center.
- D. Only a single vCenter Instance in the VMware Cloud software-defined data center (SDDC) or multiple vCenter Instances in the on-premises data center.

Answer: A

Explanation:

vCenter Mapping Mapping vCenters in a DR plan consists of selecting source vCenters that are registered to the protected site. Choosing a target vCenter for a Failover SDDC is simple; each SDDC contains a single vCenter instance. For VMware Cloud Disaster Recovery, keep in mind that a protected site can have multiple registered vCenters, but you can only map one vCenter on VMware Cloud on AWS per-DR plan.
<https://vmc.techzone.vmware.com/resource/introduction-vmware-cloud-disaster-recovery#inventory-and-re>

NEW QUESTION 44

Which types of networks are available when creating a segment in VMware Cloud on AWS?

- A. Routed, Extended, Disconnected
- B. Advertised, Extended, Isolated
- C. Routed, Stretched, Disconnected
- D. Advertised, Stretched, Isolated

Answer: A

Explanation:

VMware Cloud on AWS GovCloud supports three types of network segments: routed, extended and disconnected.

Routed networks: Routed networks allow you to route traffic between the on-premises data center and the VMware Cloud on AWS environment using a VPN or AWS Direct Connect.

Extended networks: Extended networks allow you to extend the on-premises network to the VMware Cloud on AWS environment using VXLAN. This type of network allows you to extend the on-premises VLANs to the cloud environment, providing a seamless network extension.

Disconnected networks: Disconnected networks are used when there is no direct connectivity between the on-premises data center and the VMware Cloud on AWS environment. This type of network allows you to create isolated networks in the cloud environment for specific use cases, such as disaster recovery or testing.

[https://docs.vmware.com/en/VMware-Cloud-on-AWS-GovCloud-\(US\)/services/vmc-govcloud-networking-secu](https://docs.vmware.com/en/VMware-Cloud-on-AWS-GovCloud-(US)/services/vmc-govcloud-networking-secu)

NEW QUESTION 46

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?

- A. Enhanced Linked Mode
- B. VMware HCX
- C. vCenter Single Sign-On
- D. Hybrid Linked Mode

Answer: B

Explanation:

VMware HCX is a cloud migration and workload mobility solution that allows you to view and manage workloads across both an on-premises environment and a VMware Cloud on AWS software-defined data center (SDDC). It provides a secure[1], cross-cloud network bridge between your on-premises environment and VMware Cloud on AWS, allowing you to move workloads between the two environments with minimal effort. It also provides a unified view of both environments, allowing administrators to monitor and manage workloads across clouds from a single pane of glass. [1]
[1]<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.hybrid-cloud-extensio>

NEW QUESTION 49

Which two steps does a cloud administrator need to take when protecting a VMware Cloud on AWS software-defined data center (SDDC) with VMware Site Recovery? (Choose Two.)

- A. Deploy the vSphere Replication virtual appliance.
- B. Deploy the Site Recovery manager virtual Appliance.
- C. Connect the Site Recovery manager instance on the protected recovery site.
- D. Register the vSphere Replication appliance with vCenter Single Sign-On
- E. Set the NSX-T Edge management gateway firewall rules.

Answer: AC

Explanation:

A cloud administrator needs to deploy the vSphere Replication virtual appliance and the Site Recovery manager virtual appliance when protecting a VMware Cloud on AWS software-defined data center (SDDC) with VMware Site Recovery.

The vSphere Replication virtual appliance is responsible for replicating the virtual machines from the source to the target site. Site Recovery Manager virtual appliance acts as the central management and orchestration platform for the entire disaster recovery process.

NEW QUESTION 53

A cloud administrator needs to extend a network and requires that routing be handled at the source. Which network segment type does VMware HCX Network Extension create in the VMware Cloud software-defined data center (SDDC) when extending the network?

- A. Extended
- B. Routed
- C. Private
- D. Disconnected

Answer: B

Explanation:

<https://docs.vmware.com/en/VMware-Validated-Design/services/sddc-extending-to-vmware-cloud-on-aws/GUI> <https://docs.vmware.com/en/VMware-HCX/4.5/hcx-user-guide/GUID-4052AC3F-9FFC-4FA2-ACB4-18B296>

VMware HCX Network Extension creates a routed network segment type in the VMware Cloud

software-defined data center (SDDC) when extending the network. This routed segment is used to connect the on-premises environment with the VMware Cloud SDDC, allowing traffic to flow between the two. The other options (extended, private, and disconnected segments) are not created by Network Extension.

NEW QUESTION 56

In VMware Cloud, who is responsible for the encryption of virtual machines?

- A. Native cloud provider
- B. Customer
- C. VMware Cloud Provider Partner (VCPP)
- D. VMware

Answer: B

Explanation:

Customer responsibility “Security in the Cloud” – Customers are responsible for the deployment and ongoing configuration of their SDDC, virtual machines, and data that reside therein. In addition to determining the network firewall and VPN configuration, customers are responsible for managing virtual machines (including in guest security and encryption) and using VMware Cloud on AWS User Roles and Permissions along with vCenter Roles and Permissions to apply the appropriate controls for users.

The responsibility for the encryption of virtual machines in VMware Cloud lies with the customer. The customer is responsible for configuring and managing any encryption or security related settings and configurations in the virtual machines, such as disk encryption or the configuration of security protocols. The VMware Cloud Provider Partner (VCPP) is responsible for the overall security of the cloud environment [1][2], including the encryption of data at rest, but the customer is responsible for configuring and managing the encryption settings within their virtual machines.

