

VMware

Exam Questions 2V0-33.22

VMware Cloud Professional



NEW QUESTION 1

A cloud administrator wants to enable administrator wants to enable Enterprise Federation to the Cloud Services Portal in order to be able to authenticate with the on-premises Active Directory. The Administrator Already deployed the on-premises VMware Workspace One Access Connector. Through which port does the Cloud Service Portal communicate with Workspace ONE Access Connector?

- A. Idaps/636
- B. http/80
- C. https/443
- D. Idap/389

Answer: C

Explanation:

https://docs.vmware.com/en/VMware-Workspace-ONE-Access/20.10/workspace_one_access_install/GUID-E81 The Cloud Services Portal communicates with the Workspace ONE Access Connector via port 443 (HTTPS).

According to the VMware documentation [1], the Cloud Services Portal connects to the Access Connector on port 443 to authenticate users and authorize access to the cloud service. The Access Connector listens on port 443 and communicates with the Active Directory using LDAP over TLS (LDAPS) on port 636.

Reference: <https://docs.vmware.com/en/VMware-Workspace-ONE-Access/services/com.vmware.access.admi>

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 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 4

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 5

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 6

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 7

Which logical switching component provides layer 2 forwarding functionality in a VMwareCloud software-defined data center (SDDC).

- A. Segment port
- B. Uplink
- C. N-VDS/VDS
- D. Transport node

Answer: C

Explanation:

A VMware Cloud software-defined data center (SDDC) uses a logical switching component called a Network Virtual Distributed Switch (N-VDS) or vSphere Distributed Switch (VDS) to provide layer 2 forwarding functionality [1][2]. A VDS is a network switch that provides centralized network configuration, management, and monitoring. It works with the NSX for vSphere data plane to provide layer 2 forwarding, packet filtering, and traffic monitoring services. A VDS is composed of multiple Segment Ports (which are like individual physical ports on a normal switch), Uplinks, and Transport Nodes. The Segment Ports are used to connect virtual machines to the VDS, while Uplinks are used to connect the VDS to physical networks. Transport

Nodes are the physical switches that are associated with the VDS. For more information, see the official VMware documentation here: https://docs.vmware.com/en/VMware-NSX-Data-Center/2.4/nsx_24_sdn_networking/GUID-A4A6E4A8

NEW QUESTION 8

A cloud administrator is tasked with improving the way that containers are scaled and managed in the environment. There is a currently no container orchestration solution implemented. Which solution can the administrator leverage to achieve this?

- A. VMware NSX Container Plugin
- B. Kubernetes
- C. VMware vRealize Suite Lifecycle Manager
- D. etcd

Answer: B

Explanation:

Kubernetes is an open-source container orchestration system for automating application deployment, scaling, and management, which provides features such as self-healing, auto-scaling, and service discovery. With Kubernetes, cloud administrators are able to easily scale and manage containers across multiple clusters and nodes, allowing them to more effectively manage container-based applications. Additionally, Kubernetes provides advanced features such as container scheduling, resource management, and service discovery, which are all essential for managing container-based applications in a production environment. For more information on Kubernetes, you can refer to the official VMware documentation here: https://docs.vmware.com/en/VMware-NSX-Data-Center/2.4/nsx_24_sdn_networking/GUID-A4A6E4A8

NEW QUESTION 9

A cloud administrator is tasked with moving critical business workloads between two VMware Cloud on AWS software-defined data centers (SDDCs) located in different geographical regions. The following requirements must be met:

- Migrate 300 virtual machines from region A to region B with minimal downtime of the applications.
- Non-disruptively resume application access of the targeted virtual machines in the event the migration fails.
- Support concurrent switch over of the application workloads to occur during a pre-defined maintenance window.

Which VMware HCX migration type should be used to meet these requirements?

- A. VMware HCX Cold Migration
- B. VMware HCX Bulk Migration
- C. VMware HCX vMotion

D. VMware HCX Replication Assisted vMotion

Answer: D

Explanation:

<https://docs.vmware.com/en/VMware-HCX/4.5/hcx-user-guide/GUID-741F47D5-A3C9-4D74-9672-E54D8791> "VMware HCX Replication Assisted vMotion (RAV) uses the HCX Interconnect appliance along with replication and vMotion technologies to provide large scale, parallel migrations with zero downtime."
Understanding VMware HCX Replication Assisted vMotion:<https://docs.vmware.com/en/VMware-HCX/4.6/hcx-user-guide/GUID-741F47D5-A3C9-4D74-9672-E>

NEW QUESTION 10

Which three types of gateways can be found in VMware cloud on AWS (Choose three?)

