



- Expert Verified, Online, **Free**.



CERTIFICATION TEST

- CertificationTest.net - Cheap & Quality Resources With Best Support

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.

Suggested Answer: BD

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.

praw709528

Community vote distribution



SDDC_Guy 2 years, 2 months ago

Selected Answer: BD

B- As VMW put it... <https://cormachogan.com/2018/11/01/a-closer-look-at-ebs-backed-vsan/>

D- Costly to replace i3 hosts with i3en

upvoted 1 times

SDDC_Guy 2 years, 2 months ago

I passed bigly

upvoted 1 times

🗳️ 👤 **n20d** 2 years, 5 months ago

Selected Answer: AD

I'm going with A and D, as you can mount EFS to esxi hosts, create a datastore and then svmotion the vm's across, or you can add more hosts to increase the vsan storage.

Here are the options -> <https://aws.amazon.com/blogs/storage/storage-options-and-designs-for-vmware-cloud-on-aws/>

upvoted 3 times

🗳️ 👤 **ultrium** 2 years, 5 months ago

You can't use EFS as datastore.

upvoted 3 times

🗳️ 👤 **Dmytros** 2 years, 8 months ago

Selected Answer: BD

BD

<https://cormachogan.com/2018/11/01/a-closer-look-at-ebs-backed-vsan/>

<https://vmc.techzone.vmware.com/resource/feature-brief-elastic-vsan#section2>

upvoted 2 times

🗳️ 👤 **PSE_IT** 2 years, 8 months ago

Selected Answer: BD

<https://vmc.techzone.vmware.com/resource/feature-brief-elastic-vsan#section2>

upvoted 2 times

🗳️ 👤 **lentzy** 2 years, 9 months ago

Selected Answer: CD

I am going wiht C and D

upvoted 2 times

🗳️ 👤 **BoDaddy** 2 years, 10 months ago

I am going with C & D

upvoted 1 times

🗳️ 👤 **Bobob55** 2 years, 10 months ago

Selected Answer: CD

C and d

upvoted 2 times

🗳️ 👤 **amit88** 3 years, 1 month ago

C AND D

upvoted 1 times

🗳️ 👤 **Rabbit117** 3 years, 4 months ago

I think A and D. You can mount and EFX filesystem to the Storage bound VMs and move some of their data to that.

upvoted 1 times

🗳️ 👤 **Rabbit117** 3 years, 3 months ago

Having read the answers again I now think that correct answer is C and D. Answer A says that the EFS file share would be connected to the i3.Metal host, however this would not be the case, the file share would be connected to the VM, not the host.

upvoted 2 times

🗳️ 👤 **itexampro092** 3 years, 5 months ago

B is not a supported option now, earlier it was supported with r5.metal and Elastic vSAN. Hence C and D will be correct.

upvoted 2 times

🗳️ 👤 **nemisis95** 3 years, 5 months ago

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.

upvoted 3 times

🗳️ 👤 **Cccb35** 3 years, 5 months ago

I think, the correct answers are C and D

upvoted 4 times

🗳️ 👤 **ocaptnmycaptn** 3 years, 5 months ago

Agreed

upvoted 3 times

Which API endpoint serves as the authentication point for VMware Cloud on AWS?

- A. Cloud Services Platform API
- B. NSX-T Data Center API
- C. Deployed SDDC API
- D. VMware Cloud on AWS API

Suggested Answer: A

Reference:

<https://blogs.vmware.com/code/2017/11/30/overview-vmware-cloud-aws-api/#:~:text=The%20CSP%20API%2C%20which%20serves,is%20the%20SDDC%20management%20point>

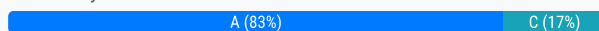
Cloud Services Platform API

The Cloud Services Platform (CSP) APIs are available for all cloud services which are offered by VMware. They contain the core features that customers will use when working with multiple cloud services from VMware.

In the context of VMware Cloud on AWS, the main use of the CSP APIs will be to serve as the authentication point. Once authenticated, the authorization token will be valid against this API as well as the VMware Cloud on AWS API. The CSP API also serves as the main point for Organization (Org) and VMware Cloud on AWS console user management. Some of the methods include displaying all the users within an Org, adding users to an Org, and removing users from an Org.

praw709528

Community vote distribution



🗳️ 👤 **SDDC_Guy** 2 years, 2 months ago

Selected Answer: A

A all day

upvoted 1 times

🗳️ 👤 **Blair77** 2 years, 6 months ago

Selected Answer: A

A is good!

upvoted 2 times

🗳️ 👤 **lentzy** 2 years, 9 months ago

Selected Answer: A

I am going with A

upvoted 2 times

🗳️ 👤 **BoDaddy** 2 years, 10 months ago

I agree with A

upvoted 3 times

🗳️ 👤 **Bobob55** 2 years, 10 months ago

Selected Answer: C

C for sure

upvoted 1 times

🗳️ 👤 **Bobob55** 2 years, 10 months ago

I meant a

upvoted 2 times

🗳️ 👤 **Rabbit117** 3 years, 3 months ago

I agree with A.

upvoted 4 times

An environment is running a cluster with six i3.metal hosts in the VMware Cloud on AWS software-defined data center (SDDC). If one host fails, what happens after a new host is automatically added to the cluster?

- A. The SDDC and NVMe drives backing VMware vSAN capacity are unmounted from the failed host and attached to the new host. There is no VMware vSAN rebuild required.
- B. The VMware vSAN rebuild starts in the background. Performance might be degraded during rebuild and the failures to tolerate (FTT) is lowered to 0.
- C. The VMware vSAN rebuild starts in the background. Performance might be degraded during rebuild and the failures to tolerate (FTT) is lowered to 1.
- D. A notification is received from VMware Support to start the VMware vSAN rebuild. Performance might be degraded during rebuild.

Suggested Answer: C

Reference:

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vsphere.vmc-aws-manage-data-center-vms.doc/GUID-EDBB551B-51B0-421B-9C44-6ECB66ED660B.html>

VMware Cloud on AWS Managed Storage Policy Profiles

When you create a cluster in your SDDC, VMware Cloud on AWS creates a managed storage policy profile that is applied by default to VMs that you create in the cluster. This storage policy profile is named "VMC Workload Storage Policy - *cluster name*". The policy settings ensure that the cluster meets the requirements outlined in the [Service Level Agreement for VMware Cloud on AWS](#) (the SLA). When you migrate a VM to a different cluster in the same SDDC, you must also change the VM storage policy. See [Assign Storage Policies to Virtual Machines](#).

Managed storage policy settings are based on the cluster configuration:

- Single host SDDCs are not covered by the SLA. They use a **No data redundancy** policy.
- Single-AZ clusters use thin provisioning and set a failure tolerance value based on cluster size and the host instance type:
 - Clusters containing 2 to 5 hosts use **1 failure - RAID-1 (Mirroring)**.
 - Clusters containing 6 or more hosts use **2 failures - RAID-6 (Erasure Coding)**.
- Stretched clusters with up to four hosts use **No data redundancy** and have **Site Disaster Tolerance** set to **Dual Site Mirroring**.
- Stretched clusters with six or more hosts use **1 failure - RAID-1 (Mirroring)**, but also have **Site Disaster Tolerance** set to **Dual Site Mirroring**.

prw709528

Community vote distribution

C (100%)

🗳️ 👤 **miguelfr** 2 years, 1 month ago

C is correct

upvoted 1 times

🗳️ 👤 **SDDC_Guy** 2 years, 2 months ago

Selected Answer: C

C is the winner

upvoted 1 times

🗨️ 👤 **[Removed]** 2 years, 5 months ago

Correct Answer is AD. I work in support so i know answer B is incorrect.

Look for vmware docs not aws here.

upvoted 1 times

🗨️ 👤 **BoDaddy** 2 years, 10 months ago

I agree with C

upvoted 2 times

🗨️ 👤 **Bobob55** 2 years, 10 months ago

C and ftt is reduced until new host is rebuilt

upvoted 2 times

🗨️ 👤 **PaulArup** 2 years, 10 months ago

C is correct. As the Cluster has 6 hosts, it means it has FTT 2. Once host down means it reduced to FTT 1.

<https://blogs.vmware.com/virtualblocks/2019/10/28/2-failure-toleration-requirements-within-vmware-cloud-on-aws/>

upvoted 2 times

🗨️ 👤 **chistensen** 3 years, 1 month ago

I think that is D, since you will get a new host, and the performance will be degraded for a few mins, so there will be no change to the FTT

upvoted 2 times

An administrator deploys a virtual machine and configures it to perform backups to an AWS Simple Storage Service (S3) bucket. After the first month of use, the administrator receives a bill from AWS indicating egress charges were applied to the backup traffic leaving the software-defined data center (SDCC), destined for the AWS S3 bucket. What can the administrator do to ensure backup traffic travels to the linked Amazon Virtual Private Cloud (VPC) through the Elastic Network Interface?

- A. Configure the S3 bucket with a public endpoint accessible over the Internet through HTTPS.
- B. Configure Direct Connect to a private virtual interface for access to AWS services.
- C. Create a gateway endpoint in the linked AWS VPC and configure it for use with the S3 bucket.
- D. Configure a route-based virtual private network (VPN) for the SDCC to the VPC.