Reference: <https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.encryption/>

NEW QUESTION 57

What are two Incident management services included in the VMware Cloud on AWS service management process? (Choose two.)

- A. Email notifications for pending upgrades
- B. Return to service
- C. Severity classification
- D. SDDC upgrades
- E. Workload incident management

Answer: BC

Explanation:

Incident and Problem Management: VMware will provide incident and problem management services (e.g., detection, severity classification, recording, escalation, and return to service) pertaining to availability of the Service Offering. VMware is responsible for incident and problem management (e.g., detection, severity

classification, recording, escalation, and return to service) pertaining to all virtual machines that you have deployed in your SDDC.
<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/vmw-cloud-aws-service-descrip>

NEW QUESTION 62

Which statement accurately describes vSphere distributed switches? (Select one option)

- A. A distributed switch is a virtual switch that is configured for a single ESXi host.
- B. A standard switch is different from a distributed switch in that standard switches contain VMkernel ports.
- C. Each ESXi host can have only one distributed switch configured at any time.
- D. A distributed switch is managed by vCenter Server for all ESXi hosts associated with the distributed switch.

Answer: D

Explanation:

A distributed switch is managed by vCenter Server for all ESXi hosts associated with the distributed switch. A standard switch is different from a distributed switch in that standard switches contain VMkernel ports, but the entire configuration is managed by each ESXi host. A distributed switch is managed by vCenter Server for all ESXi hosts associated with the distributed switch and can contain multiple VMkernel ports. Each ESXi host can have multiple distributed switches configured at any time.

NEW QUESTION 65

A cloud administrator is establishing connectivity between their on-premises data center and VMware Cloud. The Administrator wants to leverage Border gateway Protocol (BGP) to Dynamically learn when new networks are created. Which type of VPN should the administrator configure to accomplish this?

- A. Layer 2 VPN
- B. SSL VPN
- C. Policy-based IPsec VPN
- D. Route-based IPsec VPN

Answer: D

Explanation:

Route-based IPsec VPNs provide the flexibility to dynamically learn when new networks are created, making them the ideal choice for establishing connectivity between an on-premises data center and VMware Cloud. Route-based IPsec VPNs use the Border Gateway Protocol (BGP) to dynamically learn and propagate routes over the VPN tunnel, allowing for scalable and secure connectivity. [1]

[1]<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.networking/GUID-ED>

NEW QUESTION 70

A cloud administrator is asked to evaluate a number of disaster recovery solutions for the business. The current on-premises environment is built around the latest version of VMware vSphere 7.0.

The following requirements must be met:

- Follow an on-demand cloud consumption model
- Must be a managed offering
- Deliver a recovery point objective (RPO) of no more than 30 minutes
- Rapid power-on of recovered virtual machines/ assuming cloud capacity availability
- Must accommodate for single region failure Which solution would meet these requirements?

- A. VMware Cloud Disaster Recovery
- B. VMware Cloud on AWS Stretched Cluster
- C. VMware vSphere Replication
- D. VMware Site Recovery Manager

Answer: A

Explanation:

VMware Cloud Disaster Recovery is a managed disaster recovery-as-a-service offering that is built on the latest version of VMware vSphere 7.0. It provides an on-demand cloud consumption model, allowing administrators to rapidly power-on recovered virtual machines in the cloud, assuming cloud capacity availability. Additionally, VMware Cloud Disaster Recovery delivers a recovery point objective (RPO) of no more than 30 minutes, and can accommodate for single region failure.

Publishing Applications with VMware Horizon 7 <https://vcdx.vmware.com/content/dam/digitalmarketing/vmware/ru/pdf/techpaper/vmware-horizon-7-application>
VMware Technical Support Guide

<https://www.vmware.com/pdf/techsupportguide.pdf>

Quick-Start Tutorial for VMware Dynamic Environment Manager ... <https://techzone.vmware.com/resource/quick-start-tutorial-vmware-dynamic-environment-manager> VMware Cloud Disaster Recovery ----- * Protect your workloads

running on VMware Cloud on AWS SDDC using high-frequency snapshots to achieve RPOs as low as 30 minutes. * Availability Zone Failure

Handling <https://docs.vmware.com/en/VMware-Cloud-Disaster-Recovery/services/vmware-cloud-disaster-recov>

<https://docs.vmware.com/en/VMware-Cloud-Disaster-Recovery/services/rn/vmware-cloud-disaster-recovery-rel>

NEW QUESTION 72

A Cloud Administrator is looking to migrate several dozen workloads from their on-premises location to a VMware public cloud using VMware -- need to be stretched for the migration. They will also be utilizing the capabilities of the WAN application for the migration.

HCX appliance requirements are as follows:

- HCX Manager: 4 vCPU, 128GB Memory
- HCX-IX Interconnect: 8 vCPU, 3GB Memory
- HCX network Extension: 8 vCPU, 3GB Memory
- HCX WAN Optimization: 8 vCPU, 14GB Memory

What are the on-premises vCPU and Memory component requirements for the VMware HCX deployment?

