Practice Exam Questions

vmware

2V0-33.22

VMware Cloud Professional

EXAMKILLER

Help Pass Your Exam At First Try

VMware

Exam 2V0-33.22

VMware Cloud Professional

Version: 6.1

[Total Questions: 126]

Question No : 1

A cloud administrator is looking to migrate several dozen workloads from their on-premises location to a VMware public cloud using the vMotlon feature of VMware HCX. A total of three networks will need to be stretched for the migration. They will also be utilizing the capabilities of the WAN appliance to optimize migration traffic.

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

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

Answer: B

Explanation: "The VMware HCX on-premises deployment requires five IP addresses: two for the WAN appliance, two for the vMotion feature, and one for the management network."

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

Question No : 2

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

A. Policy-based virtual private network (VPN)

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

Answer: C

Explanation: The best option for a cloud administrator who wants to deploy a VMware Cloud software-defined data center (SDDC) on a cloud provider and requires a consistent 4.5 Gbps bandwidth from applications to communicate from on-premises to the SDDC is a Route-Based Virtual Private Network (VPN). This type of connection offers enhanced performance [1][2], flexibility, scalability, and security compared to other options, such as Policy-Based Virtual Private Network (VPN), Private L2 Virtual Private Network (VPN), or Private Line.
According to the VMware official site, "Route-based VPN enables a secure connection between two or more sites, or between a site and a mobile user, and provides better performance and scalability than a policy-based VPN. Route-based VPNs are also more secure than policy-based VPNs, because the traffic is encrypted with a unique encryption key for each tunnel, rather than relying on a shared key for all tunnels. This allows for secure and reliable connections for devices and applications located in different physical locations." [1]
[1] https://docs.vmware.com/en/VMware-NSX-Data-Center/2.4/com.vmware.nsx.admin.doc/GUID-D6B7B9E9-E134-4C8A-8F2E-1C60A2FEDC1A.html

Question No : 3

A cloud administrator is managing a VMware Cloud on AWS environment. Currently, there Is a single cluster consisting of four 13.metal hosts. Due to an increased demand, cluster capacity has to be expanded by 60 cores and 640 GB of memory.

What should the administrator do to meet the demand?

A. Add 16 CPU cores to the existing hosts.
B. Add three c4.metal hosts to the cluster.
C. Add two i3.metal hosts to the cluster.
D. Add one i3en.metal host to the cluster.

Answer: C

Explanation: According to the VMware Cloud on AWS documentation, the minimum capacity of an i3.metal host is 8 vCPUs and 64 GB of memory. Therefore, to meet the

demand of an additional 60 cores and 640 GB of memory, the administrator should add two i3.metal hosts to the cluster. For more information, please refer to the official VMware Cloud on AWS documentation at:https://docs.vmware.com/en/VMware-Cloud-on-AWS/index.html.

Question No : 4

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

HCX appliance requirements are as follows:

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

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

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

Answer: A

Explanation:

https://docs.vmware.com/en/VMware-HCX/4.6/hcx-user-guide/GUID-D64901F4-6AB4-4820-9303-27927648A34D.html

Question No : 5

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

A. Facilitate disaster recovery
B. Application modernization

C. Digital transformation
D. Cost savings

Answer: C

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

Question No : 6

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

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

Answer: D

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

Question No : 7

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

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

Answer: B

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

The responsibility for the encryption of virtual machines in VMware Cloud lies with the customer. The customer is responsible for configuring and managing any encryption or security related settings and configurations in the virtual machines, such as disk encryption or the configuration of security protocols. The VMware Cloud Provider Partner (VCPP) is responsible for the overall security of the cloud environment [1][2], including the encryption of data at rest, but the customer is responsible for configuring and managing the encryption settings within their virtual machines. Reference: https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.encryption/GUID-6F6921CA-44D6-4D9D-B0C0-12C18A545B7C.html

