

VMware.2V0-33.22.vJun-2024.by.Rien.85q

Number: 2V0-33.22
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: 2V0-33.22
Exam Name: VMware Cloud Professional



Exam A

QUESTION 1

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

Correct Answer: B

Section:

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/GUID-FDD3A8AC-E42C-4B92-9C1D-8EB49D6C7129.htm>

QUESTION 2

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

Correct Answer: A, C, F

Section:

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-F86D6A1F-9985-4F29-9D56-F92600B2D48A.html>

[2] <https://docs.vmware.com/en/VMware-NSX-T/services/nsxt-admin-guide.html>

[3] <https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.networking/GUID-D2E2F9A9-8661-4BDB-A8A8-4D4F4F7C4E1A.htm>

QUESTION 3

A cloud Administrator is receiving complaints about an application experiencing intermittent network connectivity. Which VMware Cloud tools can help the administrator check if packets are being dropped?

- A. VRealize Log Insight

- B. Port mirroring
- C. IPFIX
- D. Traceflow

Correct Answer: D

Section:

Explanation:

IPFIX (Internet Protocol Flow Information Export) is a standard for the format and export of network flow information for troubleshooting, auditing, or collecting analytics information. 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. Use Traceflow to inspect the path of a packet. Traceflow traces the transport node-level path of a packet. The trace packet traverses the logical switch overlay, but is not visible to interfaces attached to the logical switch. In other words, no packet is actually delivered to the test packet's intended recipients. vRealize Log Insight is a log collection and analytics virtual appliance that enables administrators to collect, view, manage and analyze syslog data. Log Insight provides real-time monitoring of application logs, network traces, configuration files, messages and performance data.

QUESTION 4

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.

Correct Answer: A, C

Section:

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. Reference: <https://docs.vmware.com/en/VMware-Site-Recovery/index.html> In order to protect a VMware Cloud on AWS software-defined data center (SDDC) with VMware Site Recovery [1][2], a cloud administrator needs to take the following two steps: A) Deploy the vSphere Replication virtual appliance - This can be done by logging into the vSphere Client, navigating to the vCenter Server, and then selecting the Deploy OVF Template option. From here, the cloud administrator can upload the OVF template for the vSphere Replication appliance and configure it. B) Connect the Site Recovery manager instance on the protected recovery site - This involves logging into the Site Recovery Manager (SRM) and setting up the connection between the protected recovery site and the SRM instance. This can be done by going to the SRM dashboard and then selecting the Connect Remote Site option.

Reference:

[1] <https://docs.vmware.com/en/VMware-Site-Recovery/services/vmc-dr-deployment/GUID-DBF6CD69-6F7E-47E2-9417-91D5C5F5AC5E.html>

[2] <https://docs.vmware.com/en/VMware-Site-Recovery/services/vmc-dr-deployment/GUID-1C8B7BCA-D4BE-4EAF-9A8A-4B42E2B7236A.html>

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.

Correct Answer: B, D

Section:



Explanation:

(Reference: <https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vcloud.admin.doc/GUID-3568D3B3-ACFE-41F1-A966-5D4784F8A7A0.html>) 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. Reference: [1] <https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/VMware-Cloud-on-AWS-Outposts/GUID-access.html>

QUESTION 6

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.

Correct Answer: C

Section:

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-Recovery-Guide.html>.

QUESTION 7

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

Correct Answer: C, D

Section:

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>

QUESTION 8

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

Correct Answer: A

Section:

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.

QUESTION 9

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

Correct Answer: B

Section:

Explanation:

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



QUESTION 10

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

Correct Answer: C

Section:

Explanation:

According to the VMware official site, the requirements for a VMware HCX deployment are a minimum of 30 vCPUs and 36GB of memory on the on-premises environment. This is outlined in the VMware HCX - Technical Overview and Sizing Guide, which can be found here:<https://docs.vmware.com/en/VMware-HCX/services/HCX-Technical-Overview-and-Sizing-Guide.html>. This document also outlines the minimum requirements for the HCX Manager, HCX-IX Interconnect, HCX Network Extension, and HCX WAN Optimization components, which are 4 vCPUs, 128GB of memory, 8 vCPUs, 3GB of memory, 8 vCPUs, 3GB of memory, and 8 vCPUs, 14GB of memory respectively.

QUESTION 11

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

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

- D. Capacity management
- E. Workload OS management

Correct Answer: B, D

Section:

Explanation:

The two incident management services included in the VMware Cloud on AWS Service Management process are Incident Management and Capacity Management. Incident Management is responsible for detecting, classifying, and resolving incidents quickly and effectively. It includes monitoring and alerting, incident response, and problem management. Capacity Management is responsible for predicting, measuring, and managing the capacity of the infrastructure. It includes capacity planning, performance analysis, and resource optimization. Reference:

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

[2] <https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.admin.doc/GUID-684D1A84-C57F-4EC1-8A18-7A9A9EB9B7FF.html>

QUESTION 12

Exhibit:

NEW FOLDER UPLOAD FILES UPLOAD FOLDERS REGISTERED VM DOWNLOAD DATE COPY to MOVE TO RENAME TO DELETE

Name	Size	Modified	Type	Path
------	------	----------	------	------

dvsData	05/03/2022, 9.10.21 AM	Folder	[vsandatastore]
---------	------------------------	--------	-----------------

.sdd.sf	05/03/2022, 9.10.21 AM	Folder	[vsandatastore]
---------	------------------------	--------	-----------------

app02-000002.vmdk	05/03/2022, 9.10.21 AM	Folder	[vsandatastore]
-------------------	------------------------	--------	-----------------

app02-000003.vmdk	05/03/2022, 9.10.21 AM	Folder	[vsandatastore]
-------------------	------------------------	--------	-----------------

app02-000002.hlog	05/03/2022, 9.10.21 AM	Folder	[vsandatastore]
-------------------	------------------------	--------	-----------------

app02-000002.vswap	05/03/2022, 9.10.21 AM	Folder	[vsandatastore]
--------------------	------------------------	--------	-----------------

app02-000002.vswap.lck	05/03/2022, 9.10.21 AM	Folder	[vsandatastore]
------------------------	------------------------	--------	-----------------

A cloud administrator is asked to troubleshoot a virtual machine (app02) that is performing slowly.