- A. 36 vCPUs, 35GB of memory
- B. 32 vCPUs, 40GB of memory
- C. 30 vCPUs, 36GB of memory
- D. 28 vCPUs, 32GB of memory

Answer: A

Explanation:

<https://docs.vmware.com/en/VMware-HCX/4.6/hcx-user-guide/GUID-D64901F4-6AB4-4820-9303-27927648A>

NEW QUESTION 76

When configuring Hybrid Linked Mode, what is the maximum supported latency between an on-premises environment and a VMware Cloud on AWS software-defined data center (SDDC)?

- A. 200 milliseconds round trip
- B. 250 milliseconds round trip
- C. 150 milliseconds round trip
- D. 100 milliseconds round trip

Answer: D

Explanation:

Hybrid Linked Mode can tolerate a time skew of up to ten minutes between the on-premises data center and the cloud SDDC. The maximum latency between your cloud SDDC and on-premises data center cannot exceed 100 msec roundtrip.

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vsphere.vmc-aws-manage-data-cen>

NEW QUESTION 79

As per company policy, all administrator level accounts need to have their password changed on a regular basis. The cloudadmin@vmc.local account password is changed by an administrator from the vSphere Client.

Another administrator is using the credentials in the VMware Cloud console and gets an 'access denied' error. What could be the problem?

- A. The password change email confirmation has NOT been approved by the organization owner.
- B. The password should only be changed through the VMware Cloud console.
- C. The new password is NOT synchronized with the password that is displayed for the Default vCenter user account.
- D. The password should be changed by escalation of privileges.

Answer: C

Explanation:

The problem could be that the new password is not synchronized with the password that is displayed for the Default vCenter user account. The administrator must make sure that the same password is used in both the vSphere Client and the VMware Cloud console in order for the user to access the account. Changing the password in one place does not automatically change it in the other, so this must be done manually.

NEW QUESTION 82

What is a prerequisite step to adding additional users to a Google Cloud VMware Engine's vCenter (GCVE)?

- A. Change the default administrator password.
- B. Add a user in Google Cloud Platform Identity and Access Management.
- C. Open a support ticket to escalate VMware vSphere privileges.
- D. Escalate VMware vSphere privileges In the GCVE portal.

Answer: B

Explanation:

The prerequisite step to adding additional users to a Google Cloud VMware Engine's vCenter (GCVE) is to add a user in Google Cloud Platform Identity and Access Management. This will allow for the user to be added to the vCenter and properly authenticated.

NEW QUESTION 84

A cloud administrator is looking for a unified solution to collect and analyze security events for troubleshooting from: VMware vSphere Windows Operating Systems Physical servers Web servers Database servers Amazon Web Services Which VMware Cloud service can meet this requirement?

- A. VMware vRealize Automation Cloud
- B. CloudHealth Secure State
- C. VMware vRealize Log Insight Cloud
- D. VMware vRealize Network Insight Cloud

Answer: C

Explanation:

<https://blogs.vmware.com/management/2022/08/forwarding-vsphere-audit-and-authentication-events-from-vreal>

NEW QUESTION 85

What are two incident management services included in the VMware Cloud on AWS service management process? (Choose two)

- A. VMware Tools management
- B. Incident Management
- C. Microsoft License management

- D. Capacity management
- E. Workload OS management

Answer: BD

Explanation:

The two incident management services included in the VMware Cloud on AWS Service Management process are Incident Management and Capacity Management.

Incident Management is responsible for detecting, classifying, and resolving incidents quickly and effectively. It includes monitoring and alerting, incident response, and problem management. Capacity Management is responsible for predicting, measuring, and managing the capacity of the infrastructure. It includes capacity planning, performance analysis, and resource optimization.

References:

[1]<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/cloud-management/vmware-cloud-o>

NEW QUESTION 86

Which use cases apply to NSX logical routing? (Select two options)

- A. You must provide external connectivity to VMs and containers.
- B. Your organization must provide connectivity between VMs and containers that are connected to different segments.
- C. You want to provide layer 2 connectivity between VMs and microservices.
- D. You require intrinsic security for VMs connected to different segments.

Answer: AB

Explanation:

The two use cases that apply to NSX logical routing are A. You must provide external connectivity to VMs and containers, and B. Your organization must provide connectivity between VMs and containers that are connected to different segments. NSX logical routing allows you to provide external connectivity to VMs and containers, and to provide layer 3 connectivity between VMs and containers that are connected to different segments. It does not provide layer 2 connectivity between VMs and microservices or intrinsic security for VMs connected to different segments.

NEW QUESTION 89

A customer is concerned about threats propagating out to their cloud disaster recovery site. Which VMware Cloud solution offers the capability for an operational air-gap to stop ransomware?

- A. VMware Cloud Disaster Recovery
- B. VMware Hybrid Cloud Extension
- C. VMware Site Recovery
- D. VMware Secure Access Service Edge

Answer: A

Explanation:

<https://blogs.vmware.com/virtualblocks/2021/09/28/operational-air-gaps/>

Operational isolation (operational “air-gapping”) is critical to DR. VMware Cloud DR was designed from the very beginning for its systems and repository to be operationally isolated and for instantiating isolated recovery environments.

NEW QUESTION 93

What is a key driver behind the multi-cloud journey?