Question No : 8

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-O gateways

Answer: B

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

Question No : 9

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

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

Answer: A,D,E

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

Question No : 10

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

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

Answer: B,C,E,F

Explanation: Example B illustrates the benefit of cloud computing where an organization can manage its cloud resources by using different cloud providers that are separate and isolated from each other. This allows the organization to make use of features and services offered by different cloud providers in order to benefit from the best of different services.
Example C illustrates the benefit of cloud computing where a business can store infrequently accessed data in the cloud in order to benefit from reduced on-premises storage costs, as cloud storage is usually cheaper than on-premise storage.
Example E illustrates the benefit of cloud computing where a developer can code an

application in a cloud-based environment, and, with a few simple commands, deploy the application on the business website. This eliminates the need for the developer to set up and manage the application on their own, as the cloud platform handles the deployment and hosting of the application.
Example F illustrates the benefit of cloud computing where a large amount of storage can be made available in seconds using a cloud option. This is useful for businesses that require a large amount of storage but don't have the resources to set up and manage their own storage solution.
For more information on the benefits of cloud computing, see the VMware official documentation athttps://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.getting-started/GUID-F0A2F338-A6A7-49AD-B158-CFFCA2F29C1B.html.

Question No : 11

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

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

Answer: B

Explanation: Compute Gateway (CGW) The CGW is a Tier 1 router that handles network traffic for workload VMs connected to routed compute network segments. Compute gateway firewall rules, along with NAT rules, run on the Tier 0 router. In the default configuration, these rules block all traffic to and from compute network segments (see Configure Compute Gateway Networking and Security).
https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/vmc-on-aws-networking-security.pdf

Question No : 12

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

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

Answer: D

Explanation: Hybrid Linked Mode can tolerate a time skew of up to ten minutes between the on-premises data center and the cloud SDDC. The maximum latency between your cloud SDDC and on-premises data center cannot exceed 100 msec roundtrip.
https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vsphere.vmc-aws-manage-data-center-vms.doc/GUID-BE75F0F1-2864-4926-97FE-37E635471C43.html

Question No : 13

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

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

Answer: C

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

Question No : 14

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

A. VMware Dynamic Environment Manager (DEM)
B. VMware ThinApp

C. VMware Workspace ONE Unified Endpoint Management (UEM)
D. VMware Horizon
E. VMware Workspace ONE Access

Answer: D,E

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

Question No : 15

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

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

Answer: B

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

Question No : 16

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

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

Answer: B

Explanation:

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

Question No : 17

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

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

Answer: B

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

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

across clouds, reducing complexity and increasing agility. VMware Multi-Cloud also provides powerful automation and orchestration capabilities to help streamline operations and improve efficiency. [1]
[1]https://www.vmware.com/products/vmware-multi-cloud.html

Question No : 18

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

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

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

Answer: A,C

Explanation: The Workspace ONE Access connector is used to synchronize groups and users from the internal Active Directory to the VMware Cloud Services Console. Additionally, the administrator should configure a SAML 2.0 Identity Provider to enable single sign-on (SSO) capability and secure access to the VMware Cloud Services Console.

Question No : 19

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

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

Answer: D

Explanation: https://docs.vmware.com/en/VMware-Cloud-Disaster-

Recovery/services/vmware-cloud-dr-security-best-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.

PREPARING FOR VMWARE CLOUD ON AWS
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vmc-aws/preparing-for-vmware-cloud-on-aws.pdf

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

What is Network Virtualization? | VMware Glossary
https://www.vmware.com/topics/glossary/content/network-virtualization.html

Question No : 20

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

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

Answer: A

Explanation: vCenter Mapping Mapping vCenters in a DR plan consists of selecting source vCenters that are registered to the protected site. Choosing a target vCenter for a

Failover SDDC is simple; each SDDC contains a single vCenter instance. For VMware Cloud Disaster Recovery, keep in mind that a protected site can have multiple registered vCenters, but you can only map one vCenter on VMware Cloud on AWS per-DR plan.https://vmc.techzone.vmware.com/resource/introduction-vmware-cloud-disaster-recovery#inventory-and-resource-mappinghttps://vmc.techzone.vmware.com/resource/protection-groups-and-recovery-plans-vcdr#create-a-disaster-recovery-plan

Question No : 21

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

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

Answer: B,C,D,G

Explanation:

- Identify the desired region. This determines where your private cloud will be deployed and which Azure services are available.
- Identify a management CIDR of size /22. This determines the IP address range for your private cloud management components such as vCenter Server, NSX Manager, etc.
- Open a support request with Microsoft Azure requesting capacity. This ensures that there are enough hosts available for your private cloud deployment.
- Identify the current number of hosts needed. This determines how many hosts will be provisioned initially for your private cloud cluster.

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

Question No : 22

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