Suggested Answer: D

Reference:

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

Community vote distribution

C (100%)

🗳️ 👤 **Cccb35** Highly Voted 👍 3 years, 5 months ago

Selected Answer: C

In AWS, when you want to redirect S3 traffic, Endpoints are used, in this way the traffic does not leave the AWS site through the Internet and the traffic is processed locally, this is a typical use with backup solutions .

upvoted 7 times

🗳️ 👤 **SDDC_Guy** Most Recent ⌚ 2 years, 2 months ago

Selected Answer: C

Once again, C

upvoted 1 times

🗳️ 👤 **[Removed]** 2 years, 5 months ago

Selected Answer: C

Correct is C as the traffic will leave SDCC to connect VPC via the ENI and then to the S3 via endpoint.

upvoted 2 times

🗳️ 👤 **BoDaddy** 2 years, 10 months ago

I agree with C

upvoted 2 times

🗳️ 👤 **Rabbit117** 3 years, 4 months ago

I agree with .C

upvoted 2 times

🗳️ 👤 **nemesis95** 3 years, 5 months ago

C. Create a gateway endpoint in the linked AWS VPC and configure it for use with the S3 bucket.

upvoted 3 times

A customer wants to ensure that VMware Cloud on AWS maintenance operations are performed during their maintenance window. Which option would allow the customer to achieve this outcome?

- A. Schedule a maintenance preference in the software-defined data center (SDDC) console.
- B. Schedule a call with VMware Cloud on AWS Support and schedule a maintenance window.
- C. Schedule a call with AWS Support and schedule a maintenance window.
- D. Schedule a maintenance window through an online support request.

Suggested Answer: A

Reference:

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/solutions/VMware-Cloud-on-AWS.39646badb412ba21bd6770ef62ae00a2/GUID-7CE2A5683B08C2C5CB0A1A373570D1F2.html>

SDDC Maintenance

VMware is responsible for managed delivery of SDDC software updates and emergency patches. This involves maintaining consistent software versions across the SDDC fleet with continuous delivery of features and bug fixes. VMware is mindful of customer IT processes and ensures the minimum impact of changes. Detailed information is available in [SDDC Upgrades and Maintenance](#) page.

praw709538

Community vote distribution

A (100%)

🗳️ 👤 **SDDC_Guy** 2 years, 2 months ago

Selected Answer: A

A most logical

upvoted 1 times

🗳️ 👤 **BoDaddy** 2 years, 10 months ago

I agree with A

upvoted 2 times

🗳️ 👤 **Mellashellas** 3 years, 4 months ago

Selected Answer: A

A – though this option is removed in latest SDDC Version (1.16)

upvoted 4 times

An administrator runs an analysis on all workloads using Live Optics and confirms there are a variety of applications, including Microsoft SQL server and Oracle databases. The Microsoft SQL workloads are averaging 4,000 IOPS per virtual machine, approximately 50% writes. The Oracle workloads are averaging 3,000 IOPS per virtual machine, and approximately 80% writes. Which method should be used to input the data into the VMware Cloud on AWS Sizer for the most accurate results?

- A. Use the Advanced Sizer in 'database' mode. Create workload profiles for the analyzed virtual machines, including profiles for Microsoft SQL and Oracle. Set the values for vCPU, vRAM, utilized storage, IOPS and I/O profile manually.
- B. Use the Quick Sizer. Set the values for vCPU, vRAM, utilized storage, IOPS and I/O profile manually.
- C. Use the Advanced Sizer in 'import' mode. Import the Live Optics data and let the Advanced Sizer set the values for vCPU, vRAM, utilized storage, IOPS and I/O automatically.
- D. Use the Advanced Sizer in 'manual' mode. Create workload profiles for the analyzed virtual machines, including profiles for Microsoft SQL and Oracle. Use the default values for the SQL and Oracle workload profiles.

Suggested Answer: D

Community vote distribution

C (100%)

🗳️ 👤 **SDDC_Guy** 2 years, 2 months ago

Selected Answer: C

C all day

upvoted 1 times

🗳️ 👤 **ieee13940** 2 years, 8 months ago

While I agree with C, which one passes in the exam? XD

upvoted 3 times

🗳️ 👤 **BoDaddy** 2 years, 10 months ago

C - Advanced mode you can import Live Optics or RVTools

upvoted 2 times

🗳️ 👤 **Rabbit117** 3 years ago

I agree C is the best answer.

upvoted 2 times

🗳️ 👤 **MellasHellas** 3 years, 4 months ago

Selected Answer: C

C – There is no 'database mod'e. Quick sizer doesn't do IOPs or IO. Manual mode with default values wont match IOPs and I/O specified here exactly.

upvoted 4 times

An administrator has deployed VMware Cloud on AWS and requires a single broadcast domain for a set of virtual machines that reside both in the data center and in the software-defined data center (SDDC) over a DirectConnect connection. How can the administrator accomplish this without adding additional components in the cloud?

- A. Duplicate the IP space in both locations and manually move the virtual machines.
- B. Deploy a Layer 2 Virtual Private Network (L2VPN).
- C. Use a third-party networking tool to extend the broadcast domain.
- D. Deploy VMware HCX and a Service Mesh with a Network Extension appliance.

Suggested Answer: B

Reference:

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vmw-deploy-horizon-seven-on-vmware-cloud-on-aws.pdf>

Community vote distribution

B (100%)

 **Cccb35** Highly Voted 3 years, 5 months ago

Selected Answer: B

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.networking-security/GUID-8BBB5707-8FB3-4F05-AEC3-668FD8EA6B8E.html>


upvoted 8 times

 **SDDC_Guy** Most Recent 2 years, 2 months ago

Selected Answer: B

B is the right choice

upvoted 1 times

 **BoDaddy** 2 years, 10 months ago

B - You can use a VMware Cloud on AWS layer 2 Virtual Private Network (L2VPN) to extend your on-premises network to one or more VLAN-based networks in your SDDC. This extended network is a single subnet with a single broadcast domain. You can use it to migrate VMs to and from your cloud SDDC without having to change their IP addresses

upvoted 2 times

 **Rabbit117** 3 years ago

B is correct.

upvoted 2 times

What are two benefits of completing a full data center evacuation to VMware Cloud on AWS? (Choose two.)

- A. Reduce the risk of migrating applications to the cloud by removing the need for application transformation.
- B. Maintain existing investment in skills and toolsets.
- C. Provide a hybrid cloud management solution.
- D. Provide a seamless way to expand the on-premises software-defined data center (SDDC) into the cloud.
- E. Diversify the risk associated with migrating applications to the cloud by automatically deploying workloads to multiple regions.

Suggested Answer: AD

Reference:

https://www.vmware.com/content/dam/learn/en/amer/fy20/pdf/333278_20Q3_WW_GLB_20ALL_WebForm_VMC_REG_20210823.pdf

In this approach workloads are moved to VMware Cloud on AWS without any changes required to the applications and IT processes need only change to the extent to which they are necessary, which typically is minimal. Also, existing IT operational management tools from the legacy infrastructure can be leveraged on the new VMware Cloud platform, again maximizing the value of existing knowledge and investments.

Multiple reasons for this business approach might exist. Perhaps they simply see no value in managing infrastructure and wish to shift attention from infrastructure lifecycle management to digital transformation. Or perhaps they are having difficulty hiring or retaining skilled staff and want to automate, streamline, and accelerate IT service delivery and management, to focus on supporting the needs of the business.

As we have seen, the VMware HCX service is a perfect fit to address data center evacuation use cases and enables transparent workload migration to the VMware Cloud SDDC, with features such as:

- Migration scheduling— enabling scheduled migrations during a specific maintenance window
- A Layer-2 network extension, simplifying workload migration by allowing an application to migrate without requiring an IP address change
- WAN optimization, including data deduplication and compression to reduce the migration timeframe and network bandwidth requirement

Community vote distribution

AB (100%)

 **MellasHellas** Highly Voted 3 years, 4 months ago

Selected Answer: AB

C & D are Hybrid, not full datacentre evacuation. VMC is multi-AZ, not multi-region and it (stretched cluster) isn't automatic.


upvoted 6 times

 **Rabbit117** Highly Voted 3 years, 3 months ago

I think A and B. A. When moving to VMC on AWS there is no need to refactor the apps.

B. The skills required for managing on-prem SDDC are the same as those for VMC on AWS.

upvoted 5 times

 **SDDC_Guy** Most Recent 2 years, 2 months ago

Selected Answer: AB

removing need for application transformation is key along with not learning new skills.

upvoted 1 times

 **chistensen** 2 years, 5 months ago

Provide a hybrid cloud management solution. This will allow the administrator to manage both the on-premises software-defined data center (SDDC) and the VMware Cloud on AWS environment using the same tools and processes. The letter for this option is A.

Maintain existing investment in skills and toolsets. By completing a full data center evacuation, the administrator can continue to use their existing skills and toolsets, such as vSphere and vCenter, to manage the workloads in the VMware Cloud on AWS environment. The letter for this option is B.

Therefore, the correct answer is A and B.



upvoted 2 times

  **chistensen** 2 years, 5 months ago

Option A is incorrect because completing a full data center evacuation does not remove the need for application transformation. Depending on the workloads being migrated, the administrator may still need to make changes to the applications to ensure that they can run effectively in the cloud.