- A. Facilitate disaster recovery
- B. Application modernization
- C. Digital transformation
- D. Cost savings

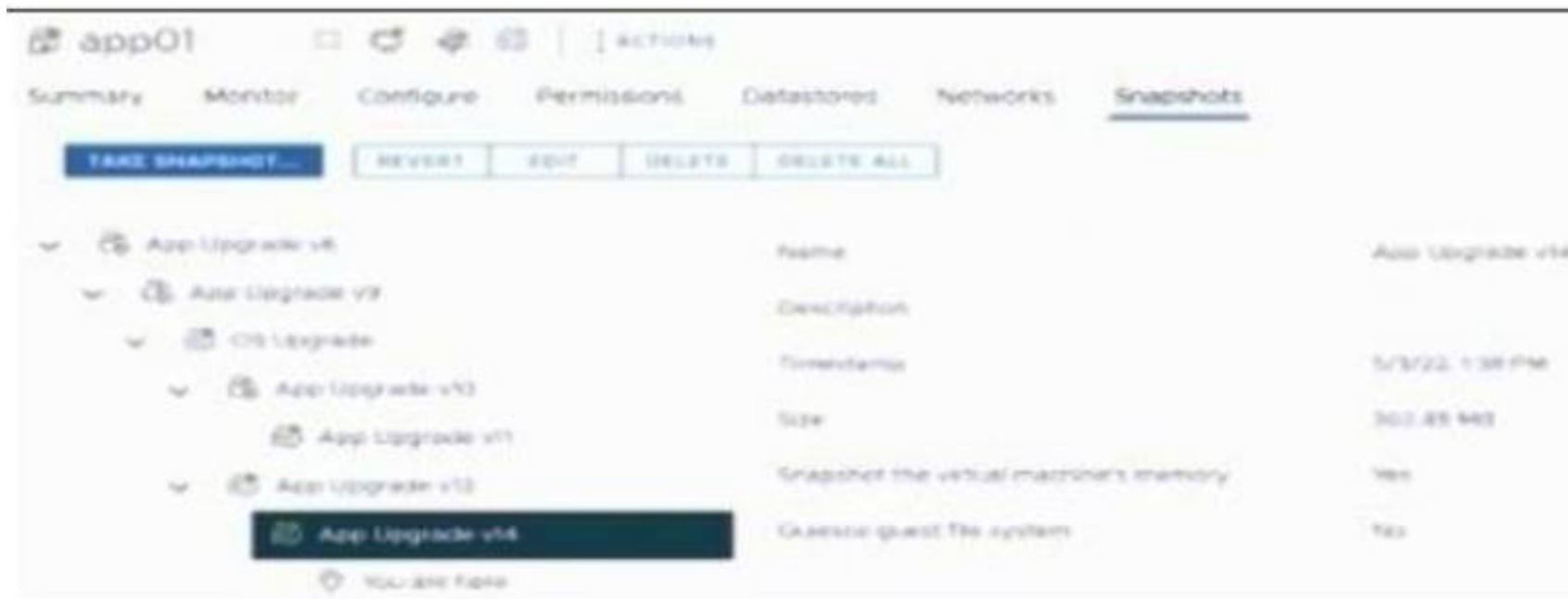
Answer: C

Explanation:

A key driver behind the multi-cloud journey is digital transformation, which is the process of using technology to optimize existing processes and systems in order to improve customer experiences, increase operational efficiency, and accelerate business growth. Multi-cloud solutions can help organizations modernize their applications and services, reduce costs, increase agility, and support digital transformation initiatives. 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>.

NEW QUESTION 96

Refer to the exhibit.



A cloud administrator is investigating a reported performance issue on a virtual machine (VM). The administrator observes low latency on the datastore but high latency within the VM. The administrator notes that it is a standard operating procedure to take a snapshot of the VM whenever there is an application or operating system upgrade on this VM.

Based on the exhibit, which snapshot characteristic will result in performance degradation?

- A. Snapshot chain length
- B. Snapshot size
- C. Snapshot type
- D. Snapshot age

Answer: A

Explanation:

<https://www.nakivo.com/blog/vmware-snapshots-vsphere-how-to/#title-12> Follow these recommendations to get the best performance when using snapshots:

- Use snapshots as a temporary measure only. The presence of snapshots can have a significant impact on guest application performance, especially in a VMFS environment, for I/O intensive workloads. The guest applications fully recover performance after snapshots are deleted.
- Keep the snapshot chain length short when possible, to minimize the guest application performance impact. Performance degradation is higher as the snapshot chain length increases.
- If you need to increase the size of a virtual disk that has snapshots associated with it, you must delete the snapshots first before you can increase the virtual disk's size.

NEW QUESTION 100

Which two steps should an administrator take to allow HTTPS access to a specific virtual machine (VM) through the public Internet for VMware Cloud on AWS? (Choose two.)

- A. Create a custom service called HTTPS using port 443.
- B. Configure AWS Direct Connect.
- C. Configure a SNAT rule translating an internal IP address to a public IP address.
- D. Request a public IP address in the VMware Cloud console.
- E. Configure a DNAT rule translating a public IP address to an internal IP address.

Answer: AD

Explanation:

To allow HTTPS access to a specific VM through the public Internet for VMware Cloud on AWS, the administrator must first create a custom service called HTTPS using port 443. They must then request a public IP address in the VMware Cloud console.

