VMware

Exam Questions 2V0-33.22

VMware Cloud Professional

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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. ldaps/636
B. http/80
C. https/443
D. ldap/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
With which solution is the cloud administrator interfacing when defining storage policies in a VMware Cloud software-defined data center (SDDC)?

A. VMware Virtual Volumes (vVols)
B. VMware vSAN
C. iSCSI
D. VMware Virtual Machine File System (VMFS)

Answer: B

Explanation:
VMware vSAN is a distributed storage platform that is integrated into the VMware Cloud software-defined data center (SDDC). It provides policy-based storage management, allowing cloud administrators to define storage policies that can be applied to virtual machines and other workloads. These policies govern how data is stored, replicated, and secured, and are used to ensure that data is stored in a consistent and compliant manner.
https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vsphere.vmc-aws-manage-data-cen

NEW QUESTION 3
Which VMware Cloud tool would an administrator use to forward all the monitored traffic to a network appliance for analysis and remediation?

A. vRealize Log Insight
B. Traceflow
C. Port mirroring
D. IPFIX

Answer: C

Explanation:
Port mirroring is a VMware Cloud tool that an administrator can use to forward all the monitored traffic to a network appliance for analysis and remediation. The network appliance can then analyze the mirrored traffic and take the appropriate remedial action. Port mirroring can also be used to identify and troubleshoot network issues, as well as monitor network activities.
Port mirroring lets you replicate and redirect all of the traffic coming from a source. The mirrored traffic is sent encapsulated within a Generic Routing Encapsulation (GRE) tunnel to a collector so that all of the original packet information is preserved while traversing the network to a remote destination.
Port mirroring is used in the following scenarios:
- Troubleshooting - Analyze the traffic to detect intrusion and debug and diagnose errors on a network.
- Compliance and monitoring - Forward all of the monitored traffic to a network appliance for analysis and remediation.

Port mirroring includes a source group where the data is monitored and a destination group where the collected data is copied to. The source group membership criteria require VMs to be grouped based on the workload such as web group or application group. The destination group membership criteria require VMs to be grouped based on IP addresses. Port mirroring has one enforcement point, where you can apply policy rules to your SDDC environment.
The traffic direction for port mirroring is Ingress, Egress, or Bi Directional traffic:
- Ingress is the outbound network traffic from the VM to the logical network.
- Egress is the inbound network traffic from the logical network to the VM.
- Bi Directional is the traffic from the VM to the logical network and from the logical network to the VM. This is the default option.

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

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
A cloud administrator needs to create a virtual machine that requires layer 2 connectivity to an on-premises workload. Which type of network segment Is required?

A. Existing
B. Outbound
C. Extended
D. Routed

Answer: C

Explanation:
An extended network segment is required for a cloud administrator to create a virtual machine that requires layer 2 connectivity to an on-premises workload. Extended networks allow for the virtual machines to communicate directly with the on-premises workload while remaining isolated from the public cloud. This allows for the virtual machines to access the same services and workloads as the on-premises workloads while still remaining secure.

NEW QUESTION 7
Which two components are required in order to deploy a Tanzu Kubernetes Grid Cluster in VMware Could 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-deploym

NEW QUESTION 8
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 9
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-componentsNode 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 10
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 10
Which three factors should a cloud administrator consider when sizing a new VMware Cloud software-defined data center (SDDC) to support the migration of workloads from an on-premises SDDC? (Choose three.)

A. Total number of 10Gb network ports required
B. Host hardware type in the target VMware Cloud
C. Total number of on-premises hosts
D. Total number of workloads
E. Total amount of available storage across all on-premises datastores
F. Average size of workload resources (CPU & RAM)

Answer: DEF

Explanation:
- Total number of workloads. This determines how many hosts are needed in the VMware Cloud SDDC cluster.
- Total amount of available storage across all on-premises datastores. This determines how much storage capacity is needed in the VMware Cloud SDDC cluster.
- Average size of workload resources (CPU & RAM). This determines how much compute capacity is needed in the VMware Cloud SDDC cluster.

https://docs.vmware.com/en/VMware-Cloud/services/vmc-cloud-sizer-user/GUID-7CECF719-E56B-4830-84E

NEW QUESTION 13
A cloud administrator wants to migrate a virtual machine using VMware vSphere vMotlon 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 Require 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 centerwith 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 15
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 16
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 21
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 heroe.r is encount

NEW QUESTION 26
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 30
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 32
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 35
How is a Tanzu Kubernetes cluster deployed in a VMware Cloud environment?