The cloud Administrator noticed that app02 is consuming an expected amount of disk space. As a first step, the cloud administrator uses VMware vCenter to check the snapshot manager for app02 and no snapshot -- cloud administrator then navigates to the app02 files on the datastore, and is presented with the information provided in the exhibits. Given the information provided, which task should the cloud administrator perform to resolve this issue?

- A. Migrate the virtual machine to a new datastore.
- B. Perform a snapshot consolidation.
- C. Power cycle the virtual machine.
- D. Execute a Delete All Snapshots task.

Correct Answer: D

Section:

QUESTION 13

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.

Correct Answer: B, C, E, F

Section:

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-F0A2F338-A6A7-49AD-B158-CFFCA2F29C1B.html>.

QUESTION 14

A cloud administrator is managing a VMware Cloud on AWS environment connected to an on-premises data center using IPSec VPN connection. The administrator is informed of performance issues with applications replicating data between VMware Cloud and the on-premises data center.

The total bandwidth used by this replication is 3.8 Gbps.

What should the administrator do to improve application performance?

- A. Deploy VMware HCX.
- B. Deploy AWS Direct Connect.
- C. Deploy a layer 2 VPN connection.
- D. Contact VMware support to request more bandwidth for IPSec VPN connection.

Correct Answer: A

Section:

Explanation:

The best solution for improving application performance in this situation is to deploy VMware HCX. VMware HCX provides efficient replication and data mobility between VMware Cloud on AWS and the on-premises data center. It also provides advanced traffic engineering capabilities, which allows the administrator to shape the traffic and prioritize applications based on the needs. This will help ensure that the replication traffic does not impact the performance of other applications. Additionally, VMware HCX supports a much larger bandwidth than an IPSec VPN connection, so it can provide a more reliable connection for replicating larger amounts of data. For more information about deploying VMware HCX, please refer to the official VMware documentation: <https://docs.vmware.com/en/VMware-HCX/index.html>.

QUESTION 15

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)

Correct Answer: B

Section:

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.

QUESTION 16

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

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

D. 100 milliseconds round trip

Correct Answer: D

Section:

Explanation:

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

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vsphere.vmc-aws-manage-data-center-vms.doc/GUID-BE75F0F1-2864-4926-97FE-37E635471C43.html>

QUESTION 17

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

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

Correct Answer: B

Section:

Explanation:

According to the VMware documentation you provided, it is possible to change a VM storage policy for an ISO image by modifying the default VM storage policy. To change the storage policy for an ISO image, the administrator can follow these steps: Go to the vSphere Web Client and navigate to the ISO image in question. Right-click the ISO image and select "Manage" > "Storage Policies". Select a new storage policy from the list or create a new policy. Click on the "Change Policy" button to apply the new storage policy to the ISO image. It's important to note that when you modify the default storage policy, all new files created after the change will be created with the new storage policy. However, this change doesn't affect the existing files that were created with the previous default storage policy. Please accept my apologies for any confusion caused by my previous response.

QUESTION 18

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

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

Correct Answer: C, D, F, G

Section:

Explanation:

Planning for the Deployment: During the planning process, you take the following steps to identify and gather information needed for your deployment: Identify the subscription that you plan to use to deploy Azure VMware Solution. Identify the resource group that you want to use for your deployment. Identify the region in which you want Azure VMware Solution deployed. Define the resource name for your Azure VMware Solution private cloud. Identify the size of the hosts that you want to use when deploying Azure VMware Solution. Define the number of hosts that you want to deploy to the first cluster for your deployment. Request a host quota (capacity) early so that you will be ready to deploy your Azure VMware Solution private cloud. Identify the /22 CIDR IP segment for your private cloud management. Define the IP address network segment for your VM workloads. Define the virtual network gateway. Define VMware HCX[®] network segments.

Reference: <https://learn.microsoft.com/en-us/azure/azure-vmware/deploy-azure-vmware-solution?tabs=azure-portal>

QUESTION 19

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.

Correct Answer: A, D, E

Section:

Explanation:

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

QUESTION 20

Which Tanzu Kubernetes Grid component is used to create, scale, upgrade and delete workload clusters?

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

Correct Answer: B

Section:

Explanation:

<https://docs.vmware.com/en/VMware-vSphere/7.0/vmware-vsphere-with-tanzu/GUID-4D0D375F-C001-4F1D-AAB1-1789C5577A94.html>Tanzu CLI is a command-line interface used to create, scale, upgrade, and delete workload clusters that are part of the Tanzu Kubernetes Grid [1]. Tanzu CLI also allows you to manage the components of the Tanzu Kubernetes Grid [1], such as the Tanzu Kubernetes cluster and the Tanzu Supervisor cluster. It also provides access to the Tanzu Kubernetes Grid extensions [1], which allow you to extend the functionality of the Tanzu Kubernetes cluster.



QUESTION 21

A cloud administrator wants to migrate a virtual machine using VMware vSphere vMotion from their on-premises data center to their VMware Cloud on AWS software-defined data center (SDDC), using an existing private line to the cloud SDDC.

Which two requirements must be met before the migration can occur? (Choose two.)