Option C is incorrect because providing a hybrid cloud management solution is one of the benefits of completing a full data center evacuation.

upvoted 2 times

  **ultrium** 2 years, 5 months ago

A is correct. As lift and shift migration, you don't need to transform the application.

upvoted 3 times

  **BoDaddy** 2 years, 10 months ago

I agree with A & B

upvoted 4 times

A new VMware Cloud on AWS customer has previously deployed a VMware Horizon-based VDI solution into their data center to support their remote developer workforce. Due to unforeseen growth, the company needs to quickly expand their remote workforce. The growth will consume any forecast capacity in the VDI solution and, therefore, additional capacity is now required. The VDI solution service owner would like the solution to support the ability to quickly scale in/out to provide additional capacity based on demand. Which three steps should the administrator take to scale out the VDI solution? (Choose three.)

- A. Deploy a new VMware Horizon pod on VMware Cloud on AWS.
- B. Deploy a new VMware Horizon pod on-premises.
- C. Configure network connectivity and firewall rules to allow communications between the two on-premises connection servers.
- D. Configure network connectivity and firewall rules to allow communications between on-premises and VMware Cloud on AWS connection servers.
- E. Connect the two VMware Horizon pods together using the security servers.
- F. Connect the two VMware Horizon pods together using a Horizon Cloud Pod Architecture (CPA).

Suggested Answer: BDF

Reference:

<https://techzone.vmware.com/resource/horizon-on-vmware-cloud-on-aws-architecture>

Linking Horizon Pods with CPA

You can use the Cloud Pod Architecture feature to connect Horizon pods regardless of whether the pods are on-premises or on VMware Cloud on AWS. When you deploy two or more Horizon pods on VMware Cloud on AWS, you can manage them independently or manage them together by linking them with Cloud Pod Architecture.

- On one Connection Server, initialize Cloud Pod Architecture and join the Connection Server to a pod federation.
- Once initialized, you can create a global entitlement across your Horizon pods on-premises and on VMware Cloud on AWS.
- Optionally, when you use Cloud Pod Architecture, you can deploy a global load balancer (such as F5, AWS Route 53, or others) between the pods. The global load balancer provides a single-namespace capability that allows the use of a common global namespace when referring to Horizon CPA. Using CPA with a global load balancer provides your end users with a single connection method and desktop icon in their Horizon Client or Workspace ONE console.

Without the global load balancer and the ability to have a single namespace for multiple environments, end users will be presented with a possibly confusing array of desktop icons (corresponding to the number of pods on which desktops have been provisioned for them). For more information on how to set up Cloud Pod Architecture, see the [Administering Cloud Pod Architecture in Horizon](#).

Use Cloud Pod Architecture to link any number of Horizon pods on VMware Cloud on AWS. The maximum number of pods must conform to the limits set for pods in Cloud Pod Architecture. For the most current numbers for Horizon 8, see the [Horizon 8 2012 Configuration Limits](#). For Horizon 7, see the VMware Knowledge Base article [VMware Horizon 7 Sizing Limits and Recommendations \(2150348\)](#).

When you connect multiple Horizon pods together with Cloud Pod Architecture, the Horizon versions for each of the pods can be different from one another.

praw709528

Community vote distribution

ADF (100%)

Cccb35 **Highly Voted** 3 years, 5 months ago

For me A, D & F
upvoted 12 times

SDDC_Guy **Most Recent** 2 years, 2 months ago

Selected Answer: ADF

A, D, and F just make the best answer
upvoted 1 times

splint 2 years, 3 months ago

Selected Answer: ADF

ADF makes sense



upvoted 2 times

  **ccie_pgh** 2 years, 4 months ago

Selected Answer: ADF

new pod in cloud to scale quickly

upvoted 2 times

  **BoDaddy** 2 years, 10 months ago

I agree with A D F

upvoted 3 times

An administrator is trying to identify how many hosts will be required to evacuate a cluster from an existing data center and relocate those workloads into VMware

Cloud on AWS. The cluster runs a variety of workloads for the corporate customer relationship management system. Which three profiles could the administrator create in the VMware Cloud on AWS Sizer? (Choose three.)

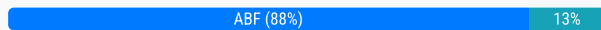
- A. Databases 1€" Oracle
- B. Databases 1€" Microsoft SQL Server
- C. General Purpose (Application VMs)
- D. VDI 1€" Instant Clone
- E. VDI 1€" Full Clone
- F. General Purpose (General VMs)

Suggested Answer: BEF

Reference:

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

Community vote distribution



Cccb35 Highly Voted 3 years, 5 months ago

A, B & F

upvoted 11 times

MellasHellas Highly Voted 3 years, 4 months ago

Selected Answer: ABF

VDI clones wont be part of a CRM system

upvoted 5 times

Salar Most Recent 2 years, 1 month ago

A, B, and F

<https://vmc.vmware.com/sizer/quick-sizing>

upvoted 1 times

SDDC_Guy 2 years, 2 months ago

Selected Answer: BEF

B, E, F are part of the sizer.

upvoted 1 times

Blair77 2 years, 6 months ago

Selected Answer: ABF

No need to evaluate the VDI workload. A-B-F

upvoted 2 times

BoDaddy 2 years, 10 months ago

I agree with A B F

upvoted 2 times

Rabbit117 3 years, 3 months ago

A, B and F.

upvoted 4 times

An administrator deploys a VMware Cloud on AWS environment and configures an IPsec virtual private network (VPN) tunnel to their data center. Hybrid Linked Mode connectivity, however, does NOT appear to be working. Before contacting VMware Support, what could the administrator do to narrow down the possible issue?

- A. Fill in the relevant IP information for the on-premises infrastructure and run the desired troubleshooting connectivity test.
- B. Download and review the Tier-0 (TO) gateway firewall logs.
- C. Configure a packet capture device in the on-premises data center to capture packets from the VMware Cloud on AWS software-defined data center (SDDC) to determine which packets are being dropped.
- D. Configure a packet capture appliance on a local segment within VMware Cloud on AWS to capture and analyze traffic across a specific NSX-T gateway interface.

Suggested Answer: A

Reference:

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

Community vote distribution


A (100%)

 **MellasHellas** Highly Voted 3 years, 4 months ago

A - You can use the network troubleshooting functionality in the VMC Console or as part of the Hybrid Linked Mode functionality in the Cloud Gateway Appliance to troubleshoot network connectivity for Hybrid Linked Mode.

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vsphere.vmc-aws-manage-data-center-vms.doc/GUID-16A52EDA-3CB2-44AD-B649-C82C4AC255B9.html>


upvoted 5 times

 **SDDC_Guy** Most Recent 2 years, 2 months ago

Selected Answer: A

A seems best


upvoted 1 times

 **Blair77** 2 years, 6 months ago

Selected Answer: A

A for sure

upvoted 2 times

 **BoDaddy** 2 years, 10 months ago

I would go with A

upvoted 2 times

 **lentzy** 2 years, 10 months ago

did you pass the exam?

upvoted 2 times

When deploying a VMware Cloud on AWS software-defined data center (SDDC), which components are deployed automatically?

- A. VMware ESXi, vCenter, vSAN, NSX, Hybrid Linked Mode
- B. VMware ESXi, vCenter, vSAN, NSX in active/passive mode
- C. VMware ESXi, vCenter, vSAN, NSX, HCX
- D. VMware ESXi, vCenter, vSAN, NSX in active/active mode

Suggested Answer: C

Reference:

<https://aws.amazon.com/vmware/features/>

Bare Metal Cloud Infrastructure



VMware Cloud on AWS provides the VMware SDDC software stack to the highly scalable AWS Cloud, including vSphere, vSAN, NSX, and vCenter Server. Configuration for production environment can range in size for the SDDC cluster depending on the host type that is selected. View the current host types on the [VMware Cloud on AWS Pricing](#) page. You can deploy a fully configured VMware SDDC Cluster in under a few hours, and scale host capacity up and down in minutes.

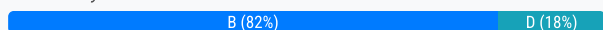
Dedicated High Performance Networking

VMware Cloud on AWS provides separate, dedicated high performance networks for management and application traffic, connected through the VMware NSX networking platform, and provides support for networking multicasting. ESXi hosts are connected to an Amazon Virtual Private Cloud (VPC) through Elastic Networking Adapter (ENA), which supports throughput up to 25 Gbps.



- **NSX and AWS Direct Connect Integration:** Now generally available, NSX integrates with AWS Direct Connect for end-to-end private networking. This is ideal for customers with traffic-heavy workloads. This enables private and consistent connectivity between VMware workloads running on AWS and those running on-premises and also accelerates migration to cloud and enables multi-tier hybrid applications. Customers can now use AWS Direct Connect for all of their hybrid connectivity requirements.

Community vote distribution



Rabbit117 Highly Voted 3 years, 3 months ago

NSX is deployed in an Active/Passive mode during the deployment along with ESXi, vCenter and vSAN. HCX is included with VMC on AWS for migrations but is not deployed during initial deployment.
upvoted 9 times

SDDC_Guy Most Recent 2 years, 2 months ago

Selected Answer: B

VMware just released VMC with NSX Active/Active. This test will not know that, so B, Active/Passive
upvoted 1 times

notVMwarepro 2 years, 3 months ago

Selected Answer: B

B is correct

upvoted 2 times

  **chistensen** 2 years, 5 months ago

Selected Answer: D

When deploying a VMware Cloud on AWS software-defined data center (SDDC), the following components are deployed automatically:

VMware ESXi

vCenter



vSAN

NSX

These components are all necessary for the operation of the SDDC, and they are deployed in an active/active configuration to provide high availability and resiliency.