A. Using the VMware Cloud Console
B. Using VMware Tanzu Mission Control
C. Using the standard open-source kubectl
D. Using the vSphere PlugIn for kubectl

Answer: A

Explanation:
Tanzu Kubernetes clusters can be deployed in a VMware Cloud environment using the VMware Cloud Console. The VMware Cloud Console provides a user-friendly interface that allows users to quickly deploy and manage Tanzu Kubernetes clusters. The standard open-source kubectl can also be used to deploy Tanzu Kubernetes clusters. However, this requires a more in-depth knowledge of the kubectl command-line interface. Additionally, users can use the vSphere Plugin for kubectl to deploy and manage Tanzu Kubernetes clusters. This plugin provides a graphical user interface to manage the clusters, as well as additional features such as the ability to make cluster-level changes

NEW QUESTION 39
Refer to the exhibit.

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 fall?

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-o 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 42
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 44
A cloud administrator needs to create an isolated network segment for use in disaster recovery test. Which type of network segment is required?

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

Answer: A

Explanation:
A private network segment is an isolated network segment that is used for disaster recovery testing. Private network segments provide a secure and isolated environment for testing, allowing administrators to test their disaster recovery plans without risking the stability of their production environment. Private network segments also provide additional security, as they are not connected to the public internet, making them less vulnerable to external attacks. [1]
[1]https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.networking/GUID-64

NEW QUESTION 47
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 49
If a company connects their data center to a VMware Cloud on AWS software-defined data center (SDDC) Instance through a virtual private network (VPN) and advertises a 0.0.0.0/0 route, what Is the expected behavior of the SDDC compute network traffic?

A. All compute and management traffic will egress to the data center.
B. All compute network traffic destined for the data center will egress through the VPN but all Internet traffic will egress through the cloud provider Internet gateway.
C. All compute network traffic will egress through the cloud provider Internet gateway.
D. All compute network traffic will egress to the data center.

Answer: D

Explanation:
When a VPN is established between the data center and the SDDC Instance, it allows the organization to create a private and secure connection between their on-premises infrastructure and their workloads running in the cloud. By advertising a 0.0.0.0/0 route, the organization is essentially routing all traffic to the VPN tunnel, which means that all traffic including traffic destinedfor the data center and internet traffic, will be sent through the VPN tunnel to the company's data center.
It is important to note that this configuration depends on the company's network architecture and security policies, and that there may be other alternatives that better fit the organization's needs.

NEW QUESTION 51
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 55
A cloud administrator is managing a container environment. The application team has complained that they need to manually restart containers in the event of a failure.
Which solution can the administrator implement to solve this issue?

A. Kubernetes
B. VMware vSphere High Availability
C. VMware vSphere Fault Tolerance
D. Prometheus

Answer: A

Explanation:
Kubernetes is an open-source container orchestration system that provides automated deployment, scaling, and management of containers. It can be used to set up an automated restart policy for containers in the event of a failure, ensuring that containers are automatically restarted when they fail.
VMware Stage Manager User's Guide https://www.vmware.com/pdf/stagemanager1_Users_Guide.pdf

NEW QUESTION 58
Given what you know about cloud, which examples illustrate its benefits? Select all options that apply.

A. An organization requires fewer developers when it uses the cloud.
B. An organization manages its cloud resources by using different cloud providers that areseparate and isolated from each other.
C. A business stores infrequently accessed data in the cloud to benefit from reduced on-premises storage costs.
D. An organization manages its cloud resources by using different cloud providers that are separate and isolated from each other.
E. A developer codes an application in a cloud-based environment, and, with a few simple commands, deploys the application on the business website.
F. In seconds, you receive a large amount of storage using a cloud option.