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

Correct Answer: C, D

Section:

Explanation:

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-operations/GUID-1A175E91-2317-4261-A63E-B398D92ECE8D.html> vMotion Requirements for SDDCs With NSX: Networking speed and latency: Migration with vMotion requires sustained minimum bandwidth of 250 Mbps between source and destination vMotion vMkernel interfaces, and a maximum latency of 100 ms round trip between source and destination. On-premises vSphere version: Your on-premises vSphere installation must be vSphere 6.7U2 or higher. See VMware Knowledge Base article 56991 for more information. On-premises DVS version: 6.0 or higher. On-premises NSX version: any Note: SDDCs configured with NSX do not support hot vMotion to or from on-premises VXLAN encapsulated networks (NSX for vSphere) or Geneve Datacenter Overlay networks (NSX). IPsec VPN: Configure an IPsec VPN for the management gateway. See Configure a VPN

Connection Between Your SDDC and On-Premises Data Center in the VMware Cloud on AWS Networking and Security guide. Direct Connect: Direct Connect over a private virtual interface between your on-premise data center and your VMware Cloud on AWS SDDC is required for migration with vMotion. See Using AWS Direct Connect with VMware Cloud on AWS. Hybrid Linked Mode: Hybrid Linked Mode is required to initiate migration from the vSphere Client. It is not required to initiate migration using the API or PowerCLI. See "Hybrid Linked Mode" in Managing the VMware Cloud on AWS Data Center. L2 VPN: Configure a Layer 2 VPN to extend virtual machine networks between your on-premises data center and cloud SDDC. Routed networks are not supported. See VMware Cloud on AWS Networking and Security. VMware Cloud on AWS firewall rules Ensure that you have created the necessary firewall rules as described in Required Firewall Rules for vMotion. On-premises firewall rules: Ensure that you have created the necessary firewall rules as described in Required Firewall Rules for vMotion. Virtual machine hardware and settings: Ensure that these requirements are met for virtual machine hardware. Virtual machine hardware version 9 or later is required for migration with vMotion from the on-premises data center to the cloud SDDC. EVC is not supported in the VMware Cloud on AWS SDDC. VMs that are created in the cloud SDDC or that have been power-cycled after migration to the cloud SDDC can't be migrated back to the on-premises data center with vMotion unless the on-premises EVC baseline is Broadwell. You can relocate these VMs after powering them off, as long as their virtual machine hardware version is compatible with the on-premises data center. Migration of VMs with DRS or HA VM overrides is not supported. For more information on VM overrides, see Customize an Individual Virtual Machine. Important: Source switch configurations (including NIOC, spoofguard, distributed firewall, and Switch Security) and runtime state are not applied at the destination as part of migration in either direction. Before you initiate vMotion, apply the source switch configuration to the destination network. In order for a virtual machine to be migrated using VMware vSphere vMotion, the versions of VMware vSphere need to match between the on-premises data center and the cloud SDDC, and a Layer 2 connection needs to be configured between them. Additionally, cluster-level Enhanced vMotion Compatibility (EVC) must be configured in both the on-premises data center and the cloud SDDC. IPsec VPN and AWS Direct Connect do not need to be configured for the migration to occur.

QUESTION 22

A company needs to increase its infrastructure capacity quickly to accommodate their rapid business growth. Which cloud use case describes their requirement?

- A. Maintain and Modernize
- B. Consolidate and Migrate
- C. Disaster Recovery
- D. Maintain and Expand

Correct Answer: A

Section:

Explanation:

<https://www.vmware.com/mena/topics/glossary/content/digital-transformation.html>



QUESTION 23

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

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

Correct Answer: B

Section:

Explanation:

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

QUESTION 24

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

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

Correct Answer: B

Section:

Explanation:

<https://www.vmware.com/topics/glossary/content/multi-cloud.html>VMware Multi-Cloud provides visibility and tools to manage resources, workloads and operations across clouds from a common operating environment. This eliminates the need to manage multiple cloud environments in different clouds and provides a unified view of all cloud resources and applications. This makes it easier to monitor and manage workloads across clouds, reducing complexity and increasing agility. VMware Multi-Cloud also provides powerful automation and orchestration capabilities to help streamline operations and improve efficiency. [1][1] <https://www.vmware.com/products/vmware-multi-cloud.html>

QUESTION 25

A customer is looking to leverage a VMware Public Cloud solution to provide them with additional compute capacity as seasonal demand increases for their online business. The current on-premises data center is configured as follows:

- VMware vSphere 7.0
- VMware vSphere Distributed Switch (vDS) 7.0
- Management and Server network - 172.18.0.0/16
- vMotion network - 192.168.120.0/24
- 250 application servers

Given the information in the scenario, which capability of VMware HCX will the customer not be able to utilize?

- A. Cold migration
- B. Layer 2 extension
- C. Bulk migration
- D. WAN optimization

Correct Answer: B

Section:

QUESTION 26

Refer to the exhibit.



The screenshot shows the AWS console interface for configuring a VPC and subnet. The first step, 'VPC and subnet', involves selecting a VPC and a subnet from an existing AWS account. The second step, 'Configure Network', involves configuring a management subnet (optional) with a private IP range (192.168.0.0/16) and a CIDR block (10.0.0.0/24).

A cloud administrator is deploying a new VMware Cloud on AWS virtual private cloud (VPC). After clicking on deploy, the screen refreshes and displays the information that is provided in the exhibit. What is the issue with the management CIDR that is causing the deployment to fail?

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

Correct Answer: A

Section:

Explanation:

<https://docs.aws.amazon.com/whitepapers/latest/sddc-deployment-and-best-practices/deployingvmware-cloud-on-aws-sddc.html>

This 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.

QUESTION 27

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.

Correct Answer: A, D

Section:

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.