Therefore, the correct answer is D. VMware ESXi, vCenter, vSAN, NSX in active/active mode.



upvoted 2 times

  **Blair77** 2 years, 6 months ago

Selected Answer: B



B is the good one

upvoted 2 times

  **BoDaddy** 2 years, 10 months ago

B is correct

upvoted 2 times

  **Cccb35** 3 years, 4 months ago

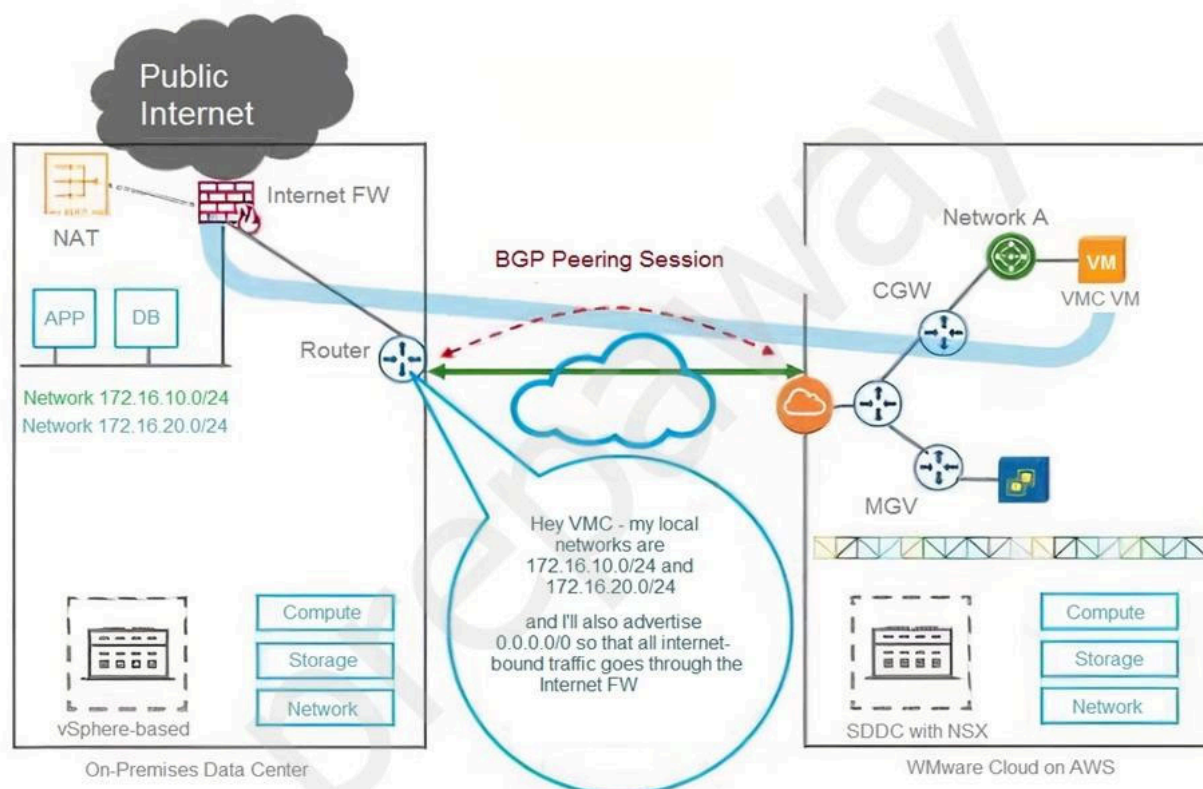
Selected Answer: B

The default NSX Edge Appliance is implemented as a pair of VMs that run in active/standby mode.

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.networking-security/GUID-658253DB-F384-4040-94B2-DF2AC3C9D396.html>

upvoted 4 times

Refer to the exhibit.



praw709528

An administrator completes an assessment of its local data center for potential migration into VMware Cloud on AWS. After reviewing and analyzing the data and taking into account the company's business and IT priorities and budget constraints, connectivity between its on-premises and VMware Cloud on AWS environment will NOT require any high speed low latency connections. All new networks should be added to the software-defined data center (SDDC) routing table automatically when created. Which connection supports these requirements?

- A. Layer 2 VPN (L2VPN)
- B. AWS Direct Connect
- C. Route-based VPN
- D. Policy-based VPN

Suggested Answer: D

Community vote distribution

C (100%)

Cccb35 Highly Voted 3 years, 5 months ago

Selected Answer: C

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.networking-security/GUID-5AF45CE6-FA53-45C0-83E5-25F8E3A055E9.html>

upvoted 12 times

acoman Most Recent 1 year, 8 months ago

I agree with C, as the others mentioned you find the answer in the training documents

upvoted 1 times

splint 2 years, 2 months ago

Selected Answer: C

Routing table is giveaway

upvoted 1 times

SDDC_Guy 2 years, 2 months ago

Selected Answer: C

C, right from training documents

upvoted 1 times

  **chistensen** 2 years, 5 months ago

Selected Answer: C



Option A is incorrect because a Layer 2 VPN (L2VPN) would not automatically add new networks to the SDDC routing table when they are created.

Option B is incorrect because AWS Direct Connect is a dedicated network connection that provides high-speed, low-latency connections between the on-premises data center and AWS. It is not suitable for this scenario because the administrator does not require high-speed, low-latency connections.

Option D is incorrect because a policy-based VPN does not automatically add new networks to the SDDC routing table when they are created. It is also not suitable for this scenario because the administrator does not require high-speed, low-latency connections.

Therefore, the correct answer is C. Route-based VPN.



upvoted 4 times

  **Blair77** 2 years, 6 months ago

Selected Answer: C

CCC - Let's GO!

upvoted 2 times

  **BoDaddy** 2 years, 10 months ago

C is correct

upvoted 2 times

  **Rabbit117** 3 years, 3 months ago

C is correct. with Route based VPN new routes are added automatically when new networks are created.

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-networking-security/GUID-92F6C09E-8E74-430E-8F79-C2E5B2150ADA.html>

upvoted 2 times

  **MellasHellas** 3 years, 4 months ago

Selected Answer: C

L3 not L2, no need for low latency of Direct Connect, When you use a policy-based VPN, you must update the routing tables on both ends of the network when new routes are added.

upvoted 4 times

A consultant is asked to help evaluate an environment for deployment into a new software-defined data center (SDDC) in VMware Cloud on AWS. The consultant is provided with a comma-separated value (CSV) file containing a list of workloads exported from VMware vCenter detailing only virtual machine configuration data, including vCPU, vRAM, and utilized storage. How should the consultant use the VMC on AWS Sizer?

- A. Use the Advanced Sizer. Create workload profiles for the different workload types and set the values for configured resources manually.
- B. Use the Advanced Sizer. Import the CSV file from VMware vCenter Server and let the VMware Cloud on AWS Sizer set the values for configured resources.
- C. Use the Advanced Sizer. Import the CSV file from VMware vCenter Server and let the VMware Cloud on AWS Sizer set the values for configured resources.
- D. Use the Quick Sizer. Manually enter the number of virtual machines and total resources for configured resources.

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **SDDC_Guy** 2 years, 2 months ago

Selected Answer: D

D is the only answer that works.

upvoted 1 times

🗳️ 👤 **Blair77** 2 years, 6 months ago

Selected Answer: D

D do the job - Let's GO!

upvoted 2 times

🗳️ 👤 **BoDaddy** 2 years, 10 months ago

D and yes duplicate answers for B & C

upvoted 3 times

🗳️ 👤 **DSITTA** 2 years, 10 months ago

error in the answers. B and C are the same.

upvoted 4 times

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.

Suggested Answer: A

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.

praw709528

Community vote distribution

D (100%)

 **Cccb35** Highly Voted 3 years, 5 months ago

Selected Answer: D

Ensure that access to S3 through the elastic network interface is enabled.

By default, S3 access through the elastic network interface in the connected Amazon VPC is enabled. If you disabled this access to allow S3 access through the internet gateway, you must re-enable it.

Log in to the VMC Console at <https://vmc.vmware.com>.

Click > Connected VPC

Under Service Access, click Enable next to S3 Endpoint.


