DUMPSARENA

VMware Cloud on AWS Master Specialist

VMware 5V0-11.21

Version Demo

Total Demo Questions: 10

Total Premium Questions: 65

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Standard security practice for a company requires that all administrator-level user accounts have their passwords changed every 60 days. The cloudadmin@vmc.local account password is changed by an administrator through the VMware vSphere Cliento adhere to the security policy. When the administrator attempts to log into the VMware Cloud on AWS vCenter Server through the VMware vSphere Client a few days later as cloudadmin@vmc.local using the account credentials copied from the VMware Cloud console, the administrator's access is denied. What is the likely cause of this issue?

A. The cloudadmin@vmc.local account password should not be changed through the VMware vSphere Client. In order to prevent unauthorized access to VMware Cloud on AWS by non-authorized individuals, VMware will lock the account out.

B. When the password for cloudadmin@vmc.local is updated from the VMware vSphere Client, the updated password is not reflected in the VMware Cloud console.

C. The cloudadmin@vmc.local password change confirmation email has not been approved by an Organization Owner.

D. The cloudadmin@vmc.local account password should only be changed through the appliance management interface of the VMware vCenter Server.

ANSWER: B

QUESTION NO: 2

An administrator is tasked with migrating workloads from one of the company's primary data centers to VMware Cloud on AWS. The migration of these workloads must meet the follow criteria: ▪ Must have zero downtime

- Must be organized based on service-level agreement (SLA)
- Should not communicate with the on-premises gateway

Which three VMware HCX features would meet these requirements? (Choose three.)

A. Mobility Optimized Networking

B. Replication-Assisted vMotion

C. Network Extension

D. Bulk Migration

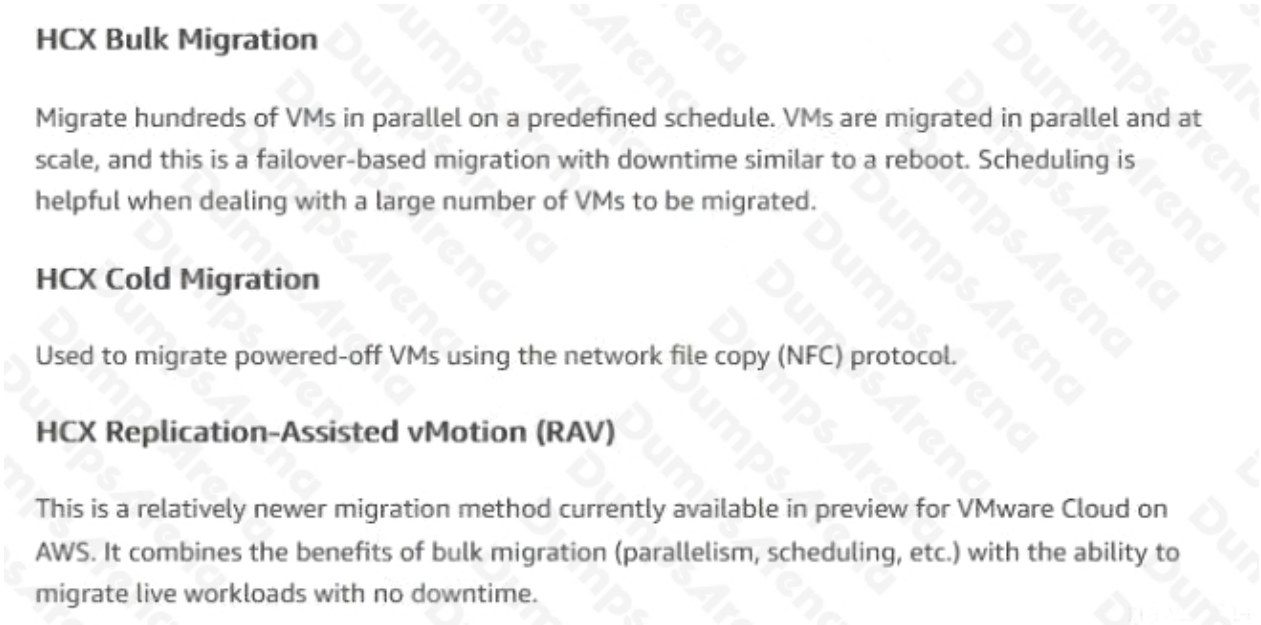
E. Mobility Groups

F. Application Path Resiliency

ANSWER: B C D

Explanation:

Reference: https://aws.amazon.com/blogs/apn/migrating-workloads-to-vmware-cloud-on-aws-with-hybrid-cloud-extension-hcx/



QUESTION NO: 3

An administrator is preparing to deploy a VMware Cloud on AWS software-defined data center (SDDC) and is planning to scale up to 48 nodes in the future. What is the minimum size management CIDR block that is needed to meet this requirement?