- A. Distributed Tier-1
- B. Standard Tier-1
- C. Tire-0
- D. Compute Tier-1
- E. Management Tire-1
- F. Management Tire-0

Answer: ABD

Explanation:

The three types of gateways that can be found in VMware Cloud on AWS are Option A: Distributed Tier-1, Option B: Standard Tier-1, and Option D: Compute Tier-1.

Distributed Tier-1 gateways are used for secure access between on-premises networks and the VMware Cloud on AWS SDDC network. Standard Tier-1 gateways are used for secure access between the VMware Cloud on AWS SDDC network and the public internet. Compute Tier-1 gateways are used for secure access between the workloads running on the VMware Cloud on AWS SDDC and the public internet.

For more information, please refer to the official VMware documentation on VMware Cloud on AWS Gateways:<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.networking/GU>

NEW QUESTION 10

What is the purpose or the VMware cloud on AWS management gateway (MGW)?

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

Answer: D

Explanation:

Management Gateway (MGW) The MGW is a Tier 1 router that handles routing and firewalling for vCenter Server and other management appliances running in the SDDC. Management gateway firewall rules run on the MGW and control access to management VMs. In a new SDDC, the Internet connection is labelled Not Connected in the Overview tab and remains blocked until you create a Management Gateway Firewall rule allowing access from a trusted source.

NEW QUESTION 13

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 16

Refer to the exhibit.

VPC and subnet Specify the VPC and the subnet to connect to your AWS account.

Choose the VPC and subnet from your AWS account where you have or may want to deploy AWS EC2 workloads to work with resources in your SDDC. You will only be able to choose subnets that are in the same availability zone as where the SDDC EC2 hosts are deployed.

What is an AWS VPC and subnet?

What is an Availability Zone?

VPC:

Subnet:

Configure Network Management Subnet (optional)

- Specify a private subnet range (CIDR block) to be used for vCenter, NSX Manager, and ESXi hosts.
- Choose a range that will not overlap with other subnets or CIDR blocks in your VPC that connect to this SDDC.
- Minimum CIDR size: /28 for up to 254 hosts, /29 for up to 254 hosts, /30 for up to 4096 hosts.
- Reserved CIDRs: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16.

Management Subnet:

A cloud administrator is deploying a new VMware Cloud on AWS virtual private cloud (VPC). After clicking on deploy, the screen refreshes and displays the information that is provided in the exhibit.

What is the issue with the management CIDR that is causing the deployment to fail?

- A. It overlaps with the AWS subnet.
- B. It overlaps with the AWS VPC CIDR.
- C. It is part of the reserved CIDRs.
- D. It is an invalid size.

Answer: A

Explanation:

<https://docs.aws.amazon.com/whitepapers/latest/sddc-deployment-and-best-practices/deploying-vmware-cloud-on-aws> must be a RFC1918 private address space (10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16) with CIDR block sizes of /16, /20, or /23. The management CIDR block cannot be changed after the SDDC is deployed. Choose a range of IP addresses that does not overlap with the AWS subnet you are connecting to. If you plan to connect the SDDC to an on-premises DC or another environment, the IP subnet must be unique within your enterprise network infrastructure. Choose a CIDR that will give you future scalability.

NEW QUESTION 18

A Cloud administrator is starting to plan a workload migration and wants to estimate the cost of running those workloads on VMware Cloud. Which VMware Cloud service should the administrator use to achieve this goal?

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

Answer: B

Explanation:

Managing Costs:

With its capacity and cost management features, vRealize Operations Cloud can predict future demand and provide actionable recommendations to help in managing costs.

Reclamation of Existing Resources:

Assess workload status and resource contention in data centers across your environment:

- Determine the time remaining until CPU, memory, or storage resources run out.
- Realize cost savings when underutilized VMs are identified and reclaimed to be deployed more effectively.

Future Infrastructure Requirements

Run what-if scenarios:

- Identify how much capacity remains after you add or remove VMs or hosts.
- Add hyperconverged infrastructure (HCI) nodes.
- Get a recommendation based on the cost relative to workload placement on different hosts, clusters, data centers, and even different clouds.