Answer: BCEF

Explanation:
Example B illustrates the benefit of cloud computing where an organization can manage its cloud resources by using different cloud providers that are separate and isolated from each other. This allows the organization to make use of features and services offered by different cloud providers in order to benefit from the best of different services.
Example C illustrates the benefit of cloud computing where a business can store infrequently accessed data in the cloud in order to benefit from reduced on-premises storage costs, as cloud storage is usually cheaper than on-premise storage.
Example E illustrates the benefit of cloud computing where a developer can code an application in a
cloud-based environment, and, with a few simple commands, deploy the application on the business website. This eliminates the need for the developer to set up and manage the application on their own, as the cloud platform handles the deployment and hosting of the application.
Example F illustrates the benefit of cloud computing where a large amount of storage can be made available in seconds using a cloud option. This is useful for businesses that require a large amount of storage but don't have the resources to set up and manage their own storage solution.
For more information on the benefits of cloud computing, see the VMware official documentation athttps://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.getting-started/GUID-F

NEW QUESTION 63
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 65
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 70
A cloud administrator wants to deploy a VMware Cloud software-defined data center (SDDC) ona 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 71
A cloud administrator is managing a VMware Cloud on AWS environment. Currently, there Is a single cluster consisting of four 13.metal hosts. Due to an increased demand, cluster capacity has to be expanded by 60 cores and 640 GB of memory.
What should the administrator do to meet the demand?

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 73
On VMware Cloud on AWS, which type of host do you use when you require high local storage requirements and additional cores for your workloads? (Select one option)

A. ve-standard-72
B. i3e
C. metal
D. i3.metal
E. AV36

Answer: C

Explanation:
when you require high local storage requirements and additional cores for your workloads on VMware Cloud on AWS. i3.metal instances offer up to 4TB of local NVMe storage and up to 96 CPU cores, giving you the power and storage you need to handle large workloads. Additionally, i3.metal instances are great for applications that benefit from high CPU-to-memory ratios, like artificial intelligence, machine learning, big data analysis, and HPC workloads.

NEW QUESTION 74
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 79
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 80
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 82
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

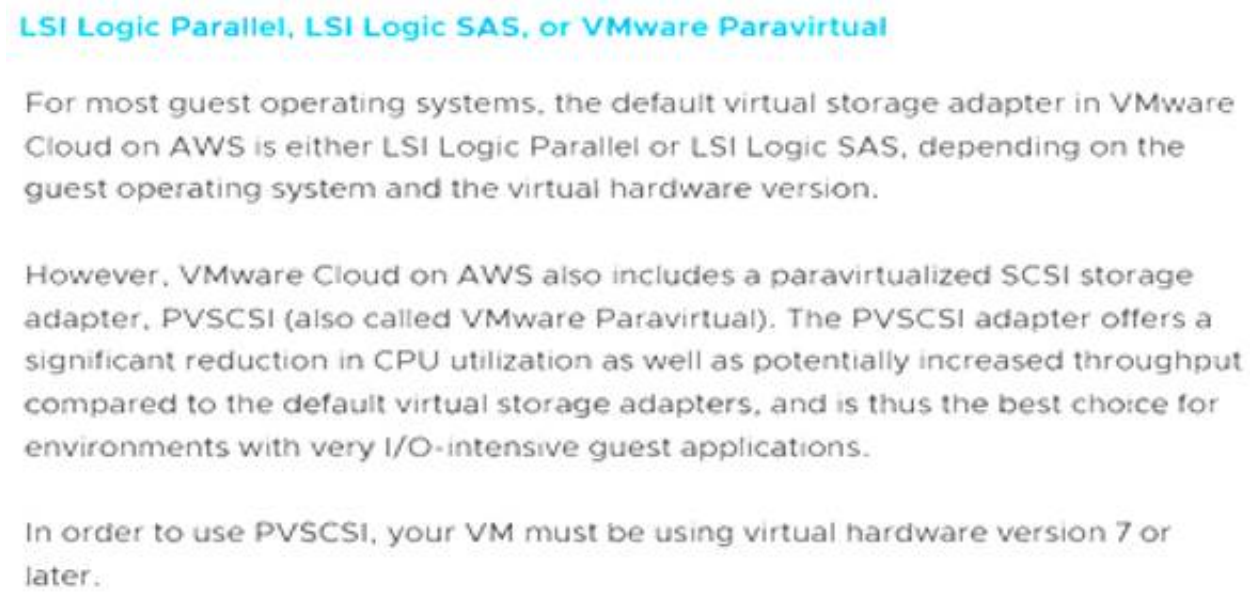
NEW QUESTION 86
A cloud administrator is responsible for managing a VMware Cloud solution and would like to ensure that I/O-intensive workloads run in the most optimum way possible.
Which two steps should the administrator complete on I/O-intensive workloads to meet this requirement? (Choose two.)