<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-operations/GUID-B501FA3C-EAF9-4005-AC72-155C3F592281.html>

upvoted 8 times

 **BoDaddy** Highly Voted 2 years, 10 months ago

I am going with D


upvoted 5 times

 **SDDC_Guy** Most Recent 2 years, 2 months ago

Selected Answer: D

D is the only one that works.

upvoted 1 times

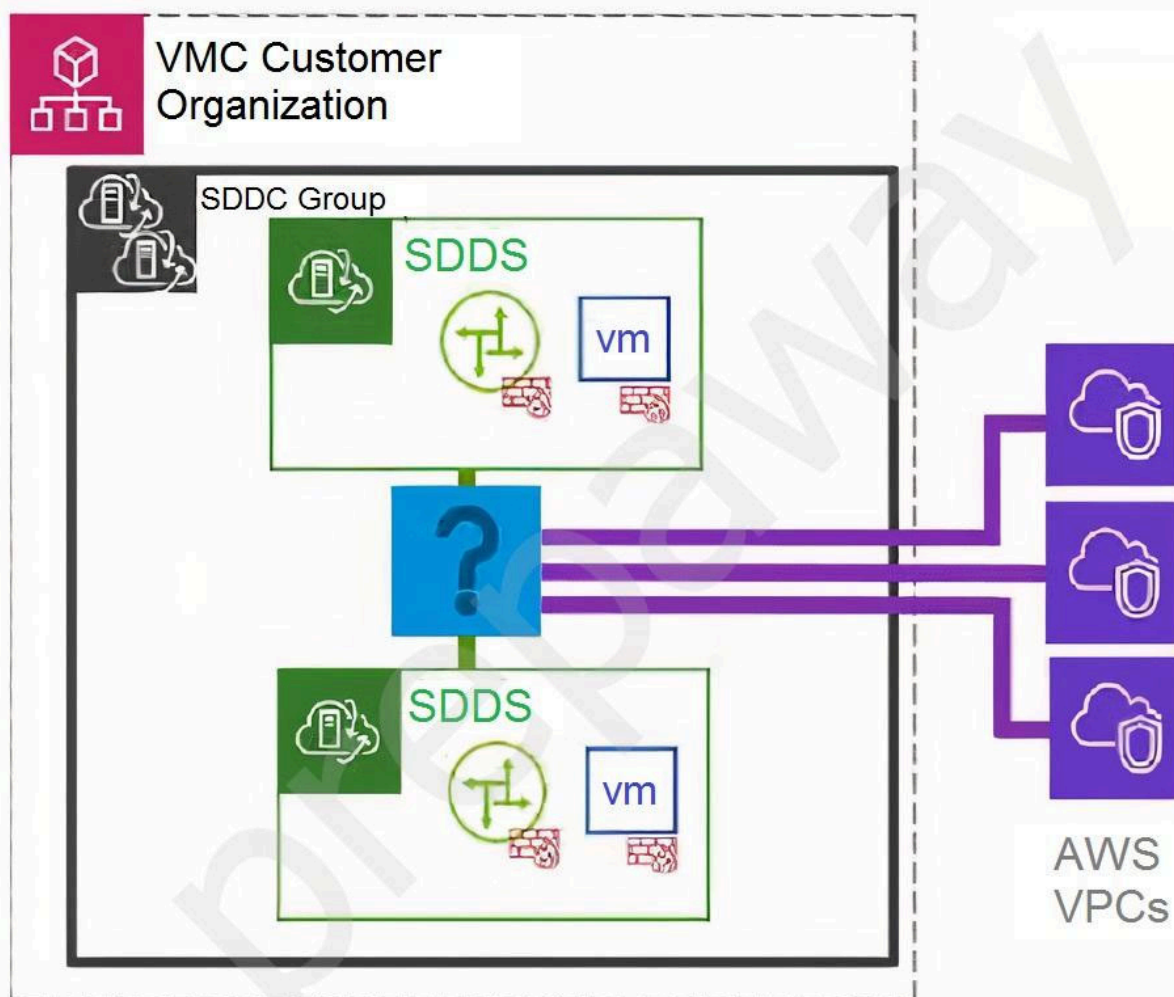
 **Blair77** 2 years, 6 months ago

Selected Answer: D

DDD - Let's GO!

upvoted 2 times

Refer to the exhibit.



An administrator builds a software-defined data center (SDDC) group to enable connectivity to native Amazon Virtual Private Clouds (VPCs). Which connectivity option is needed to enable connectivity across environments?

- A. Tier-0 (T0) Router
- B. Transit Gateway
- C. Virtual Private Network
- D. The Default Storage Scale-Out policy storage threshold is set 5% higher than the other Elastic DRS storage policies.

Suggested Answer: A

Community vote distribution

B (100%)

itexampro092 Highly Voted 3 years, 4 months ago

The answer is B. Yes, it is confusing but as per the diagram, VMware Transit Gateway would be the right fit.
upvoted 10 times

handraco Most Recent 2 years, 1 month ago

Selected Answer: B

B
<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-operations/GUID-C957DBA7-16F5-412B-BB72-15B49B714723.html>
upvoted 2 times

SDDC_Guy 2 years, 2 months ago

Selected Answer: B

This is all about Transit Gateway

upvoted 1 times

🗨️ 👤 **Blair77** 2 years, 6 months ago

Selected Answer: B

BBB - VMware Transit Gateway! Let's GO!

upvoted 2 times

🗨️ 👤 **BoDaddy** 2 years, 10 months ago

B is correct , check out Rabbit117's link it shows the EXACT diagram.

upvoted 3 times

🗨️ 👤 **Rabbit117** 3 years ago

B is correct. see diagram at the following link.

<https://vmc.techzone.vmware.com/resource/introduction-vmware-transit-gateway-vmware-cloud-aws#architecture>

upvoted 4 times

🗨️ 👤 **amit88** 3 years, 1 month ago

B is Correct

upvoted 3 times

🗨️ 👤 **amit88** 3 years, 1 month ago

Answer is B

upvoted 3 times

🗨️ 👤 **Rabbit117** 3 years, 3 months ago

I think B is correct. The T0 router would be part of the SDDC and connect to the transit GW.

upvoted 4 times

🗨️ 👤 **Cccb35** 3 years, 5 months ago

It's correct <https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-operations/GUID-C957DBA7-16F5-412B-BB72-15B49B714723.html>

upvoted 3 times

🗨️ 👤 **Cccb35** 3 years, 4 months ago

I agree with itexampro092

upvoted 4 times

Which two statements are true about the characteristics of the Default Storage Scale-Out policy? (Choose two.)

- A. Elastic DRS automatically sets to the Default Storage Scale-Out policy, adding hosts only when storage utilization exceeds a certain threshold.
- B. When the storage threshold of the Default Storage Scale-Out policy has been resolved, Elastic DRS automatically performs a scale-in operation.
- C. The Default Storage Scale-Out policy storage threshold level is set to meet SLA requirements and can not be superseded by other Elastic DRS policies.
- D. The Default Storage Scale-Out policy thresholds for CPU or memory usage are set higher than the other Elastic DRS policies.
- E. The Default Storage Scale-Out policy storage threshold is set 5% higher than the other Elastic DRS storage policies.

Suggested Answer: AC

Reference:

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

Select Elastic DRS Policy

Feedback

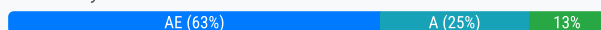
Share

Updated on 09/28/2021

Set the Elastic DRS policy on a cluster to optimize for your workloads' needs.

In a new SDDC, elastic DRS uses the **Default Storage Scale-Out** policy, adding hosts only when storage utilization exceeds the threshold of 75%. You can select a different policy if it provides better support for your workload VMs. For any policy, scale-out is triggered when a cluster reaches the high threshold for any resource. Scale-in is triggered only after all of the low thresholds have been reached. See [How the Elastic DRS Algorithm Works](#) for more information about EDRS scale-out and scale-in logic.

Community vote distribution



MellasHellas Highly Voted 3 years, 4 months ago

A, E. Question is out of date, the 'Default Storage Scale-Out policy' has been superseded by the 'Elastic DRS Baseline policy', adding hosts after storage utilization reaches 80% (not 75%)
upvoted 5 times

gv84 Most Recent 1 year, 5 months ago

A & C
I go with A & C, as Scale-Out threshold for Storage is same 80% across all 4 policies
upvoted 1 times

SDDC_Guy 2 years, 2 months ago

Selected Answer: AC

These are the only correct two answers. The question is old.
upvoted 1 times

Blair77 2 years, 6 months ago

Selected Answer: A

A is good. But this is an outdated question.
<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-operations/GUID-961C4B32-6093-4C2E-AFE5-5B1F56BF4EEE.html>
upvoted 2 times

BoDaddy 2 years, 10 months ago

I agree with A & E



upvoted 2 times

  **Rabbit117** 3 years ago

Selected Answer: AE

I agree with MellasHellas.

upvoted 2 times

  **MJ_PL** 3 years, 4 months ago

Selected Answer: AE

A as it always scale out for storage

E as all the other policies are 70%

upvoted 3 times

Which two accounts are mandatory prerequisites for the successful deployment of a VMware Cloud on AWS solution? (Choose two.)

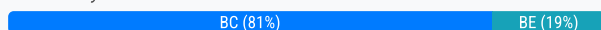
- A. A VMware vCenter Server account
- B. An AWS account
- C. A VMware Cloud account
- D. An Amazon Elastic Compute Cloud (EC2) account
- E. A VMware Cloud on AWS account

Suggested Answer: AE

Reference:

<https://d1.awsstatic.com/whitepapers/sddc-deployment-and-best-practices.pdf>

Community vote distribution



MellasHellas Highly Voted 3 years, 4 months ago

Selected Answer: BC

A VMware Cloud account is used to sign into all VMware Cloud services, including VMC.

upvoted 9 times

handraco Most Recent 2 years, 1 month ago

Selected Answer: BE

<https://d1.awsstatic.com/whitepapers/sddc-deployment-and-best-practices.pdf>

Follow this document page 6-7. It's B,E

upvoted 1 times

SDDC_Guy 2 years, 2 months ago

Selected Answer: BC

Requires AWS and VMware Cloud Accounts to access SDDC

upvoted 1 times

splint 2 years, 3 months ago

Selected Answer: BE

AWS Account and VMware Cloud on AWS per the requirements section in <https://d1.awsstatic.com/whitepapers/sddc-deployment-and-best-practices.pdf>

upvoted 2 times

Blair77 2 years, 6 months ago

Selected Answer: BC

B & C are good for me

upvoted 2 times

n20d 2 years, 6 months ago

says AWS account and VMware Cloud on AWS account here: <https://docs.aws.amazon.com/whitepapers/latest/sddc-deployment-and-best-practices/account-requirements.html>

B & E

upvoted 2 times

BoDaddy 2 years, 10 months ago

B & C are correct


upvoted 4 times

Rabbit117 3 years ago

However... the AWS doc at the link <https://d1.awsstatic.com/whitepapers/sddc-deployment-and-best-practices.pdf> calls out the AWS Account and VMware cloud on AWS account (Page5). The other two VMware links which I have added in previous comments all refer to the VMware account as either VMware Cloud Account or VMware Cloud services account. So it appears that both B & C and B & E are correct depending on whether you read the VMware or AWS docs.