A. /24

B. /16

C. /23

D. /20

ANSWER: D

Explanation:

The management CIDR must be one of 3 available sizes: /16, /20 or /23. The primary factor in selecting the size is the anticipated scalability of the SDDC. In single-AZ deployment, a /23 CIDR can support 27 ESXi hosts, while a /20 can support up to 251.

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

The management CIDR must be one of 3 available sizes: /16, /20 or /23. The primary factor in selecting the size is the anticipated scalability of the SDDC. In single-AZ deployment, a /23 CIDR can support 27 ESXi hosts, while a /20 can support up to 251, and a /16 up to 4091, but currently limited to the SDDC maximum of 300 hosts. When deploying a multi-AZ (or stretched cluster) SDDC, the limits are 22 hosts, 246 hosts, and the SDDC maximum hosts for /23, /20 and /16 CIDRs respectively. If SDDCs larger than 300 hosts are supported in the future, only a /16 will allow you to take advantage of that. It's also important to note that some hosts are reserved for maintenance operations: the number of usable hosts will be reduced by 2, plus 1 per cluster. As an example, an SDDC using a /23 management CIDR, configured with 2 clusters will only be able to deploy 23 hosts. The remaining 4 hosts are reserved to be added by maintenance operations (upgrades, in case of a host failure, etc.)

QUESTION NO: 4

An environment is running a VMware Cloud on AWS software-defined data center (SDDC) with six i3.metal hosts. Storage space usage has increased and the administrator is required to add storage capacity. Which two approaches can the administrator take to add storage capacity? (Choose two.)

A. Deploy Amazon Elastic File System (EFS) file shares from the AWS console and attach them to the i3.metal hosts. Use VMware Storage vMotion to migrate the storage-bound virtual machines to the Amazon EFS data stores.

B. Deploy Amazon Elastic Block Store (EBS) storage volumes (GP2) from the AWS console and attach them to the i3.metal hosts. Allow VMware vSAN extend the storage capacity automatically.

C. Deploy an additional cluster based on i3en.metal hosts and migrate the storage-bound virtual machines to the i3en.metal hosts.

D. Add additional i3.metal hosts to increase the total vSAN storage space.

E. Add additional i3en.metal hosts and migrate the storage-bound virtual machines to the i3en.metal hosts.

ANSWER: B D

Explanation:

Reference: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-attaching-volume.html

You can attach an available EBS volume to one or more of your instances that is in the same Availability Zone as the volume.

For information about adding EBS volumes to your instance at launch, see Instance block device mapping.

Prerequisites

- Determine how many volumes you can attach to your instance. For more information, see Instance volume limits.
- Determine whether you can attach your volume to multiple instances and enable Multi-Attach. For more information, see Attach a volume to multiple instances with Amazon EBS Multi-Attach.
- If a volume is encrypted, it can only be attached to an instance that supports Amazon EBS encryption. For more information, see Supported instance types.
- If a volume has an AWS Marketplace product code:
  - The volume can only be attached to a stopped instance.
  - You must be subscribed to the AWS Marketplace code that is on the volume.
  - The configuration (instance type, operating system) of the instance must support that specific AWS Marketplace code. For example, you cannot take a volume from a Windows instance and attach it to a Linux instance.
  - AWS Marketplace product codes are copied from the volume to the instance.

QUESTION NO: 5

What are three possible reasons that would prevent virtual machines from migrating to VMware Cloud on AWS using VMware vSphere vMotion? (Choose three.)