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



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

NEW QUESTION 87
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 90
An administrator wants to have a global view of all managed Tanzu Kubernetes clusters and manage the policies across them. Which solution would the administrator use?

A. VMware Tanzu Mission Control
B. VMware Tanzu Observability by Wavefront
C. VMware Tanzu Service Mesh
D. VMware Tanzu Kubernetes Grid

Answer: A

Explanation:
VMware Tanzu Mission Control provides a central platform to manage and view all Tanzu Kubernetes clusters and workloads running in the environment. It allows administrators to set policies across multiple clusters, set up cluster identities, monitor cluster health and performance, and much more. Tanzu Mission Control also provides access to a variety of cloud-native tools, such as Kubernetes Dashboard, Helm, and Kubeapps.
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 Tanzu® Mission ControlTM is a centralized management platform for consistently operating,
managing, and securing Kubernetes infrastructure and modern applications across teams and clouds. It provides a global view of all of the Kubernetes clusters.
You can use the resource hierarchy to manage and enforce consistent policies across Kubernetes clusters. "

NEW QUESTION 92
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 93
A cloud administrator is planning to migrate 1,000 VMs from their existing on-premises location into VMware Cloud on AWS. The migration will need to be completed as quickly as possible. Upon completion, the users will need the most reliable, lowest latency connection possible.
Which on-premises data center connectivity option will meet these requirements?

A. Layer 2 VPN
B. AWS Direct Connect
C. VMware Transit Connect
D. IPsec VPN

Answer: B

Explanation:
The best option to meet the requirements of quickly migrating 1,000 VMs with the lowest latency and most reliable connection possible is to use AWS Direct Connect. AWS Direct Connect provides a dedicated network connection between an on-premises data center and the Amazon Web Services (AWS) cloud, allowing for the transfer of data across the two locations. It is more reliable and has lower latency than other options such as Layer 2 VPN, VMware Transit Connect, and IPsec VPN. Additionally, AWS Direct Connect provides the highest performance and throughput of any of the on-premises data center connectivity options.
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

NEW QUESTION 96
A cloud administrator is asked to validate a proposed internetworking design that will provide connectivity to a VMware Cloud on AWS environment from multiple company locations.
The following requirements must be met:
• Connectivity to the VMware Cloud on AWS environment must support high-throughput data transfer.
• Connectivity to the VMware Cloud on AWS environment must NOT have a single point of failure.
• Any network traffic between on-premises company locations must be sent over a private IP address space. Which design decisions should be made to meet these network connectivity requirements?

A. • Configure a Direct Connect from headquarters to VMware Cloud on AWS.• Use a private VIF for this connection.• Configure a secondary, standby Direct Connect from headquarters using a public VIF.• Configure dual, redundant, policy-based IPsec VPN connections from each regional office to VMware Cloud on AWS.
B. • Configure a Direct Connect from headquarters to VMware Cloud on AWS.• Use a public VIF for this connection.• Configure a route-based IPsec VPN tunnel as a secondary method of connectivity from headquarters to VMware Cloud on AWS.• Configure dual, redundant, route-based IPsec VPN connections from each regional office to VMware Cloud on AWS.
C. • Configure a Direct Connect from headquarters to VMware Cloud on AWS.• Use a private VIF for this connection.• Configure a route-based IPsec VPN tunnel as a secondary method of connectivity from headquarters to VMware Cloud on AWS, taking care to enable the "Use VPN as Backup to Direct Connect" option.• Configure dual, redundant, route-based IPsec VPN connections from each regional office to VMware Cloud on AWS.
D. • Configure a Direct Connect from headquarters to VMware Cloud on AWS.• Use a private VIF for this connection.• Configure a policy-based IPsec VPN tunnel as a secondary method of connectivity from headquarters to VMware Cloud on AWS, taking care to enable the "Use VPN as Backup to Direct Connect" option.• Configure dual, redundant, policy-based IPsec VPN connections from each regional office to VMware Cloud on AWS.

Answer: C

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

NEW QUESTION 98
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 103
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 scalingoperation. 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 athttps://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.sddc-management/GUI

NEW QUESTION 106
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 110
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 114
.....

Relate Links

100% Pass Your 2V0-33.22 Exam with Exambible Prep Materials

https://www.exambible.com/2V0-33.22-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/