NEW QUESTION 104

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

- 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: AD

Explanation:

As per the official guide from VMware, VMware is responsible for managing the capacity of the cloud software-defined data centers (SDDCs) and for updating the software-defined data center (SDDC) software. This includes managing the underlying infrastructure, such as the hosts, storage, and networking, and ensuring that the SDDCs are running the latest version of the software.

NEW QUESTION 105

Which statement describes the VMware Multi-Cloud vision?

- A. Flexibility to operate globally and consistently
- B. Flexibility to choose any hardware vendor
- C. Flexibility to manage infrastructure through outsourcing
- D. Flexibility to choose any hypervisor

Answer: A

Explanation:

<https://www.vmware.com/cloud-solutions/multi-cloud.html>

Multi-Cloud Solutions Redefine the foundation of IT to power every application on any cloud. With

Multi-Cloud solutions from VMware, you can migrate to the cloud without recoding your apps, modernize your infrastructure, and operate consistently across the data center, the edge, and any cloud.

NEW QUESTION 110

What is the purpose of the VMware Cloud on AWS Compute Gateway (CGW)?

- A. A Tier-1 router that handles routing and firewalling for the VMware vCenter Server and other management appliances running in the software-defined data center (SDDC)
- B. A Tier-1 router that handles workload traffic that is connected to routed compute network segments
- C. A Tier-0 router that handles routing and firewalling for the VMware vCenter Server and other management appliances running in the software-defined data center (SDDC)
- D. A Tier-0 router that handles workload traffic that is connected to routed compute network segments

Answer: B

Explanation:

Compute Gateway (CGW) The CGW is a Tier 1 router that handles network traffic for workload VMs connected to routed compute network segments. Compute gateway firewall rules, along with NAT rules, run on the Tier 0 router. In the default configuration, these rules block all traffic to and from compute network segments (see Configure Compute Gateway Networking and Security).

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/vmc-on-aws-networking-security.pdf>

NEW QUESTION 115

A cloud administrator wants to deploy a VMware Cloud software-defined data center (SDDC) on a cloud provider and requires a consistent 4.5 Gbps bandwidth from applications to communicate from on-premises to the SDDC. Which type of connection should be used for this type of traffic?

- A. Policy-based virtual private network (VPN)
- B. Private L2 virtual private network (VPN)
- C. Route-based virtual private network (VPN)
- D. Private line

Answer: C

Explanation:

The best option for a cloud administrator who wants to deploy a VMware Cloud software-defined data center (SDDC) on a cloud provider and requires a consistent 4.5 Gbps bandwidth from applications to communicate from on-premises to the SDDC is a Route-Based Virtual Private Network (VPN). This type of connection offers enhanced performance [1][2], flexibility, scalability, and security compared to other options, such as Policy-Based Virtual Private Network (VPN), Private L2 Virtual Private Network (VPN), or Private Line.

According to the VMware official site, "Route-based VPN enables a secure connection between two or more sites, or between a site and a mobile user, and provides better performance and scalability than a policy-based VPN. Route-based VPNs are also more secure than policy-based VPNs, because the traffic is encrypted with a unique encryption key for each tunnel, rather than relying on a shared key for all tunnels. This allows for secure and reliable connections for devices and applications located in different physical locations." [1]

[1] <https://docs.vmware.com/en/VMware-NSX-Data-Center/2.4/com.vmware.nsx.admin.doc/GUID-D6B7B9E>

NEW QUESTION 118

What must a cloud administrator configure in order to allow a company's on-premises data center to access the VMware Cloud on AWS vCenter Server.

- A. Management network segment
- B. Compute gateway firewall
- C. Management gateway firewall
- D. Compute network segment

Answer: C

Explanation:

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-networking-security/GUI>

NEW QUESTION 122

Which out-of-the-box role is required in order to create a content library in VMware Cloud on AWS?

- A. CloudGlobalAdmin
- B. CloudAdmin
- C. Active Directory ESXi Admin
- D. Administrator@vSphere
- E. local

Answer: B

Explanation:

The CloudAdmin role has the privileges necessary to create and manage SDDC workloads and related objects such as storage policies, content libraries, vSphere tags, and resource pools

NEW QUESTION 126

Which Tanzu Kubernetes Grid component provides authentication, ingress, logging and service discovery?

- A. Tanzu Supervisor cluster
- B. Tanzu CU
- C. Tanzu Kubernetes cluster
- D. Tanzu Kubernetes Grid extensions

Answer: C

Explanation:

<https://docs.vmware.com/en/VMware-vSphere/7.0/vmware-vsphere-with-tanzu/GUID-4D0D375F-C001-4F1D-> <https://docs.vmware.com/en/VMware-vSphere/7.0/vmware-vsphere-with-tanzu/GUID-4D0D375F-C001-4F1D->

NEW QUESTION 130

VMware Engine cloud administrator is tasked with ensuring that a dedicated, secure, high-speed, and low-latency connection exists between an on-premises VMware Engine. Which two options are available for Google Cloud VMware Engine? (Choose two.)

- A. Partner Interconnect
- B. Global Reach
- C. Dedicated Interconnect
- D. ExpressRoute
- E. Direct Connect

Answer: AC

Explanation:

<https://cloud.google.com/architecture/private-cloud-networking-for-vmware-engine>

Dedicated Interconnect provides a private[1][2], dedicated connection between your on-premises network and Google's network. It offers low latency, high bandwidth, and a secure connection. Partner Interconnect provides a connection to Google Cloud Platform through a partner's network, such as a service provider or a carrier. It offers the same low latency, high bandwidth, and secure connection, but is slightly slower than Dedicated Interconnect.