QUESTION 28

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

Correct Answer: A

Section:

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. <https://vcdx.vmware.com/content/dam/digitalmarketing/vmware/ru/pdf/techpaper/vmware-horizon-7-application-publishing.pdf> Publishing Applications with VMware Horizon 7 <https://vcdx.vmware.com/content/dam/digitalmarketing/vmware/ru/pdf/techpaper/vmware-horizon-7-application-publishing.pdf> <https://www.vmware.com/pdf/techsupportguide.pdf> VMware Technical Support Guide <https://www.vmware.com/pdf/techsupportguide.pdf> <https://techzone.vmware.com/resource/quick-start-tutorial-vmware-dynamic-environment->



QUESTION 29

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

The following requirements must be met:

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

Which solution would meet these requirements?

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

Correct Answer: A

Section:

Explanation:

VMware Cloud Disaster Recovery is a managed disaster recovery-as-a-service offering that is built on the latest version of VMware vSphere 7.0. It provides an on-demand cloud consumption model, allowing administrators to rapidly power-on recovered virtual machines in the cloud, assuming cloud capacity availability. Additionally, VMware Cloud Disaster Recovery delivers a recovery point objective (RPO) of no more than 30 minutes, and can accommodate for single region failure. <https://vcdx.vmware.com/content/dam/digitalmarketing/vmware/ru/pdf/techpaper/vmware-horizon-7-application-publishing.pdf> Publishing Applications with VMware Horizon 7 <https://www.vmware.com/pdf/techsupportguide.pdf> VMware Technical Support Guide <https://www.vmware.com/pdf/techsupportguide.pdf> <https://techzone.vmware.com/resource/quick-start-tutorial-vmware-dynamic-environment-manager> Quick-Start Tutorial for VMware Dynamic Environment Manager ... <https://techzone.vmware.com/resource/quick-start-tutorial-vmware-dynamic-environment-manager>

QUESTION 30

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

Correct Answer: B

Section:

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. <https://communities.vmware.com/t5/VMware-Education-Services/Why-does-VMware-refuse-to-educate-their-customers/td-p/2005973> Why does VMware refuse to educate their customers ... - VMware ... <https://www.vmware.com/pdf/techsupportguide.pdf> VMware Technical Support Guide <https://www.vmware.com/pdf/techsupportguide.pdf> <https://vcdx.vmware.com/content/dam/digitalmarketing/vmware/ru/pdf/techpaper/vmware-horizon-7-application-publishing.pdf> Publishing Applications with VMware Horizon 7 <https://vcdx.vmware.com/content/dam/digitalmarketing/vmware/ru/pdf/techpaper/vmware-horizon-7-application-publishing.pdf>

QUESTION 31

Which two networking planes are converged in a VMware NSX-T Data Center? (Choose two.)

- A. Control Plane
- B. I/O Plane
- C. Management Plane
- D. Consumption Plane
- E. Data Plane

Correct Answer: A, E

Section:

Explanation:

The two networking planes that are converged in a VMware NSX-T Data Center are the Control Plane and the Data Plane. The Control Plane is responsible for making decisions such as which routes to take, which ports to open, and which services to enable. The Data Plane is responsible for forwarding data from one source to another, using the information provided by the Control Plane. The Management Plane is responsible for configuring the Control Plane and Data Plane, while the I/O Plane is responsible for managing the physical network devices. The Consumption Plane is not part of a VMware NSX-T Data Center.

<https://communities.vmware.com/t5/VMware-Education-Services/Why-does-VMware-refuse-to-educate-their-customers/td-p/2005973>

Why does VMware refuse to educate their customers ... - VMware ...

<https://communities.vmware.com/t5/VMware-Education-Services/Why-does-VMware-refuse-to-educate-their-customers/td-p/2005973>

<https://www.vmware.com/pdf/techsupportguide.pdf> VMware Technical Support Guide <https://www.vmware.com/pdf/techsupportguide.pdf>

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

Publishing Applications with VMware Horizon 7

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

QUESTION 32

A cloud administrator with an existing virtual private cloud (VPC) needs to create a dedicated connection to VMware Cloud on AWS. Which connection type would meet this requirement?

- A. Public virtual interface
- B. AWS Direct Connect
- C. Transit virtual interface
- D. Private virtual interface

Correct Answer: B

Section:

Explanation:

The best option to meet the requirements of creating a dedicated connection to VMware Cloud on AWS 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 public virtual interface, transit virtual interface, and private virtual interface. Additionally, AWS Direct Connect provides the highest performance and throughput of any of the on-premises data center connectivity options.

<https://communities.vmware.com/t5/VMware-Education-Services/Why-does-VMware-refuse-to-educate-their-customers/td-p/2005973>

Why does VMware refuse to educate their customers ... - VMware ...

<https://communities.vmware.com/t5/VMware-Education-Services/Why-does-VMware-refuse-to-educate-their-customers/td-p/2005973><https://www.vmware.com/pdf/techsupportguide.pdf>

VMware Technical Support Guide <https://www.vmware.com/pdf/techsupportguide.pdf>

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

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

QUESTION 33

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.

Correct Answer: A, D

Section:

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.

<https://communities.vmware.com/t5/VMware-Education-Services/Why-does-VMware-refuse-to-educate-their-customers/td-p/2005973>

QUESTION 34

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)

Correct Answer: A, D, F

Section:

Explanation:

When sizing a new VMware Cloud software-defined data center (SDDC) to support the migration of workloads from an on-premises SDDC, a cloud administrator should consider the total number of workloads, the average size of workload resources (CPU & RAM), and the total number of 10Gb network ports required. The total number of workloads will help determine the total number of hosts and the amount of CPU and RAM resources that will be needed to support the workloads. The average size of workload resources (CPU & RAM) will help ensure that the resources available in the SDDC are sufficient to meet the demands of the workloads. Finally, the total number of 10Gb network ports required will help determine the number of network switches and the types of ports that will be needed to support the workloads. The host hardware type in the target VMware Cloud, the total number of on-premises hosts, and the total amount of available storage across all on-premises datastores are not factors that should be considered when sizing an SDDC.