A. Paravirtual SCSI disks are mounted.

B. Virtual serial ports are connected with network output.

C. Remote devices are attached.

D. VMware Tools are NOT installed.

E. The virtual machine (VM) is a linked clone.

F. The virtual machine (VM) remote console is open.

ANSWER: A D E

QUESTION NO: 6

An administrator deploys a virtual machine to its software-defined data center (SDDC) and configures it to perform backups of the other virtual machines in the SDDC. The administrator also creates an AWS Simple Storage Service (S3) bucket in the linked Amazon Virtual Private Cloud (VPC) and is attempting to use the S3 bucket as a repository for their backups. The administrator confirms that the backup software is capable of using AWS S3 storage as a backup repository, and that the AWS S3 bucket is configured to use an endpoint in the linked VPC. What else should the administrator do to ensure connectivity between SDDC virtual machines and the AWS S3 repository in the linked VPC through the Elastic Network Interface?

A. Configure Direct Connect to a Private Virtual Interface for access to AWS services.

B. Configure a route-based VPN for the SDDC to the VPC.

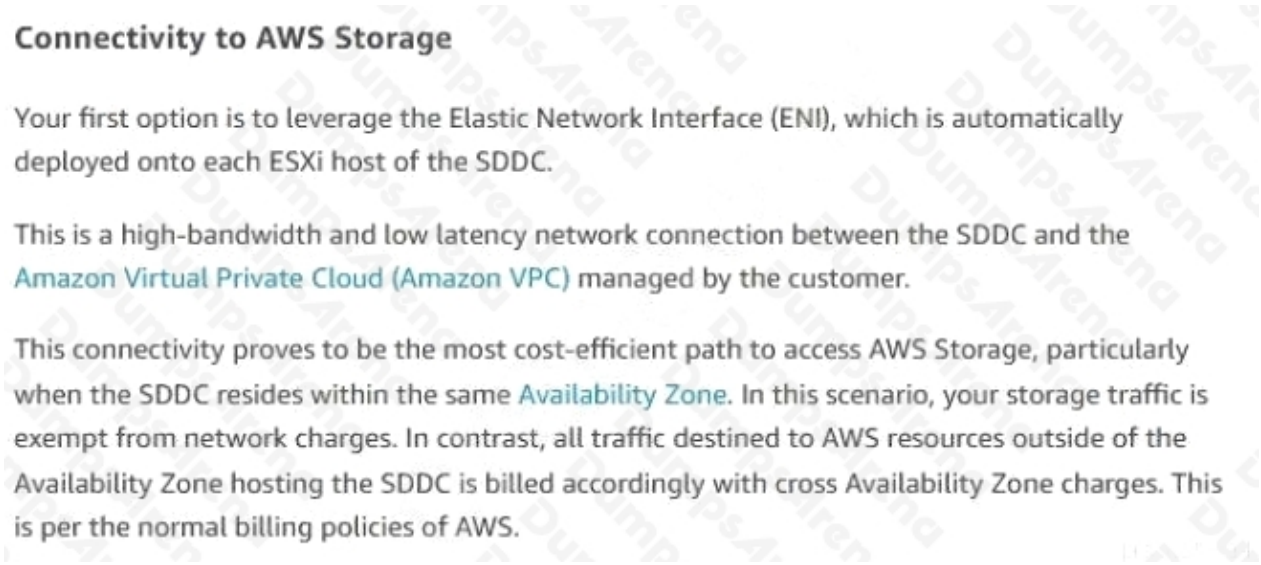
C. Configure Direct Connect to a Public Virtual Interface for access to AWS services.

D. Ensure Service Access for S3 is enabled in Networking and Security for the SDDC.

ANSWER: A

Explanation:

Reference: https://aws.amazon.com/blogs/storage/storage-options-and-designs-for-vmware-cloud-on-aws/



Connectivity to AWS Storage

Your first option is to leverage the Elastic Network Interface (ENI), which is automatically deployed onto each ESXi host of the SDDC.

This is a high-bandwidth and low latency network connection between the SDDC and the Amazon Virtual Private Cloud (Amazon VPC) managed by the customer.

This connectivity proves to be the most cost-efficient path to access AWS Storage, particularly when the SDDC resides within the same Availability Zone. In this scenario, your storage traffic is exempt from network charges. In contrast, all traffic destined to AWS resources outside of the Availability Zone hosting the SDDC is billed accordingly with cross Availability Zone charges. This is per the normal billing policies of AWS.