References: [1]<https://cloud.google.com/interconnect/docs/concepts/types>[2]<https://docs.vmware.com/en/VMware-Cloud-on>

NEW QUESTION 135

A cloud administrator successfully configures a policy-based VPN between an on-premises data center and an instance of VMware Cloud Software-defined data center (SDDC). Although the workloads are reachable from both locations over the IP network, the cloud virtual machines cannot access an on-premises web service. What should the cloud administrator check first to resolve this issue?

- A. On-premises DNS settings
- B. VMware Cloud DNS settings
- C. On-premises gateway settings
- D. VMware Cloud gateway settings

Answer: B

Explanation:

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-networking-security/GUI>

NEW QUESTION 140

What is one way in which VMware Multi-Cloud addresses challenges with the cloud computing model?

- A. Provides savings on capital expenses and the use of a flexible payment structure where payment is only done based on the resources used.
- B. Provides visibility and tools to manage resources, workloads and operations across clouds from a common operating environment.
- C. Eliminates worry associated with managing IT infrastructures and shifts focus to application development and other priorities using the most up-to-date technology.
- D. Increases agility that encompasses scalability, customizability, and access to the cloud service from anywhere and on any device.

Answer: B

Explanation:

<https://www.vmware.com/topics/glossary/content/multi-cloud.html>

VMware Multi-Cloud provides visibility and tools to manage resources, workloads and operations across clouds from a common operating environment. This eliminates the need to manage multiple cloud environments in different clouds and provides a unified view of all cloud resources and applications. This makes it easier to monitor and manage workloads across clouds, reducing complexity and increasing agility.

VMware Multi-Cloud also provides powerful automation and orchestration capabilities to help streamline operations and improve efficiency. [1]

[1]<https://www.vmware.com/products/vmware-multi-cloud.html>

NEW QUESTION 143

A user is assigned the CloudAdmin role in a VMware Cloud on AWS software-defined data center (SDDC). At which level in the inventory hierarchy can the user deploy virtual machines?

- A. Compute-ResourcePool in the Hosts and Clusters view
- B. Discovered virtual machine folder in the VMs and Templates view
- C. vsanDatastore in the Storage view
- D. Mgmt-ResourcePool in the Hosts and Clusters view

Answer: B

Explanation:

This would enable the user to have the necessary permissions to deploy virtual machines - and thus, would ensure that all of the necessary virtual machines are deployed in a timely and efficient manner.

- VMware Cloud on AWS Documentation: "Deployment of virtual machines"
- VMware Cloud on AWS Documentation: "Creating virtual machines with the VMware Cloud on AWS console"
- VMware Cloud on AWS Documentation: "Managing virtual machines with the VMware Cloud on AWS console"

NEW QUESTION 148

A cloud administrator is responsible for managing a VMware Cloud solution and would like to ensure that I/O-intensive workloads run in the most optimum way possible.

Which two steps should the administrator complete on I/O-intensive workloads to meet this requirement? (Choose two.)

- A. Ensure that the VMware hardware version is 7 or later.
- B. Enable the memory hot-add feature.
- C. Configure the LSI Logic Parallel SCSI controller.
- D. Configure the VMware Paravirtual SCSI (PVSCSI) adapter.
- E. Configure a maximum of two CPU cores per socket.

Answer: AD

Explanation:

The two steps that the cloud administrator should complete on I/O-intensive workloads to ensure the best performance possible are to configure the VMware Paravirtual SCSI (PVSCSI) adapter and to ensure that the VMware hardware version is 7 or later. The PVSCSI adapter provides improved performance and scalability compared to the LSI Logic Parallel SCSI controller. Additionally, the hardware version should be 7 or later to ensure that the virtual machine is able to take advantage of the latest features and enhancements. Enabling the memory hot-add feature and configuring a maximum of two CPU cores per socket will not improve the performance of I/O-intensive workloads.

Why does VMware refuse to educate their customers ... - VMware ... <https://communities.vmware.com/t5/VMware-Education-Services/Why-does-VMware-refuse-to-educate-their-c> VMware Technical Support Guide

<https://www.vmware.com/pdf/techsupportguide.pdf> Publishing Applications with VMware Horizon 7

<https://vcdx.vmware.com/content/dam/digitalmarketing/vmware/ru/pdf/techpaper/vmware-horizon-7-application>

LSI Logic Parallel, LSI Logic SAS, or VMware Paravirtual

For most guest operating systems, the default virtual storage adapter in VMware Cloud on AWS is either LSI Logic Parallel or LSI Logic SAS, depending on the guest operating system and the virtual hardware version.

However, VMware Cloud on AWS also includes a paravirtualized SCSI storage adapter, PVSCSI (also called VMware Paravirtual). The PVSCSI adapter offers a significant reduction in CPU utilization as well as potentially increased throughput compared to the default virtual storage adapters, and is thus the best choice for environments with very I/O-intensive guest applications.

In order to use PVSCSI, your VM must be using virtual hardware version 7 or later.

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/vmc-aws-performance.pdf>

NEW QUESTION 151

A customer is running a software-defined data center (SDDC) in the US-East-2 region and wants to connect the workload network segment to their on-premises data center and multiple company Amazon Virtual Private Clouds (VPCs) running in US-East-2.