QUESTION 35

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)

Correct Answer: D

Section:

Explanation:

<https://docs.vmware.com/en/VMware-Cloud-Disaster-Recovery/services/vmware-cloud-dr-security-best-practices/GUID-BCC03463-437B-4DBE-BE21-0D43D5BA5776.html>

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.

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



QUESTION 36

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

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

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

Correct Answer: D

Section:

Explanation:

RAID-6 provides the highest level of redundancy possible, by using two parity disks instead of one, which allows for a double fault tolerance (FTT) of 2. With six hosts in the cluster, this is the optimal choice for providing the necessary redundancy for a storage I/O intensive application. For additional information, please refer to the VMware official documentation on Storage Policies: <https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.storage.doc/GUID-7F7CF2D2-7E2F-4D0E-A0F1-9768E8ABE0F5.html>

QUESTION 37

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



Correct Answer: B

Section:

Explanation:

This role is designed to give administrators access to manage virtual machines, networks, and other settings within the folder. The CloudAdmin role will also give the junior administrators access to all global permissions that are associated with the Development folder. "The CloudAdmin role is designed to give administrators access to manage a single folder. This role grants access to manage virtual machines, networks, and other settings within the folder. Additionally, this role grants access to all global permissions that are associated with the folder. For example, if the folder has global permissions that allow users to create or delete virtual machines, the CloudAdmin role will grant access to those permissions within the folder." The CloudAdmin user can grant other users or groups read-only access to VMware Cloud on AWS vCenter management objects such as the Mgmt-ResourcePool, Management VMs folder, Discovered Virtual Machines folder, vmc-hostswitch, and vsanDatastore. Because this read-only access does not propagate to management objects, you cannot grant it as a Global Permission and instead must explicitly grant it for each management object.

VMware Cloud on AWS runs a script once a day that updates any newly-created management objects (such as objects in a new cluster) so that the CloudAdmin user and CloudAdminGroup SSO group have the updated role applied. The script itself does not grant additional access to any user or group, so you'll need to wait until it completes before the CloudAdmin can use this workflow to grant read-only access to those objects.

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

QUESTION 38

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

Correct Answer: D

Section:

Explanation:

A valid management network CIDR based on the requirements is 10.1.0.0/20, as this provides a range of 4096 IP addresses, which is more than enough for 30 hosts. A /23 CIDR only provides 512 IP addresses, which is not enough for 30 hosts, while a /24 CIDR provides 256 IP addresses and a /16 CIDR provides 65,536 IP addresses, which is more than is needed for the 30 hosts. <https://blogs.vmware.com/cloud/2019/10/03/selecting-ip-subnets-sddc/>

QUESTION 39

A cloud administrator is looking to migrate several dozen workloads from their on-premises location to a VMware public cloud using the vMotion feature of VMware HCX. A total of three networks will need to be stretched for the migration.

They will also be utilizing the capabilities of the WAN appliance to optimize migration traffic.

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

- A. four
- B. five
- C. three
- D. six

Correct Answer: B

Section:

Explanation:

"The VMware HCX on-premises deployment requires five IP addresses: two for the WAN appliance, two for the vMotion feature, and one for the management network." In this scenario, the cloud administrator is utilizing the vMotion feature of VMware HCX to migrate several dozen workloads from an on-premises location to a VMware public cloud. They are also stretching three networks for the migration.

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

QUESTION 40

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

Correct Answer: A, D

Section:

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.

QUESTION 41

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

Which solution meets this requirement?

- A. Enhanced Linked Mode

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

Correct Answer: B

Section:

Explanation:

VMware HCX is a cloud migration and workload mobility solution that allows you to view and manage workloads across both an on-premises environment and a VMware Cloud on AWS software-defined data center (SDDC). It provides a secure [1], cross-cloud network bridge between your on-premises environment and VMware Cloud on AWS, allowing you to move workloads between the two environments with minimal effort. It also provides a unified view of both environments, allowing administrators to monitor and manage workloads across clouds from a single pane of glass. [1][1] <https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.hybrid-cloud-extension/GUID-E7CD1DDB-1C9F-4B88-AD41-D867E2C735D3.html>

QUESTION 42

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

- A. 25 Gbps
- B. 40 Gbps
- C. 100 Gbps
- D. 10 Gbps

Correct Answer: C

Section:

Explanation:

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

QUESTION 43

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.

Correct Answer: C

Section:

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.

QUESTION 44

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?

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

Correct Answer: C

Section:

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.

QUESTION 45

The VMware Cloud on Dell EMC subscription entitles companies to services and support in addition to the server and rack hardware and SDDC software. Which two services are included in the subscription? (Choose two.)

- Onsite support for hardware break-fix within four hours
- Remote lifecycle management of the SDDC software
- Automated capacity forecasting and expansion
- Remote lifecycle management of virtual machine operating system software
- Professional services assistance with application migration

Correct Answer: A, B

Section:

Explanation:

VMware Cloud on Dell EMC is a fully managed VMware Cloud Service which includes a physical Dell VxRail hyper-converged infrastructure built to a customer's capacity needs and is delivered onsite preloaded with VMware vSphere®, VMware NSX®, and VMware vSAN™ software. Included with this service is full management of the hardware infrastructure, including monitoring, software patching and upgrades, security updates, lifecycle management, and break-fix service in the event of a hard failure. This service is backed by an Enterprise-grade Service Level Agreement (SLA). Figure 1 shows the VMware Cloud on Dell EMC infrastructure in greater detail, including all hardware necessary to deploy the infrastructure quickly right out of the crate.

QUESTION 46

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

Correct Answer: B

Section:

Explanation:

<https://docs.vmware.com/en/VMware-Validated-Design/services/sddc-extending-to-vmware-cloudon-aws/GUID-EDF0E8DB-2195-4EC2-9CE8-1BF51C5173A5.html>

<https://docs.vmware.com/en/VMware-HCX/4.5/hcx-user-guide/GUID-4052AC3F-9FFC-4FA2-ACB4-18B21962F4D3.html>

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.