QUESTION NO: 7

An architect is designing a solution for a customer that will include VMware Cloud on AWS. The solution will enable the customer to progress with their business objective to migrate all of their VMware vSphere workloads to the cloud and completely exit their physical data center. The following information was provided by key stakeholders as part of the initial design workshop:

- The customer already consumes a number of AWS native services as part of their existing application landscape.
- The customer currently uses both VMware vRealize Log Insight Cloud and VMware vRealize Operations Cloud to monitor their existing on-premises vSphere solution.
- The customer currently has configured Federated Identity Management to enable role based access control to VMware Cloud services using their on-premises Active Directory.

What should the architect recommend to ensure that all the prerequisites for deploying a VMware Cloud on AWS solution are successfully met while minimizing operational complexity?

A. A new VMware Cloud account must be created to enable access to the VMware Cloud on AWS service.

B. A new AWS account must be created to enable dedicated connectivity for VMware Cloud on AWS.

C. The existing VMware Cloud account should be used to enable access to the VMware Cloud on AWS service.

D. The ownership of the existing AWS account should be transferred to VMware so that the VMware Cloud on AWS software-defined data center (SDDC) can be deployed.

ANSWER: D

QUESTION NO: 8

What are three benefits of using VMware Cloud on AWS? (Choose three.)

A. With VMware Cloud on AWS, IT teams can manage their VMware Cloud on AWS resources with familiar VMware tools.

B. With VMware Cloud on AWS, IT teams can manage their native AWS resources with familiar VMware tools.

C. VMware Cloud on AWS supports optimized virtual AWS Elastic Compute Cloud (EC2) instances.

D. Native VMware workloads can be migrated back and forth between on-premises VMware vSphere environments and VMware Cloud on AWS.