I think, as this is a VMware Exam, I will go with B&C.

upvoted 4 times

  **Rabbit117** 3 years ago

Selected Answer: BC

Also see

<https://blogs.vmware.com/cloud/2019/02/27/understanding-accounts-roles-privileges-vmware-cloud-aws/>



upvoted 1 times

  **Rabbit117** 3 years ago

I think B and C are correct.

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.getting-started/GUID-9CAB2B3E-42D5-44A1-9428-E8FFD22BDD01.html#:~:text=VMware%20Cloud%20accounts%20are%20based,additional%20users%20to%20the%20account.>

upvoted 3 times

  **Cccb35** 3 years, 5 months ago

B & E are corrects

upvoted 4 times

An architect is designing a company's hybrid cloud environment. Traffic between their local data center and VMC on AWS software-defined data center (SDDC) requires a high-speed, low latency connection. The connection type should also support connectivity to services currently being consumed in AWS. Which connection type will meet these requirements?

- A. Multiprotocol Label Switching (MPLS)
- B. AWS Direct Connect
- C. Four IPSec tunnels for greater bandwidth & resiliency
- D. Route-based VPN

Suggested Answer: B

Reference:

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

(18)

AWS Direct Connect is a service provided by AWS that allows you to create a high-speed, low latency connection between your on-premises data center and AWS services. When you configure AWS Direct Connect, VPNs can use it instead of routing traffic over the public Internet. Because Direct Connect implements Border Gateway Protocol (BGP) routing, use of an L3VPN for the management network is optional when you configure Direct Connect. Traffic over Direct Connect is not encrypted. If you want to encrypt that traffic, you can configure an IPsec VPN that uses private IP addresses and Direct Connect.

praw709528

Community vote distribution

B (100%) **handraco** 2 years, 1 month ago**Selected Answer: B**


No doubt.

upvoted 1 times

 **SDDC_Guy** 2 years, 2 months ago**Selected Answer: B**


B it is

upvoted 1 times

 **Blair77** 2 years, 6 months ago**Selected Answer: B**

BBB - Let's GO!

upvoted 2 times

 **BoDaddy** 2 years, 10 months ago**Selected Answer: B**

B - Direct Connect

upvoted 2 times

An administrator is asked to create a new network segment in VMware Cloud on AWS. This network segment should be accessible from the on-premises data center. How would the administrator create this new network and what segment type should it be?

A.

- ⇒ Connect to the on-premises VMware vCenter Server and create the network segment through the VMware vSphere user interface.
- ⇒ Select the stretched network segment type.

B.

- ⇒ Connect to the VMware Cloud console to create the network segment.
- ⇒ Select the routed network segment type.

C.

- ⇒ Connect to the VMware Cloud console to create the network segment.
- ⇒ Select the extended network segment type.

D.

- ⇒ Connect to the VMware Cloud on AWS vCenter Server and create the network segment through the VMware vSphere user interface.
- ⇒ Select the routed network segment type.

Suggested Answer: C

Reference:

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.networking-security/GUID-267DEADB-BD01-46B7-82D5-B9AA210CA9EE.html> -

VMware Cloud on AWS supports three types of network segments: routed, extended and disconnected.

- A routed network segment (the default type) has connectivity to other logical networks in the SDDC and, through the SDDC firewall, to external networks.
- An extended network segment extends an existing L2VPN tunnel, providing a single IP address space that spans the SDDC and an on-premises network.
- A disconnected network segment has no uplink, and provides an isolated network accessible only to VMs connected to it. Disconnected segments are created when needed by HCX (see [Getting started with VMware HCX](#)). You can also create them yourself, and can convert them to other segment types.

praw709528

👤 **PaulAuchon** Highly Voted 3 years, 1 month ago

B - no need to have L2 extension so the segment is not extended
upvoted 5 times

👤 **Mellashellas** Highly Voted 3 years, 4 months ago

C - Segments are created in the Cloud Console. Extended segments provide a single IP address space that spans the SDDC and an on-premises network.

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.networking-security/GUID-267DEADB-BD01-46B7-82D5-B9AA210CA9EE.html>
upvoted 5 times

👤 **gv84** Most Recent 1 year, 5 months ago

Will go with B. Key point to look is "Should be accessible from On-Premises DC". Question didn't mention about should be usable.
upvoted 1 times

👤 **wuwu** 2 years ago

I think B
upvoted 1 times

👤 **handraco** 2 years, 1 month ago

B is correct.

C only if you have L2VPN Tunnel.



<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.networking-security/GUID-267DEADB-BD01-46B7-82D5-B9AA210CA9EE.html>

upvoted 1 times

  **SDDC_Guy** 2 years, 2 months ago



I feel B is best

upvoted 1 times

  **splint** 2 years, 3 months ago



No L2 so B

upvoted 3 times

  **Blair77** 2 years, 6 months ago

B - Let's GO!

upvoted 2 times

  **BoDaddy** 2 years, 10 months ago

I agree with C

upvoted 3 times

What is a supported approach when deploying multiple instances of VMware Site Recovery with VMware Cloud on AWS?

- A. A single software-defined data center (SDDC) paired with up to 25 remote sites
- B. A single software-defined data center (SDDC) connected to multiple on-premises sites and to other cloud SDDCs
- C. VMware Site Recovery add-on deployed in the VMware vSphere Web Client
- D. VMware Site Recovery with multiple protected sites and a shared recovery site

Suggested Answer: B

Reference:

<https://aws.amazon.com/blogs/apn/design-considerations-for-disaster-recovery-with-vmware-cloud-on-aws/>

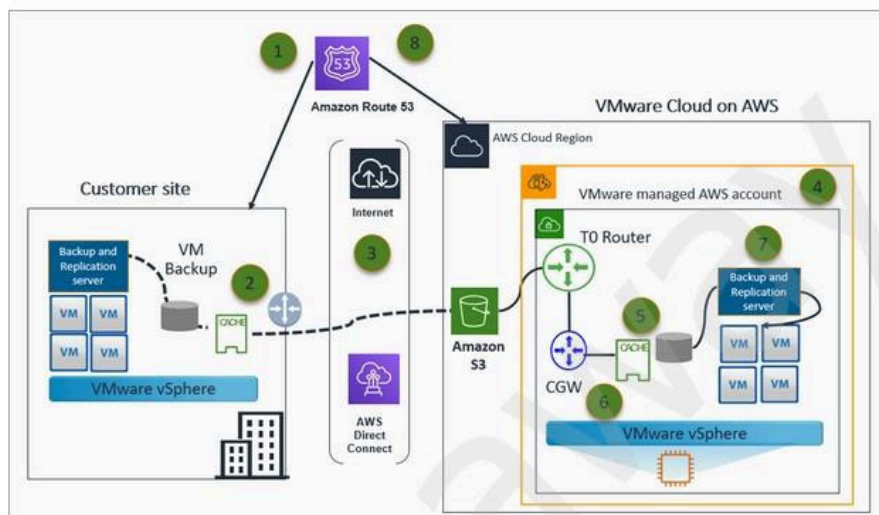


Figure 2 – DR using backup and restore architecture.

Here's what you see happening in the architecture above:

1. Amazon Route 53 handles DNS requests to the primary data center.
2. The Backup & Replication server backs up workloads to the backup repository.
3. Local data from the backup repository offloads to the Capacity Tier in Amazon S3 through AWS Direct Connect or the internet.
4. The recovery process launches and configures the VMware SDDC cluster in the designated AWS recovery region through web portal automation scripts using vRA or vCLI.
5. A new backup repository instance deployed and configured within the newly-created SDDC.
6. Previous data stored in S3 is detected. The initial metadata and archive index sync is executed.
7. Workloads recovered into the SDDC cluster and services are brought back online.
8. Amazon Route 53 record setting updates to resolve requests to the new secondary data center in the cloud.

Community vote distribution

D (60%)

B (40%)

MellasHellas Highly Voted 3 years, 4 months ago

Selected Answer: D

Tricky one.

VMware Site Recovery also supports many-to-many or N:N configurations, and other complex multi-site topologies such as a single site A being protected to a recovery site B, while also serving as a recovery site for a third site C.