Cloud Migration Planning:

Migration planning shows you the capacity and cost information after the migration to a cloud-based infrastructure.

Cost Overview

vRealize Operations Cloud supports costing for private clouds, public clouds, and VMware Cloud infrastructure.

You can track expenses for a single virtual machine, and identify how these expenses attribute to the overall cost associated with your private cloud accounts and VMware Cloud infrastructure accounts.

On the Cost Overview

home page in vRealize Operations Cloud, you can find details about the costs

associated with your VMware Cloud infrastructure accounts, public cloud accounts, and your private cloud accounts.



You can view the Total Cost of Ownership, Potential Savings, and Realized Savings for your VMware Cloud infrastructure cloud accounts and vSphere private cloud accounts, and Total Cost of Ownership for your private cloud accounts.

NEW QUESTION 23

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 27

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 29

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:

- A. Connectivity the VMware Cloud on AWS environment must NOT have a single point of failure.
- B. Any network traffic between on-premises company locations must be sent over a private IP address space.
- C. Connectivity the VMware Cloud on AWS environment must support high-throughput data transfer.

Answer: A

NEW QUESTION 34

A customer needs additional capacity to handle seasonal spikes and decides to use a VMware Public cloud provider the extra capacity. Which use case describes this customer scenario?

- A. Disaster recovery
- B. Data center extension
- C. Cloud migrations
- D. Modernizing applications

Answer: B

Explanation:

This customer scenario describes a use case of extending the capacity of an existing data center with a public cloud provider, such as VMware Cloud. This allows the customer to extend their capacity to handle seasonal spikes in demand, without having to invest in additional physical infrastructure or make significant changes to their existing setup.

According to VMware's official website, "VMware Cloud enables customers to extend their data centers to the public cloud and dynamically scale capacity up or down with the same tools, processes, and policies they use today in their private cloud or data center environments." [1]

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

NEW QUESTION 39

A cloud administrator Is tasked with deploying two virtual machines (APP01 and APP02) to a software-defined data center (SDDC) with multiple clusters hosted In VMware Cloud on AWS based on the following requirements:

- APP01 and APP02 should NOT run on the same host.
- Only three hosts in the SDDC are entitled to run the software installed on these servers.

- All entitled hosts are in cluster 1.

Which two actions should the administrator take to meet these requirements? (Choose two)

- A. Create a Disable DRS vMotion policy.
- B. Create a VM-VM anti-affinity policy.
- C. Deploy APP01 to Cluster 1 and APP02 to cluster 2. a Create a VM-Host anti-affinity policy.
- D. Create a VM-Host affinity policy.

Answer: BD

Explanation:

VM-VM Anti-Affinity

A VM-VM anti-affinity policy describes a relationship between members of a category of VMs.

Use case:

When you want to place VMs running critical workloads on separate hosts so that the failure of one host does not affect other VMs in the category

Graphical user interface, text, application, email Description automatically generated

VM-Host Affinity

A VM-Host affinity policy describes a relationship between a category of VMs and a category of hosts.

Use cases:

- When host-based licensing requires that VMs running certain applications be placed on hosts that are licensed to run those applications
- When VMs with workload-specific configurations require placement on hosts that have certain characteristics

NEW QUESTION 40

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 45

A cloud administrator is managing a VMware Cloud on AWS environment. Currently, there is a single cluster consisting of four i3.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?

- 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>.

NEW QUESTION 50

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 54

Which two steps must an administrator take in order to deploy an instance of Azure VMware Solutions? (Choose two.)

- A. Create a support request with Microsoft Azure Support to create a host quota.
- B. Deploy and configure Microsoft Enterprise Edge (MSEE) appliances.
- C. Create a support request with VMware Support to create a private cloud.
- D. Associate the subscription with a Microsoft Enterprise Agreement.
- E. Deploy and Configure Microsoft Azure ExpressRoute.

Answer: AD

Explanation:

According to the VMware Cloud Professional Administration guide, to deploy an instance of Azure VMware Solutions, an administrator must first create a support request with VMware Support to create a private cloud. This will enable the administrator to access the Azure VMware Solutions environment.

The guide also states that an administrator must associate the subscription with a Microsoft Enterprise Agreement in order to use Azure VMware Solutions. This will ensure that the administrator has the necessary permissions and access to the environment in order to configure and manage it.