E. With VMware Cloud on AWS, VMware and AWS administrators will manage, maintain and update all virtual machines.

F. Native AWS services can be consumed over the global AWS backbone with high bandwidth and low latency.

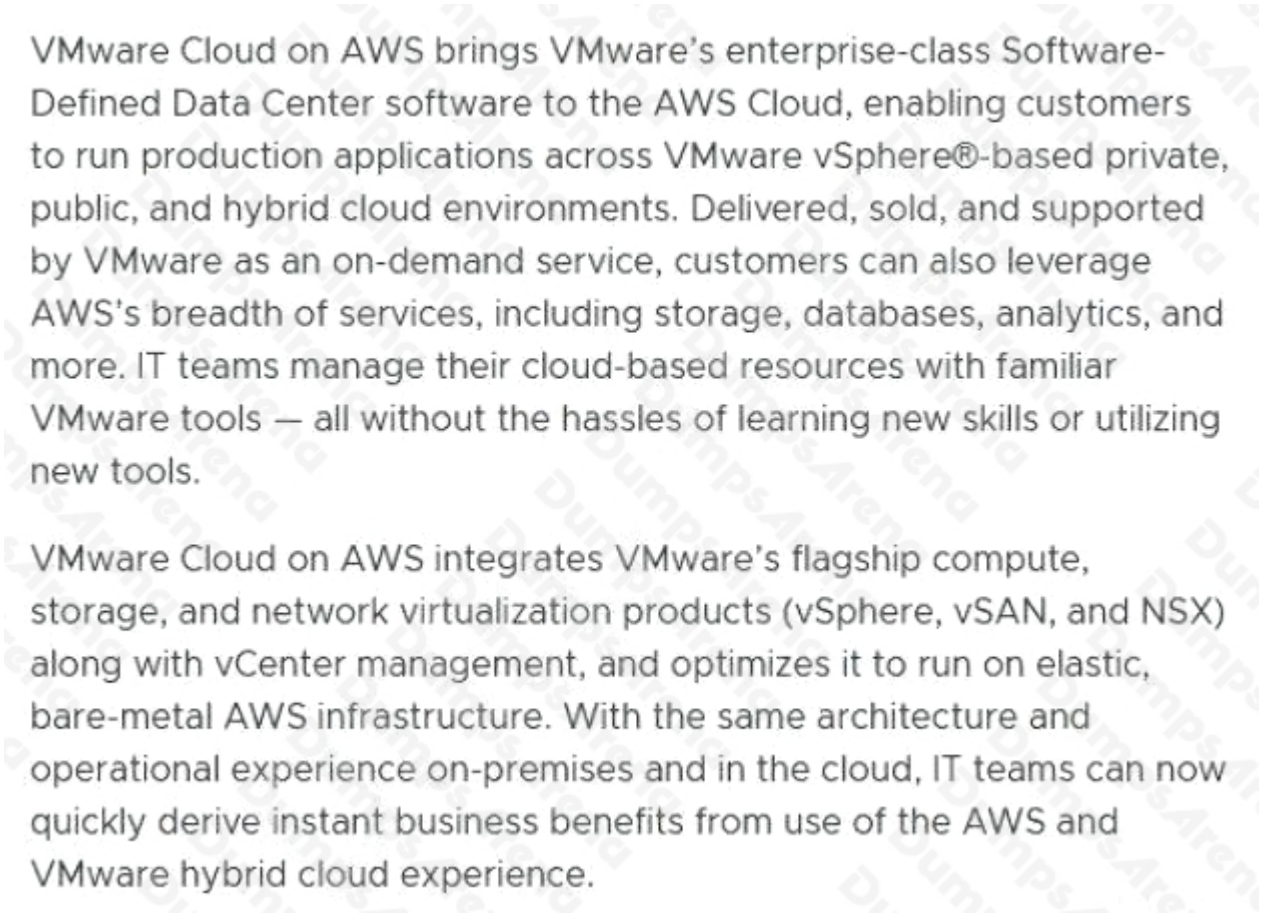
ANSWER: A C E

Explanation:

IT teams manage their cloud-based resources with familiar VMware tools.

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers. Managing Virtual Machines in VMware Cloud on AWS.

Reference: https://docs.vmware.com/en/VMware-Cloud-on-AWS/solutions/VMware-Cloud-on-AWS.39646badb412ba21bd6770ef62ae00a2/GUID-2EF52910E0945214C0020069FDCD484E.html



https://aws.amazon.com/ec2/?ec2-whats-new.sort-by=item.additionalFields.postDateTime&ec2-whats-new.sort-order=desc
https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/vmc-aws-manage-data-center-vms.pdf

QUESTION NO: 9

A company is operating a main data center and two smaller data centers in branch offices. The main data center is being replicated to a disaster recovery site at a co-located data center with a recovery point objective (RPO) of five minutes and a recovery time objective (RTO) of two hours. The branch data centers are shipping backup tapes to the main data center on a weekly basis. What would be a cost-efficient VMware solution that would improve RTO and RPO for the branch office data centers while maintaining the recovery time for the main data center?

A. Create a software-defined data center (SDDC) in VMware Cloud on AWS. Create a shared content librand let the branch offices subscribe to it. Export the virtual machines in the branch offices to OVF files on the shared content library on a weekly basis.

B. Create a software-defined data center (SDDC) in VMware Cloud on AWS. Migrate the disaster recovery solution from the co-located data center to the VMware Cloud on AWS SDDC. Create regular copies of the virtual machines at the branch offices and use AWS Snowball to directly ship the copies to an AWS data center and store them on AWS S3 buckets.

C. Create a software-defined data center (SDDC) in VMware Cloud on AWS. Activate VMware Site Recovery. Replace the co-located disaster recovery (DR) site for the main data center with VMware Site Recovery. For the branch offices, implement VMware Cloud Disaster Recovery (VCDR).

D. Create a software-defined data center (SDDC) in VMware Cloud on AWS. Replace the co-located site for the main data center and the backup tape shipping for the branch offices with VMware Cloud Disaster Recovery (VCDR).

ANSWER: A

QUESTION NO: 10

Which three statements are true about the Elastic DRS Optimize for Rapid Scale-Out policy? (Choose three.)

A. Hosts are added incrementally when needed for storage.

B. Hosts will NOT be removed automatically when they are no longer needed.

C. Multiple hosts are added at a time when needed for memory or CPU.

D. After a storage scale-out event is triggered, single hosts are added every 30 minutes.

E. High threshold for storage, like the other policies, is set at 75%.

F. To resolve constraints related to CPU and memory, hosts are added two at a time.

ANSWER: A C F

Explanation:

Adds hosts incrementally when needed for storage.

This policy adds multiple hosts at a time when needed for memory or CPU, his policy adds multiple hosts at a time when needed for memory or CPU, and adds hosts incrementally when needed for storage. By default, hosts are added two at a time.

Reference: https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-operations/GUID-961C4B32-6093-4C2E-AFE5-5B1F56BF4EEE.html