You can use VMware Site Recovery in a shared recovery site configuration in any of the deployment models that vCenter Server supports.

https://docs.vmware.com/en/VMware-Site-Recovery/services/com.vmware.srmaas.install_config.doc/GUID-BC46053B-644C-420B-BC68-B71D450711A5.html

upvoted 5 times

🗨️ 👤 **handraco** Most Recent 2 years, 1 month ago

Selected Answer: D

The answer is from here:

https://docs.vmware.com/en/VMware-Site-Recovery/services/com.vmware.srmaas.install_config.doc/GUID-BC46053B-644C-420B-BC68-B71D450711A5.html

upvoted 1 times

🗨️ 👤 **SDDC_Guy** 2 years, 2 months ago

Selected Answer: B

Answer B is in Marketing slides.

upvoted 1 times

🗨️ 👤 **SDDC_Guy** 2 years, 2 months ago

Although, D is the same answer. I have seen B in many presentations on DRaaS

upvoted 1 times

🗨️ 👤 **splint** 2 years, 3 months ago

B doesn't make sense grammatically since if you peer with other cloud SDDCs you are using multiple, not single. Seems like D.

upvoted 3 times

🗨️ 👤 **chistensen** 2 years, 5 months ago

Selected Answer: B

A supported approach when deploying multiple instances of VMware Site Recovery with VMware Cloud on AWS is to have a single software-defined data center (SDDC) connected to multiple on-premises sites and to other cloud SDDCs. This approach allows an administrator to use a single SDDC as the recovery site for multiple on-premises environments and other cloud SDDCs. This provides a centralized, cloud-based disaster recovery solution that can be managed from the VMware Cloud console.

Option A is incorrect because a single SDDC can be paired with multiple remote sites, not just 25.

Option C is incorrect because VMware Site Recovery is not an add-on that is deployed in the vSphere Web Client. It is a standalone product that is integrated with VMware Cloud on AWS.

Option D is incorrect because while VMware Site Recovery can support multiple protected sites and a shared recovery site, this is not the only supported approach.

Therefore, the correct answer is B. A single software-defined data center (SDDC) connected to multiple on-premises sites and to other cloud SDDCs.

upvoted 2 times

🗨️ 👤 **Blair77** 2 years, 6 months ago

Selected Answer: B

Go with B:

https://docs.vmware.com/en/VMware-Site-Recovery/services/com.vmware.srmaas.install_config.doc/GUID-BC46053B-644C-420B-BC68-B71D450711A5.html

To deploy VMware Site Recovery in a multi-site topology, you deploy Site Recovery Manager Server instances on one or more remote sites, and deploy a corresponding number of VMware Site Recovery instances on the shared VMware Cloud on AWS SDDC.

upvoted 1 times

🗨️ 👤 **Blair77** 2 years, 6 months ago

In a multi-site topology, you have multiple remote sites that you configure to recover to or to protect a single, shared VMware Cloud on AWS SDDC.

upvoted 1 times

🗨️ 👤 **BoDaddy** 2 years, 10 months ago

D is correct, you have multi "protected sites" but 1 "recovery site"

upvoted 2 times

🗨️ 👤 **Rabbit117** 3 years ago


B is correct. Extract from VMC on AWS training course.

"You can deploy multiple instances of Site Recovery in a VMware Cloud on AWS SDDC: • Multiple instances support fan-in, fan-out, and other multisite topologies.

• You can connect a single VMware Cloud on AWS SDDC to multiple on-premises sites and to other VMware Cloud on AWS SDDCs for disaster recovery purposes.

• You can pair up to 10 remote sites with a single SDDC."

upvoted 3 times

  **MellasHellas** 3 years, 4 months ago

Discounting A & B because 'a single SDDC connected/paired' (one-to-many) is not the only supported approach, many-to-many is also supported.

Discounting C because the Recovery add-on is deployed in the Cloud Console, not vSphere Client.

upvoted 2 times

What is the minimum value for Maximum Transmission Unit (MTU) of the AWS network hardware used with VMware Cloud on AWS?

- A. 1500 MTU
- B. 9000 MTU
- C. 1492 MTU
- D. 1600 MTU

Suggested Answer: A

Reference:

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.networking-security/GUID-1B51A82F-1AB5-4D35-A170-1044A3A85913.html>

The value you set must be less than or equal to the smallest MTU value for all your DX virtual interfaces. In practice this means that you should set all your VIFs to the same MTU value (the default, at 1500 or Jumbo, at 9001), since having any VIF that does not support a Jumbo MTU effectively limits all DX connections to an MTU of 1500. Mixing MTU sizes within a network can lead to packet fragmentation and other problems that result in poor network performance.

praw709528

Community vote distribution

D (79%)

A (21%)

🗳️ **manvvee** 1 year, 7 months ago

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-networking-security/GUID-1B51A82F-1AB5-4D35-A170-1044A3A85913.html>

A- 1500 MTU

upvoted 2 times

🗳️ **Mwafrika** 2 years ago

Selected Answer: A

A is the Answer, key word is Minimum supported, and 1500 is by default the supported MTU. Ref: <https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/vmc-on-aws-networking-security.pdf>

upvoted 2 times

🗳️ **handraco** 2 years, 1 month ago

Selected Answer: A

1500 for all.

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-networking-security/GUID-1B51A82F-1AB5-4D35-A170-1044A3A85913.html#:~:text=The%20default%20Maximum%20Transmissible%20Unit,SDDC%20networks%20is%201500%20bytes.>

upvoted 1 times

🗳️ **SDDC_Guy** 2 years, 2 months ago

Selected Answer: D

NSX requires 1600

upvoted 1 times

🗳️ **Blair77** 2 years, 6 months ago

Selected Answer: D

DDD:

Provide an MTU size of 1600 or greater on any network that carries Geneve overlay traffic must. Geneve packets cannot be fragmented. The MTU size must be large enough to support extra encapsulation overhead.

upvoted 2 times

🗳️ **viqvar** 2 years, 7 months ago

AWS network hardware is configured with a maximum transmission unit(MTU) of 1600+ and VLAN Trunks.

upvoted 2 times

🗲️ 👤 **mefor** 2 years, 8 months ago

Selected Answer: D

1600 is the MTU

upvoted 3 times

🗲️ 👤 **pablits** 2 years, 8 months ago

A or D???

upvoted 1 times

🗲️ 👤 **Dmytros** 2 years, 8 months ago

A- 1500

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-networking-security/GUID-1B51A82F-1AB5-4D35-A170-1044A3A85913.html>

upvoted 2 times

🗲️ 👤 **c11** 2 years, 9 months ago

Selected Answer: D

D: from the VMC training: "AWS network hardware is configured with a minimum maximum transmission unit (MTU) of 1600+ and VLAN trunks."

upvoted 3 times

🗲️ 👤 **BoDaddy** 2 years, 10 months ago

A - 1500 is correct they are looking for the MIN (MTU) not the MAX

upvoted 2 times

🗲️ 👤 **Bobob55** 2 years, 10 months ago

A 1500

upvoted 2 times

🗲️ 👤 **Rabbit117** 3 years ago

D is correct.

Extract from VMware VMC on AWS training course,

"A maximum transmission unit (MTU) of 1,600 or more is required so that NSX-T Data Center can support the GENEVE overlay for frame encapsulation."

upvoted 3 times

🗲️ 👤 **Ishmwklpytunrsvq** 3 years, 1 month ago

Selected Answer: D

What do we have within the SDDC?

Yeah NSX-T with a T0 Router and between each physical ESXi you also want to ensure that GENEVE Traffic for the Segments is working, therefore 1600 is the minimum MTU on the HW or else no Networking between the Hosts.

upvoted 2 times

🗲️ 👤 **sarkarbaba** 3 years, 2 months ago

A is correct : <https://configmax.esp.vmware.com/guest?vmwareproduct=VMware%20Cloud%20on%20AWS&release=SDDC%201.17&categories=53-0>

upvoted 4 times

🗲️ 👤 **Cccb35** 2 years, 11 months ago

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/solutions/VMware-Cloud-on-AWS.91696a39d9cb804e2888c43d538bab50/GUID-5ED7528BA47FA13CC449B2D5EB64F4FA.html>

upvoted 2 times

A customer is currently running 153 virtual machines in an eight-node vSphere cluster. Each host is equipped with 256GB RAM, two AMD CPUs and four 10Gb NICs. Which migration strategy should the administrator recommend?

- A. HCX Replication Assisted vMotion (RAV) with Enhanced vMotion Compatibility
- B. HCX Cold Migration
- C. Cross vCenter vMotion with Hybrid Linked Mode
- D. HCX vMotion with Enhanced vMotion Compatibility


Suggested Answer: C

Reference:

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/vmc-aws-manage-data-center-vms.pdf>

Community vote distribution

B (100%)


 **PaulAuchon** Highly Voted 3 years, 1 month ago

Because CPUs at source are AMD i think B is the correct answer. Unable to do a live migration between AMD and Intel.
upvoted 8 times

 **SDDC_Guy** Most Recent 2 years, 2 months ago


Selected Answer: B

AMD to Intel = Cold Migration.
upvoted 2 times

 **uchiken** 2 years, 5 months ago

Selected Answer: B

B is correct answer.
upvoted 2 times

 **BoDaddy** 2 years, 10 months ago

Answer is B - you need to cold migrate AMD to Intel
upvoted 4 times

 **DSITTA** 2 years, 10 months ago

on AWS SDDC hosts are of two type i3.metal and i3en.metal both based on Intel CPU, not AMD. So the only supported way is B. HCX Cold Migration.
upvoted 3 times

 **Rabbit117** 3 years ago

I agree with PaulAuchon that B is correct. The AMD CPU is the only piece of info to differentiate between the possible answers.
upvoted 3 times


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.