Which connectivity option can they use to accomplish this?

- A. AWS Direct Connect
- B. Two VPN connections
- C. VMware Transit Connect
- D. One VPN connection

Answer: C

Explanation:

To connect the workload network segment to their on-premises data center and multiple company Amazon VPCs running in US-East-2, the customer can use VMware Transit Connect. VMware Transit Connect is a service that provides secure connectivity between AWS and on-premises data centers or other clouds. It allows customers to connect and extend their networks to the AWS cloud with minimal effort and cost.

NEW QUESTION 155

Which three functions are provided by the components within the Kubernetes control plane? (Choose three.)

- A. Balances pods across the nodes within a Kubernetes cluster.
- B. Ensures that containers are running in a pod.
- C. Configures network rules to route traffic to containers within the Kubernetes cluster.
- D. Stores Kubernetes cluster data in a key-value data store.
- E. Watches the API for changes and responds with appropriate actions.
- F. Stores and distributes container images.

Answer: ADE

Explanation:

<https://kubernetes.io/docs/concepts/overview/components/#control-plane-components>

NEW QUESTION 156

Which vSphere HA default response is applied when a virtual machine crashes on a VMware Cloud cluster?

- A. Restart the impacted virtual machine on the same host in the same SDDC cluster
- B. Shut down the impacted virtual machine and do not restart it anywhere
- C. Restart the impacted virtual machine on other hosts in other SDDC Cluster
- D. Restart the impacted virtual machine on other hosts in the same SDDC Cluster

Answer: D

Explanation:

VMware High Availability (HA) is a feature of the VMware Cloud platform that monitors the health of virtual machines and restarts virtual machines on other hosts if they crash or become unresponsive. This ensures that the virtual machines are always available and that no downtime is experienced. The default response is to restart the impacted virtual machine on other hosts in the same SDDC Cluster, however, this can be customized to suit the needs of the customer.

References:

[1]https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.availability_and_scala

NEW QUESTION 158

A cloud administrator is tasked with migrating workloads from an on-premises environment to a VMware Cloud on AWS software-defined datacenter (SDDC) with no downtime while retaining their IP Address. Which connectivity type should be used?

- A. Private policy-based IPsec VPN
- B. Private route-based IPsec VPN
- C. Open VPN
- D. Private Layer 2 VPN

Answer: D

Explanation:

Private L2 VPN: To migrate running VMs between SDDCs in different geographical locations.

You use a private layer 2 (L2) VPN to extend an on-premises network to your cloud SDDC. This extended network is a single subnet with a single broadcast domain.

You can use L2 VPNs to migrate VMs to and from your cloud SDDC, for disaster recovery, or for dynamic access to cloud computing resources (often called cloud bursting).

VM migrations across an L2 VPN support VLAN tagging and GENEVE frame encapsulation when migrating between a cloud SDDC to another SDDC.

The L2 VPN tunnel extends layer 2 networks across geographic sites. VMs can move across sites (using vSphere vMotion) and keep the same IP addresses using an L2 VPN.

NEW QUESTION 162

A cloud administrator needs to configure a VM storage policy for virtual machines that will host a business critical application. The environment consists of a single cluster with six hosts. The application is storage I/O intensive and redundancy must be provided at the highest level possible.

Which VM storage policy settings should the administrator configure to meet these requirements?

- A. RAID-1 FTT = 3
- B. RAID-1 FTT = 2
- C. RAID-5
- D. RAID-6

Answer: B

Explanation:

RAID-1 is a mirror configuration that provides high availability by creating multiple copies of a VMDK. RAID-5 and RAID-6 are erasure coding configurations that provide fault tolerance by distributing data and parity across multiple hosts.

The number of failures to tolerate (FTT) determines how many copies or parity blocks are created for each VMDK. For example, RAID-1 FTT = 2 means that there are three copies of each VMDK.

Therefore, based on your requirements, a possible VM storage policy setting could be RAID-1 FTT = 2, which would provide redundancy at the highest level possible with six hosts.

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vsphere.vmc-aws-manage-data-cen>

NEW QUESTION 163

An administrator is tasked with collecting a support bundle from a Tanzu Kubernetes cluster for a support case. How can the administrator collect this support bundle for the Tanzu Kubernetes cluster?

- A. Run the -tkc-support-bundler command.
- B. Run the kubact1 logs my-pod command
- C. Run a compression tool of the log files located in /var/log/vmware/wcp/.
- D. Run the vm-support command.

Answer: A

Explanation:

<https://kb.vmware.com/s/article/80949>

Tanzu Kubernetes Grid (TKG) provides a command line tool called tkg-support-bundler which can be used to collect the necessary information and logs for troubleshooting and support cases. The command can be run on the TKG CLI and it will gather all the necessary information and logs from the TKG control plane and worker nodes, and package them into a single compressed bundle file. This bundle file can then be provided to VMware support for further analysis.

NEW QUESTION 164

Which three items should be considered when performing a hot migration of a virtual machine (VM)? (Choose three.)

- A. The source and destination host management network IP address families must match
- B. The vGPU configuration of the VM
- C. The status of the guest operating system in the VM
- D. The CPU instruction set required by the VM
- E. The source and destination host must have shared access to the storage that contains the VM
- F. The status of VMware Tools on the VM

Answer: CEF

Explanation:

For the source and destination host to have shared access to the storage that contains the VM, they must be able to access the same datastore. This requires that the datastore be available to both hosts and that the datastore has the same name on both hosts.