QUESTION 47

A cloud administrator is managing a VMware Cloud on AWS environment consisting of a single cluster with six hosts. There have been no changes made to the Elastic DRS configuration. In which two situations will Elastic DRS add another host to the cluster? (Choose two.)

- A. When availability zone failure occurs
- B. When memory utilization reaches 90%
- C. When network utilization reaches 90%
- D. When CPU utilization reaches 90%
- E. When storage utilization reaches 80%

Correct Answer: A, D

Section:

Explanation:

Elastic DRS will add another host to the cluster when CPU utilization reaches 90%, or when storage utilization reaches 80%. When memory utilization reaches 90%, or when network utilization reaches 90%, Elastic DRS will recommend adding additional hosts, but it will not automatically add another host without the administrator's approval.

QUESTION 48

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

Correct Answer: D, E

Section:

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.

QUESTION 49

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

Correct Answer: D

Section:

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.

QUESTION 50

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.

Correct Answer: A

Section:



QUESTION 51

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

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

Correct Answer: A, C

Section:

Explanation:

<https://cloud.google.com/architecture/private-cloud-networking-for-vmware-engine>Dedicated Interconnect provides a private [1][2], dedicated connection between your on-premises network and Google's network. It offers low latency, high bandwidth, and a secure connection.Partner Interconnect provides a connection to Google Cloud Platform through a partner's network, such as a service provider or a carrier. It offers the same low latency, high bandwidth, and secure connection, but is slightly slower than Dedicated Interconnect.

Reference: [1] <https://cloud.google.com/interconnect/docs/concepts/types>

[2] <https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.networking.doc/GUID-6D3A8E3B-A7B1-4A05-A9A8-C4F4A4A4C1A2.html>

QUESTION 52

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.

Correct Answer: C

Section:

Explanation:

<https://cloud.google.com/vmware-engine/docs/concepts-vmware-components> Node Considerations

You can specify the number of hosts to add or remove to or from their cluster. Private cloud initial setup happens in ~30 minutes. Additional hosts can be added in ~15 minutes. A three-node cluster is the minimum for production.

You can have up to 32 hosts per cluster. You can have up to 64 hosts per private cloud. Reference: <https://cloud.google.com/vmware-engine/docs/concepts-vmware-components>

QUESTION 53

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

Correct Answer: D

Section:

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-EDA5A6E5-6C5B-4F66-9C2F-2C6D4F6EF8F6.html>

QUESTION 54

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

Correct Answer: C, D

Section:

Explanation:

The two valid subnet sizes that meet the requirement for the VMware vSphere/vSAN subnet are /22 and /23. According to the VMware documentation, the subnet size must be between /22 and /23 for optimal performance and scalability.

Reference: <https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc.networking.doc/GUID-8D8F3C3E-2171-4B00-8F1C-F6D7D6F793A2.html>

QUESTION 55

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

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

Correct Answer: D

Section:

Explanation:

VMware High Availability (HA) is a feature of the VMware Cloud platform that monitors the health of virtual machines and restarts virtual machines on other hosts if they crash or become unresponsive. This ensures that the virtual machines are always available and that no downtime is experienced. The default response is to restart the impacted virtual machine on other hosts in the same SDDC Cluster, however, this can be customized to suit the needs of the customer. Reference: [1] https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.availability_and_scalability.doc/GUID-C7E2C2A2-B9A8-4CD0-A2F2-EA6C08C8D95B.html
[2] <https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.admin.doc/GUID-F9C7F1B8-4855-4C3A-A723-C9A2F7CDBFFB.html>

QUESTION 56

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

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

Correct Answer: A

Section:

Explanation:

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



QUESTION 57

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

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

Correct Answer: C, D

Section:

Explanation:

<https://docs.vmware.com/en/VMware-Tanzu-Kubernetes-Grid/1.6/air-gap-reference-architecture/GUID-deployment-guides-tkg-vsphere-vds-airgap.html>

QUESTION 58

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

Correct Answer: A

Section:

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-64D7A8F3-45C9-4A83-8528-A8C2A2C7001D.html>

QUESTION 59

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

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

Correct Answer: D

Section:

Explanation:

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

QUESTION 60

Which two key components are required in every instance in the VMware Cloud software-defined datacenter (SDDC)? (Choose two.)

- A. VMware vSphere
- B. VMware vRealize Operations
- C. VMware Tanzu Kubernetes Grid
- D. VMware NSX-T
- E. CloudHealth by VMware

Correct Answer: A, D

Section:

Explanation:

The correct answers are A and D. Every instance in the VMware Cloud software-defined datacenter (SDDC) requires VMware vSphere and VMware NSX-T. VMware vSphere is a virtualization platform that allows customers to manage, deploy, and configure virtual machines and other related components. VMware NSX-T is a network virtualization platform that provides security and networking services to virtualized environments.

QUESTION 61

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

Correct Answer: B

Section:

Explanation:

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-networking-security/GUID-2D31A9A6-4A80-4B5B-A382-2C5B591F6AEB.html>

QUESTION 62

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

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

Correct Answer: B

Section:

Explanation:

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

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

Reference: <https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-encryption/GUID-6F6921CA-44D6-4D9D-B0C0-12C18A545B7C.html>

QUESTION 63

A cloud administrator is using VMware HCX to migrate application workloads between an on-premises data center and a VMware Public Cloud (UI!) capability of VMware HCX is being used to extend a number of on-premises network segments into the cloud to avoid IP re-addressing concerns. When the cloud administrator tries to extend a native layer 2 network segment from the cloud back into the on-premises data center, an error is encountered and the extension fails. What should the administrator do to enable network extension from the cloud side to on-premises in this scenario?

