

2V0-33.22 Dumps

VMware Cloud Professional

<https://www.certleader.com/2V0-33.22-dumps.html>



NEW QUESTION 1

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

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

- A. CloudAdmin role and global permissions
- B. CloudAdmin role on the Development folder
- C. Administrator role on the Development folder
- D. Administrator role on the cloud vCenter Server instance

Answer: B

Explanation:

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

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

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

NEW QUESTION 2

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

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

- A. 10.4.0.0/23
- B. 10.3.0.0/24
- C. 10.2.0.0/16
- D. 10.1.0.0/20

Answer: D

Explanation:

A valid management network CIDR based on the requirements is 10.1.0.0/20, as this provides a range of 4096 IP addresses, which is more than enough for 30 hosts. A /23 CIDR only provides 512 IP addresses, which is not enough for 30 hosts, while a /24 CIDR provides 256 IP addresses and a /16 CIDR provides 65,536 IP addresses, which is more than is needed for the 30 hosts.

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

NEW QUESTION 3

Which two use cases can be met with VMware Cloud on Dell EMC and VMware Cloud on AWS Outposts? (Choose two.)

- A. Administrator rights in SDDC Manager to configure and operate the solution
- B. Ability to create public services
- C. Applications needing local data processing and/or low latency integrations
- D. Critical workloads that use restricted data
- E. On demand rapid scalability

Answer: CD

Explanation:

The two use cases that can be met with VMware Cloud on Dell EMC and VMware Cloud on AWS Outposts are Option C: Applications needing local data processing and/or low latency integrations, and Option D: Critical workloads that use restricted data.

VMware Cloud on Dell EMC and VMware Cloud on AWS Outposts both provide local data processing and low latency integrations, making them ideal for applications that require quick and efficient access to data. Additionally, the highly secure infrastructure of both solutions make them a great choice for critical workloads that use restricted data.

For more information, please refer to the official VMware documentation on VMware Cloud on Dell EMC:<https://www.vmware.com/products/vmware-cloud-on-dellemc.html> And the official VMware documentation on VMware Cloud on AWS

Outposts:<https://www.vmware.com/products/vmware-cloud-on-aws-outposts.html>

NEW QUESTION 4

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

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

Answer: CEF

Explanation:

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

the datastore be available to both hosts and that the datastore has the same name on both hosts.

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

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

The CPU instruction set required by the VM and the vGPU configuration of the VM are not items to consider when performing a hot migration of a virtual machine.

The source and destination host management network IP address families do not need to match for the hot migration to be successful.

References:

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

NEW QUESTION 5

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 6

A cloud administrator requires an external secure connection into their data center to use Border Gateway Protocol (BGP). Which connection type can they use to connect to an Instance of VMware Cloud?

- A. Policy-based virtual private network (VPN)
- B. Public IPs over the Internet
- C. Private L2 virtual private network (VPN)
- D. Route-based virtual private network (VPN)

Answer: D

Explanation:

<https://docs.vmware.com/en/VMware-Cloud-Disaster-Recovery/services/vmware-cloud-dr-security-best-practic> A cloud administrator requires an external secure connection into their data center to use Border Gateway Protocol (BGP). The best connection type to use for this purpose is a Route-based virtual private network (VPN). This type of VPN is secure, as it uses encryption and authentication to protect the data transmitted over the connection. Additionally, it allows for the configuration of BGP to ensure that the data traffic is routed to the desired destination.

PREPARING FOR VMWARE CLOUD ON AWS

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vmc-aws/preparing-for-vmwar>

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

What is Network Virtualization? | VMware Glossary

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

NEW QUESTION 7

What are two key benefits of VMware's partnerships with hyperscalers? (Choose two.)

- A. Access to native public cloud services
- B. Automation of infrastructure operations in a single view
- C. Seamless workload migration across clouds
- D. One-click conversion to cloud native services
- E. Elimination of egress costs

Answer: AC

Explanation:

VMware's partnerships with hyperscalers, such as AWS and Google Cloud, provide customers with access to native public cloud services and the ability to easily and securely migrate workloads between clouds. This allows customers to take advantage of the best features of each cloud provider while managing their workloads in a single view. It also eliminates the need to pay egress costs when moving workloads between clouds.