The status of VMware Tools on the VM should also be checked before performing a hot migration. VMware Tools is a suite of utilities that enhances the performance of a virtual machine's guest operating system and improves the management of the virtual machine. If VMware Tools is not installed or not up to date, the hot migration may fail.

Finally, the status of the guest operating system in the VM should also be checked before performing a hot migration. The guest operating system should be up and running and not in a suspended state. If the guest operating system is in a suspended state, the hot migration may fail.

The CPU instruction set required by the VM and the vGPU configuration of the VM are not items to consider when performing a hot migration of a virtual machine. The source and destination host management network IP address families do not need to match for the hot migration to be successful.

References:

[1] https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.vm_admin.doc/GUID-B2B7F78A

NEW QUESTION 169

Which four steps must a cloud administrator take to deploy a new private cloud In Azure VMware Solution? (Choose four.)

- A. Identify the maximum number of hosts needed for future capacity.
- B. Identify the desired availability zone.
- C. Identify a management CIDR of size /22.
- D. Open a support request with Microsoft Azure requesting capacity.
- E. Identify a management CIDR of size /20.
- F. Identify the desired region.
- G. Identify the current number of hosts needed.

Answer: BCDG

Explanation:

➤ Identify the desired region. This determines where your private cloud will be deployed and which Azure services are available.

➤ Identify a management CIDR of size /22. This determines the IP address range for your private cloud management components such as vCenter Server, NSX Manager, etc.

➤ Open a support request with Microsoft Azure requesting capacity. This ensures that there are enough hosts available for your private cloud deployment.

➤ Identify the current number of hosts needed. This determines how many hosts will be provisioned initially for your private cloud cluster.

<https://vmc.techzone.vmware.com/resource/avs-planning-and-deployment-guide>

NEW QUESTION 172

In VMware Cloud Disaster Recovery (VCDR), a protection group consists of which two components? (Choose two.)

- A. Members
- B. Policies for snapshots
- C. Virtual Machine File System (VMFS) datastores
- D. VM customizations
- E. Clusters

Answer: AB

Explanation:

<https://docs.vmware.com/en/VMware-Cloud-Disaster-Recovery/services/vmware-cloud-disaster-recovery/GUID-> A protection group in VMware Cloud Disaster Recovery (VCDR) consists of members (virtual machines or VMs) and policies for snapshots. These policies define the consistent point-in-time copies of the VMs, which are used for disaster recovery. The protection group also includes virtual machine file system (VMFS) datastores, which are used to store the copies of the VMs, and VM customizations, which are used to customize the VMs. Clusters are not part of a protection group in VCDR.

NEW QUESTION 175

Which three components can be part of a virtual machine template? (Choose three.)

- A. Installed applications, tools, and patches
- B. vSphere tags
- C. Custom attributes
- D. Virtual Machine hardware configuration
- E. Guest operating system
- F. Virtual machine snapshots

Answer: ADE

Explanation:

To create a virtual machine template, you will need to configure the virtual machine hardware configuration, install the necessary applications, tools, and patches, and select the guest operating system. The template can also include vSphere tags and custom attributes to further customize the virtual machine. Additionally, the

template can include virtual machine snapshots which will save the current state of the virtual machine and can be used to quickly restore the machine to the same state.

VMware Technical Support Guide <https://www.vmware.com/pdf/techsupportguide.pdf> Publishing Applications with VMware Horizon 7

<https://vcdx.vmware.com/content/dam/digitalmarketing/vmware/ru/pdf/techpaper/vmware-horizon-7-application> What is Server Virtualization? | VMware Glossary

<https://www.vmware.com/topics/glossary/content/server-virtualization.html>

NEW QUESTION 176

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?

- 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/>

NEW QUESTION 181

Which software development challenge can a cloud administrator address by adopting a cloud operating model?

- A. The length of time needed to provision the required infrastructure
- B. High operating expense (OPEX) spending due to software licenses
- C. The use of different programming languages by developers
- D. Lack of standardization of operating systems used by developers

Answer: A

Explanation:

<https://blogs.vmware.com/management/2021/10/introduction-to-vmware-cloud-operating-model.html>

NEW QUESTION 185

Which VMware technology ensures availability of the VMs in your SDDC and uses multiple ESXi hosts to provide rapid recovery from outages and cost-effective high availability for applications? (Select one option)

- A. vSphere DRaaS
- B. vSphere HA
- C. vSphere DPM
- D. vSphere eDRS

Answer: B

Explanation:

The VMware technology that ensures availability of the VMs in your SDDC and uses multiple ESXi hosts to provide rapid recovery from outages and cost-effective high availability for applications is B.vSphere HA. vSphere HA is an agentless cluster-level availability solution that enables rapid recovery from outages and cost-effective high availability for applications. vSphere DRaaS, vSphere DPM, and vSphere eDRS are not suitable for this purpose.

NEW QUESTION 189

.....

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

2V0-33.22 Practice Exam Features:

- * 2V0-33.22 Questions and Answers Updated Frequently
- * 2V0-33.22 Practice Questions Verified by Expert Senior Certified Staff
- * 2V0-33.22 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 2V0-33.22 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 2V0-33.22 Practice Test Here](#)