- A. Enable reverse L2E in the advanced configuration menu of HCX. Make the appropriate change and re-deploy the HCX Service Mesh.
- B. Ensure that the on-premises environment that has at minimum a VMware vSphere Distributed Switch with version 6.5 configured.
- C. Install VMware NSXT into the on-premise data center.
- D. Enable reverse L2E in the advanced configuration menu of HCX. Make the appropriate change, redeploy the on-premise HCX Manager and re-pair the sites together.

Correct Answer: B

Section:

Explanation:

The best solution for enabling network extension from the cloud side to the on-premises data center in this scenario is to ensure that the on-premises environment has at least a VMware vSphere Distributed Switch with version 6.5 configured. This will enable the reverse L2E feature, which is necessary for extending the native layer 2 network segment from the cloud back into the on-premises data center. For more information on how to configure reverse L2E and extend a network segment from the cloud to the on-premises data center, please refer to the official VMware documentation here.

QUESTION 64

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

Correct Answer: B

Section:

Explanation:

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-networking-security/GUID-586C053D-9553-461E-B6A8-FF508C8F091C.html>

QUESTION 65

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

Correct Answer: D

Section:

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.

QUESTION 66

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

Correct Answer: A, B, D

Section:

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/GUID-1F2D1BFC-F5C7-4534-8B49-39F9D08E7F1A.htm>

QUESTION 67

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

Correct Answer: C

Section:

Explanation:

https://docs.vmware.com/en/VMware-Workspace-ONE-Access/20.10/workspace_one_access_install/GUID-E81B6B1B-A3D1-40D0-806A-3D31502C53A5.htmlThe 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.admin.configure.doc/GUID-F5C6FD9E-36DA-4B1F-A7E7-CF8F64A81D78.html>

QUESTION 68

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

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

Correct Answer: B

Section:

Explanation:

This would enable the user to have the necessary permissions to deploy virtual machines - and thus, would ensure that all of the necessary virtual machines are deployed in a timely and efficient manner. VMware Cloud on AWS Documentation: "Deployment of virtual machines" VMware Cloud on AWS Documentation: "Creating virtual machines with the VMware Cloud on AWS console" VMware Cloud on AWS Documentation: "Managing virtual machines with the VMware Cloud on AWS console"

QUESTION 69

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

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

Correct Answer: C

Section:

Explanation:

A VMware Cloud software-defined data center (SDDC) uses a logical switching component called a Network Virtual Distributed Switch (N-VDS) or vSphere Distributed Switch (VDS) to provide layer 2 forwarding functionality [1][2]. A VDS is a network switch that provides centralized network configuration, management, and monitoring. It works with the NSX for vSphere data plane to provide layer 2 forwarding, packet filtering, and traffic monitoring services. A VDS is composed of multiple Segment Ports (which are like individual physical ports on a normal switch), Uplinks, and Transport Nodes. The Segment Ports are used to connect virtual machines to the VDS, while Uplinks are used to connect the VDS to physical networks. Transport Nodes are the physical switches that are associated with the VDS. For more information, see the official VMware documentation here: https://docs.vmware.com/en/VMware-NSX-Data-Center/2.4/nsx_24_sdn_networking/GUID-A4A6E4A8-FD7C-4B6E-A3D3-6F9B6D0578C2.html.

QUESTION 70

In order to provide overlapping IP address segments within a VMware cloud Environment, what must be configured?

- A. Additional NSX Edge appliances
- B. Additional Tier-1 gateways
- C. Additional network segments
- D. Additional Tier-0 gateways

Correct Answer: B

Section:

Explanation:

<https://vmc.techzone.vmware.com/understanding-segments-vmc-aws>

QUESTION 71

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

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

Correct Answer: A

Section:

Explanation:

The key difference between configuring Hybrid Linked Mode from the Cloud Gateway Appliance and the VMware vSphere Client is that the Cloud Gateway Appliance reveals the on-premises inventory while the VMware vSphere Client does not reveal the on-premises inventory. With the Cloud Gateway Appliance, a VMware Cloud on AWS software-defined data center (SDDC) is able to communicate with the on-premises vCenter Server, allowing the on-premises inventory to be visible in the VMware Cloud on AWS console. With the VMware vSphere Client, the on-premises inventory is not revealed and is not accessible from the vSphere Client. Reference: [1] <https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/Hybrid-Linked-Mode/GUID-Copy-Hybrid-Linked-Mode.html>

QUESTION 72

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

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

Correct Answer: A, D

Section:

Explanation:

[https://blogs.vmware.com/virtualblocks/2021/09/28/operational-air-gaps/Operational isolation \(operational "air-gapping"\) is critical to DR. VMware Cloud DR was designed from the very beginning for its systems and repository to be operationally isolated and for instantiating isolated recovery environments.](https://blogs.vmware.com/virtualblocks/2021/09/28/operational-air-gaps/Operational%20isolation%20(operational%20%22air-gapping%22)%20is%20critical%20to%20DR.%20VMware%20Cloud%20DR%20was%20designed%20from%20the%20very%20beginning%20for%20its%20systems%20and%20repository%20to%20be%20operationally%20isolated%20and%20for%20instantiating%20isolated%20recovery%20environments.)

QUESTION 73

Which solution would an administrator use to manage the lifecycle operations of Tanzu Kubernetes clusters?