NEW QUESTION 8

An organization is running multiple applications that span different public clouds. The cloud administrator is asked to perform budget management, cost reporting and cost forecasting from a single platform.

Which VMware Cloud service can the cloud administrator use to meet this requirement?

- A. VMware vRealize Operations Cloud
- B. VMware vRealize Network Insight Cloud

- C. VMware vRealize Log Insight Cloud
- D. CloudHealth by VMware

Answer: D

Explanation:

CloudHealth by VMware is a cloud cost governance platform that provides budget management, cost reporting, and cost forecasting from a single platform. It provides comprehensive visibility and control to manage cloud costs in hybrid and multi-cloud environments. CloudHealth by VMware also provides cost optimization, resource optimization, and real-time alerting capabilities to help organizations make cost-effective decisions to reduce cloud costs.

NEW QUESTION 9

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

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

Answer: C

Explanation:

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

NEW QUESTION 10

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 10

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

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

Answer: C

Explanation:

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

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

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

NEW QUESTION 13

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 15

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 are separate 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 at <https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.getting-started/GUID-F>

NEW QUESTION 19

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

- A. Capacity management of the cloud software-defined data centers (SDDCs)
- B. Updates to VMware hardware compatibility
- C. Notifications sent before a regular update
- D. Updates to the software-defined data center (SDDC) software
- E. Creation and configuration of VPC during the software-defined data center (SDDC) deployment

Answer: AD

Explanation:

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

NEW QUESTION 24

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

Which solution can accomplish this goal?

- A. VMware Site Recovery Manager
- B. VMware vRealize Network Insight
- C. VMware NSX
- D. VMware Cloud Director

Answer: C

Explanation:

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

NEW QUESTION 29

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

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

Answer: C

Explanation:

A key driver behind the multi-cloud journey is digital transformation, which is the process of using technology to optimize existing processes and systems in order to improve customer experiences, increase operational efficiency, and accelerate business growth. Multi-cloud solutions can help organizations modernize their applications and services, reduce costs, increase agility, and support digital transformation initiatives. For more information, please refer to the official VMware Cloud on AWS documentation at: <https://docs.vmware.com/en/VMware-Cloud-on-AWS/index.html>.

NEW QUESTION 33

Refer to the exhibit.



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

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 35

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 37

A cloud administrator is managing a VMware Cloud on AWS environment containing of a single cluster with three hosts. Which acts recovery site for the on-premises environment. The on-premises environment consists of eight hosts. what should the cloud administrator configure to optimize scaling for full disaster recovery?

- A. Configure an Elastic DRS policy and set the maximum cluster Size to 8.
- B. No Additional configuration is required Default Elastic DRS will fulfill the requirement
- C. Configure an Elastic DRS policy and select 'Optimize for Rapid scale-out'.
- D. Configure an Elastic DRS policy and set minimum cluster size to 8.

Answer: C

Explanation:

According to the VMware official documentation, in order to optimize scaling for full disaster recovery in a VMware Cloud on AWS environment, it is necessary to configure an Elastic DRS policy and select 'Optimize for Rapid scale-out' as the policy type. This option allows for a rapid increase in the number of hosts within the cluster, which is necessary for full disaster recovery. For more information, please refer to the VMware Cloud on AWS Disaster Recovery Guide, which can be found

here: <https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/VMware-Cloud-on-AWS-Disaster-Recover>

NEW QUESTION 38

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 43

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 47

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

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

Answer: D

Explanation:

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

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

NEW QUESTION 49

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

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

Answer: B

Explanation:

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

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

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

NEW QUESTION 54

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 59

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 60

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 63

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

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

Answer: ACF

Explanation:

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

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

NEW QUESTION 65

What is a benefit of public cloud computing?

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

Answer: D

Explanation:

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

NEW QUESTION 69

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 73

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 78

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 2V0-33.22 Exam with Our Prep Materials Via below:

<https://www.certleader.com/2V0-33.22-dumps.html>