Search results: [1] VMware Cloud Professional is a cloud service that provides a secure, reliable, and cost-effective way to deliver cloud-based solutions for organizations. [2] This guide provides step-by-step instructions to deploy and configure Microsoft Azure VMware Solutions[1], a cloud-based solution that enables organizations to run VMware workloads in the public cloud. [3] To deploy an Azure VMware Solution instance, the customer must have an active Microsoft Enterprise Agreement (EA) and a valid subscription associated with it. [4] The customer must also create a support request with VMware support to create a private cloud. This will enable the customer to access the Azure VMware Solutions environment. [5] Once the customer has created a support request and associated their 1. Manually Creating Optimized Windows Images for VMware Horizon ...

<https://techzone.vmware.com/resource/manually-creating-optimized-windows-images-vmware-horizon-vms> VMware Technical Support Guide

<https://www.vmware.com/pdf/techsupportguide.pdf> VMware vCloud Air Networking Guide - vCloud Air

https://www.vmware.com/pdf/vchs_networking_guide.pdf

NEW QUESTION 58

A cloud administrator has a portion of its on-premises infrastructure hardware that is going to be again out of its support lifecycle later this year. Due to the regulatory requirement, the applications running on this hardware cannot be migrated to the public cloud, but the Administrator is also trying to reduce its operational expenses of managing and maintaining the hardware it owns and reduce capital expenditures. Which two solutions would achieve these goals? (Choose two.)

- A. VMware Cloud on AWS Outpost
- B. VMware Cloud on Dell EMC
- C. VMware Cloud Foundation
- D. Oracle Cloud VMware Solution
- E. VMware Cloud on AWS

Answer: BE

Explanation:

VMware Cloud on Dell EMC is a service that allows customers to deploy and manage VMware Cloud Foundation in their own data center, eliminating the need to buy and maintain their own hardware. This solution allows customers to reduce costs associated with maintaining their own hardware, as well as reduce capital expenditures by not needing to buy new hardware.

VMware Cloud on AWS is a fully managed service that allows customers to run their VMware-based workloads on the AWS Cloud. This solution allows customers to take advantage of the scalability and cost savings of the public cloud, while still being able to maintain regulatory compliance for their workloads.

According to VMware's official website, "VMware Cloud on AWS is an on-demand service that enables customers to run applications across vSphere-based cloud environments with access to a broad range of AWS services. Customers get the same architecture, features, and operational experience regardless of where you deploy applications – on-premises, in the cloud, or in a hybrid or multi-cloud configuration." [1]

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

NEW QUESTION 60

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 64

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 69

A Cloud Administrator is tasked with choosing a correct Elastic DRS policy. The existing VMware Cloud on AWS environment consists of a single cluster with two hosts.

The following guidelines regarding the expected performance must be met:

- The cluster should be able to scale automatically when additional resources are required.
- Application performance should NOT be affected when the cluster scaling operation is being performed.

Which Elastic DRS policy should the cloud administrator Select?

- A. Optimize for Best Performances
- B. Elastic DRS Baseline
- C. Optimize for Rapid Scale-Out
- D. Optimize for Lowest Cost

Answer: B

Explanation:

Based on the given guidelines, the cloud administrator should select the Elastic DRS Baseline policy[1]. This policy is designed to scale the cluster automatically when additional resources are required, while also ensuring that application performance is not affected during the scaling operation. The Elastic DRS Baseline policy also ensures that resources are allocated efficiently and optimally[1], to minimize cost while ensuring that performance requirements are met.

For more information on the Elastic DRS Baseline policy[1], see the VMware official documentation at <https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.sddc-management/GUI>

NEW QUESTION 71

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 76

A cloud administrator is asked to configure access to the VMware Cloud Services Console based on the following requirement:

• Groups and users should be synchronized from the internal Active Directory Which two options should the administrator configure to meet this requirement? (Choose two.)

- A. Workspace ONE Access connector
- B. Enterprise federation with dynamic (connectorless) authentication setup
- C. SAML 2.0 Identity Provider
- D. Enterprise federation with connector-based authentication setup
- E. Workspace ONE Assist

Answer: AC

Explanation:

The Workspace ONE Access connector is used to synchronize groups and users from the internal Active Directory to the VMware Cloud Services Console. Additionally, the administrator should configure a SAML 2.1 Identity Provider to enable single sign-on (SSO) capability and secure access to the VMware Cloud Services Console.

NEW QUESTION 77

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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](#)