- A. VMware Tanzu Service Mesh
- B. VMware vSphere Lifecycle Manager
- C. VMware Tanzu Observability by Wavefront
- D. VMware Tanzu Kubernetes Grid

Correct Answer: D

Section:

Explanation:

VMware Tanzu Kubernetes Grid is described as a comprehensive solution for operating Kubernetes- based applications in production, as well as creating, scaling and managing clusters. It provides a centralized control plane for managing the lifecycle operations of Tanzu Kubernetes clusters. (Source:<https://tanzu.vmware.com/kubernetes>)

QUESTION 74

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

Correct Answer: C, E, F

Section:

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. Reference:

[1] https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.vm_admin.doc/GUID-B2B7F78A-5D5F-4A3E-BEA9-9F6A02A7E1B2.html

[2] https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.vm_admin.doc/GUID-EAAE04A9-9DAF-4DAC-B4A0-F35A4F4F2A6A.html

[3] https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.vm_admin.doc/GUID-9FADCD7E-F4A8-4F29

QUESTION 75

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

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

Correct Answer: C, E

Section:

Explanation:

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

The SDDC management network will be used for communication between the VMware Cloud components and the data center, and must be isolated from the customer network. Reference: [1]

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/VMware-Cloud-on-AWS-Outposts/GUID-prerequisites-network.html>

QUESTION 76

A Cloud Administrator is managing a VMware Cloud environment consisting of a single cluster with two hosts. The administrator is trying to create a new virtual machine and is getting the following error message: cannot

complete file creation operation. There are currently 2 unable failure domains. the operation requires 3 more usable fault domain. failed to create object.

- A. The VM storage policy is configured Incorrectly for the cluster.
- B. There is insufficient CPU and memory based on the current virtual machine resource reservation settings.
- C. One of the hosts is in maintenance mode.
- D. vSphere Distributed Resource Scheduler (DRS) is enabled.

Correct Answer: C

Section:

Explanation:

The error message that the Cloud Administrator is receiving indicates that the cluster is not able to meet the requirements of the new virtual machine due to insufficient fault domains. The most likely cause of this is that one of the hosts is in maintenance mode. When a host is in maintenance mode, it is not available to the cluster, and thus cannot provide the necessary fault domains. To correct this issue, the Cloud Administrator should ensure that all hosts in the cluster are available and not in maintenance mode before attempting to create the new virtual machine. Reference: [1] <https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/VMware-Cloud-on-AWS-Outposts/GUID-host-maintenance-mode.html>

QUESTION 77

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



Correct Answer: B, E

Section:

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>

QUESTION 78

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.

Correct Answer: A

Section:

Explanation:

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

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

QUESTION 79

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

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

Correct Answer: A, D, E

Section:

Explanation:

To create a virtual machine template, you will need to configure the virtual machine hardware configuration, install the necessary applications, tools, and patches, and select the guest operating system. The template can also include vSphere tags and custom attributes to further customize the virtual machine. Additionally, the template can include virtual machine snapshots which will save the current state of the virtual machine and can be used to quickly restore the machine to the same state.

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

QUESTION 80

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

Correct Answer: A

Section:

Explanation:

<https://www.nakivo.com/blog/vmware-snapshots-vsphere-how-to/#title-12>

QUESTION 81

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

Correct Answer: D

Section:

Explanation:

<https://docs.vmware.com/en/VMware-HCX/4.5/hcx-user-guide/GUID-741F47D5-A3C9-4D74-9672-E54D8791D8F0.html>

QUESTION 82

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

- A. Having enough existing rack space for the components
- B. Distance between loading dock and datacenter
- C. Size of the doorways between loading dock and datacenter
- D. Having enough people to carry the equipment
- E. Floor and elevator weight capacity between loading dock and datacenter



Correct Answer: A, E

Section:

Explanation:

<https://aws.amazon.com/vmware/outposts/faqs/>

When deploying VMware Cloud on Dell EMC or VMware Cloud on AWS Outposts in a data center, it is important to consider the amount of existing rack space available for the components, as well as the floor and elevator weight capacity between the loading dock and the data center. The distance between the loading dock and the data center, the size of the doorways between the loading dock and the data center, and the number of people available to carry the equipment are not relevant factors to consider.

QUESTION 83

A virtual machine running in VMware Cloud on AWS is experiencing poor CPU performance. What are two steps the cloud administrator can take to troubleshoot this issue? (Choose two.)

- A. Physically access the console of the VMware ESXi host where the virtual machine resides and use the command line to review the logs.
- B. Use the Troubleshooting Workbench in VMware vRealize Operations Cloud to look for potential evidence.
- C. Set the power management policy on the VMware ESXi host to "High Performance."
- D. Log in to the VMware ESXi host using SSH and run 'esxtop' to examine CPU statistics.
- E. Use the VMware vSphere Client to connect to the VMware vCenter which manages the virtual machine and examine its performance statistics.

Correct Answer: D, E

Section:

Explanation:

The correct answers are D. Log in to the VMware ESXi host using SSH and run 'esxtop' to examine CPU statistics, and E. Use the VMware vSphere Client to connect to the VMware vCenter which manages the virtual machine and examine its performance statistics. To troubleshoot a virtual machine experiencing poor CPU performance in VMware Cloud on AWS, a cloud administrator can log in to the VMware ESXi host using SSH and run 'esxtop' to examine CPU statistics, as well as use the VMware vSphere Client to connect to the VMware vCenter which manages the virtual machine and examine its performance statistics. Additionally, the cloud administrator can review the logs of the VMware ESXi host and use the Troubleshooting Workbench in VMware vRealize Operations Cloud to look for potential evidence. Another step the cloud administrator can take is to set the power management policy on the VMware ESXi host to "High Performance" to ensure the host is running at its peak performance. For more information, please refer to the official VMware Cloud on AWS documentation at: <https://docs.vmware.com/en/VMware-Cloud-on-AWS/index.html>.

QUESTION 84

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

Correct Answer: C

Section:

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-D6B7B9E9-E134-4C8A-8F2E-1C60A2FEDC1A.html>

QUESTION 85

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

Correct Answer: B

Section:

Explanation:

<https://docs.vmware.com/en/vRealize-Business/7.6/vRBforCloud.user.doc/GUID-AA3C209A-2DFA-433F-BD57-67E66A598E5D.html>