Suggested Answer: ADE

Community vote distribution

ABC (100%)

  **itexamp092** Highly Voted 3 years, 4 months ago

abc are correct
upvoted 10 times

  **Rabbit117** Highly Voted 3 years ago

A,B and C. See below extract from VMC on AWS training course.

VM Configurations with Limited Support in VMware Cloud on AWS:

These VM configurations have limited support and, as a result, are incompatible with VM migrations that use vSphere vMotion in VMware Cloud on AWS:

- Remote devices attached (CDs, floppy disks, and so on)
- Serial ports with network output • Mounted paravirtual SCSI (PVSCSI) disks

upvoted 9 times

  **splint** Most Recent 2 years, 2 months ago

Selected Answer: ABC


Verified in my training manual as well.

upvoted 1 times

  **HeyItsMe2** 2 years, 3 months ago

paravirtual scsi disks are allowed - do they mean "mounted" to the vm? Thats supported. It's a choice other than LSI Logic for example. I think its B,C,E If you svmotion a linked-clone, the link will be broken to the parent. It's B-C-E

upvoted 2 times

  **Blair77** 2 years, 6 months ago

Selected Answer: ABC

Agreed with ABC



upvoted 2 times

  **Dmytros** 2 years, 8 months ago

Selected Answer: ABC

From VMware Cloud on AWS VM Configurations

upvoted 2 times

  **BoDaddy** 2 years, 10 months ago

I am unsure about the answer, but going with A - B - C

upvoted 2 times

An administrator is planning to migrate a VMware vSphere environment to VMware Cloud on AWS. A first analysis returns the following specifications:

- ⇒ 37 virtual machines will be live migrated
- ⇒ All virtual machines have been created using VMware vSphere 5.0 (Compatibility Version 8)
- ⇒ All virtual machines are connected to Standard Switches
- ⇒ The bandwidth between the local data center and VMware Cloud on AWS is 250 Mbps

What are two valid approaches for live migrating these virtual machines? (Choose two.)

A.

- ⇒ Upgrade Virtual Machine Compatibility to Version 9.
- ⇒ Ensure Standard Switch is named the same as the target segment in VMware Cloud on AWS.
- ⇒ Activate and deploy VMware HCX.
- ⇒ Let HCX configure Enhanced vMotion Compatibility (EVC) automatically.

B.

- ⇒ Upgrade Virtual Machine Compatibility to Version 9.
- ⇒ Configure Hybrid Linked Mode for Cross vCenter vMotion.

Configure AWS Direct Connect Private VIF.

▪

- ⇒ Configure Enhanced vMotion Compatibility (EVC) on the source virtual machines as required.

C.

- ⇒ Upgrade Virtual Machine Compatibility to Version 9.
- ⇒ Migrate the Virtual Machines to a Distributed Virtual Switch.
- ⇒ Activate and deploy VMware HCX.
- ⇒ Let HCX configure Enhanced vMotion Compatibility (EVC) automatically.

D.

- ⇒ Upgrade the bandwidth between the local data center and VMware Cloud on AWS to 400 Mbps.
- ⇒ Migrate the virtual machines to a Distributed Virtual Switch.
- ⇒ Activate and deploy VMware HCX.
- ⇒ Let HCX configure Enhanced vMotion Compatibility (EVC) automatically.

E.

- ⇒ Upgrade the bandwidth between the local data center and VMware Cloud on AWS to 400 Mbps.
- ⇒ Configure Hybrid Linked Mode for Cross vCenter vMotion.
- ⇒ Configure AWS Direct Connect Private VIF.
- ⇒ Configure Enhanced vMotion Compatibility (EVC) on the target software-defined data center (SDDC) as required.

Suggested Answer: BE

  **gv84** 1 year, 5 months ago

HCX Network Extension does not support the following source configurations:

vSphere Standard Switch (vSS) networks.

<https://docs.vmware.com/en/VMware-HCX/4.8/hcx-user-guide/GUID-DBDB4D1B-60B6-4D16-936B-4AC632606909.html#GUID-DBDB4D1B-60B6-4D16-936B-4AC632606909>

upvoted 1 times

  **HeyItsMe2** 2 years, 3 months ago

A - NO - Standard switches won't extend L2, so no Live migration - Naming doesn't matter - HCX does not change EVC and neither does vMotion.

B - Weird - Cross vCenter vMotion won't be "live" as there wouldn't be an L2 stretch, unless you're happy to migrate and have no destination network that would function for the VM. (maybe this one technically?)

C - Weird - HCX doesn't configure EVC - You can configure evc on a per VM basis on-prem though. If the VM was on a distributed switch you could use L2 stretch, but thats not mentioned.

D - Werid - Bandwidth minimum for HCX to work is 100 mbps. HCX does not change EVC - Sure, you can take a VM running on old and move it to new, but thats only because it's using CPU instructions the new hosts fully understands.

E - NO - You can't change EVC settings on an SDDC cluster. Bandwidth is fine.

If i was forced to pick the least worse two answers, it would be B and C

upvoted 2 times

🗨️ 👤 **splint** 2 years, 3 months ago

A - No standard switch support for live migration

B - CORRECT, has enough BW, 250Mbps

C - CORRECT, HCX only needs 100Mbps

D - Doesn't address HW version

E - Do not need to upgrade BW

upvoted 4 times

🗨️ 👤 **johnadama** 2 years, 5 months ago

"37 virtual machines will be LIVE migrated"

Live migration requires distributed switch...

upvoted 3 times

🗨️ 👤 **balabharath** 2 years, 5 months ago

cross vcenter vmotion is not supported in 5.0. So B is invalid.

A & C is right because it upgrades VM hardware.

In D&E upgrading VM hardware is not listed. Also 400Mbps is not required. 250Mbps is the min.requirement.

upvoted 1 times

🗨️ 👤 **SDDC_Guy** 2 years, 2 months ago

Only says it was created in 5.0, for purpose of saying HW8.

B/C

upvoted 1 times

🗨️ 👤 **rembix** 2 years, 6 months ago

A & B

VSS is supported on HCX

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-operations/GUID-DAE9B318-294A-4422-BBF4-82AE9DDFF043.html>

upvoted 1 times

🗨️ 👤 **Blair77** 2 years, 6 months ago

B - C :

HCX Network Extension does not support the following source configurations: vSphere Standard Switch (VSS) networks.

upvoted 2 times

🗨️ 👤 **Cobra005** 2 years, 7 months ago

B&C as BW is sufficient and because HCX Network Extension does not support the following source configurations: vSphere Standard Switch (VSS) networks.

<https://docs.vmware.com/en/VMware-HCX/4.5/hcx-user-guide-45.pdf>

upvoted 2 times

🗨️ 👤 **Dmytros** 2 years, 8 months ago

BC& is correct

In LIVE Migration Need DVS:

On-premises DVS version 6.0 or higher.

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-operations/GUID-1A175E91-2317-4261-A63E-B398D92ECE8D.html>

upvoted 3 times

🗨️ 👤 **Calidude** 2 years, 8 months ago

BD

NOT A: Standard sw naming doesn't matter

NOT C: don't have enough BW per migration

E: don't have to configure EVC on target SDDC

Deploy, Configure, Manage 2021

8-31 Live Migration Using Hybrid Linked Mode



VM is powered on.

Source to destination settings are as follows: – Bandwidth of 250 Mbps (per migration)

Networking settings are configured: – IPsec VPN to management gateway – L2 VPN or AWS Direct Connect – vSphere Distributed Switch 6.x or later VM Compatibility version 9 is used.

Enhanced vMotion Compatibility is considered.

Each live migration requires 250 Mbps of bandwidth per vSphere vMotion migration
upvoted 2 times

  **BoDaddy** 2 years, 10 months ago

I don't think you need to upgrade the bandwidth to 400mb and Standard Switches are supported in HCX , So I am going with A & B
upvoted 1 times

  **Rabbit117** 3 years ago

Standard switch is supported. See <https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-operations/GUID-DAE9B318-294A-4422-BBF4-82AE9DDFF043.html>
upvoted 1 times


  **Rabbit117** 3 years ago

I think A and B are correct.

You would need to upgrade VM compatibility to v9 and the bandwidth is already 250Mbps so that is D and E out.

No need to migrate the VMs to DVS as Standard switches are supported, so that rules out C.

upvoted 2 times



  **MellasHellas** 3 years, 4 months ago

250MB bandwidth per concurrent vMotion, so not D or E.

<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vcenterhost.doc/GUID-3B41119A-1276-404B-8BFB-A32409052449.html>

HCX supports standard switch, but cannot see requirement to name the segment the same anywhere. Makes more sense than migrating to VDS if you dont have to, so going with A, B.

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-operations/GUID-DAE9B318-294A-4422-BBF4-82AE9DDFF043.html>
upvoted 4 times

  **Cccb35** 3 years, 4 months ago

I think, the corrects are B and C.

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-operations/GUID-6EC9D234-6B9D-4C66-9385-D6AB3BFFFBC9.html>
upvoted 3 times

An administrator recently completed the first migration of on-premises production workloads into VMware Cloud on AWS. The administrator intends to scale the hybrid cloud environment in a phased approach over the next 12 months, but the Service Owner has some concerns about being able to complete workload optimization and balancing, capacity and cost management, and compliance reporting. Which VMware solution should the administrator recommend to address the concerns of the Service Owner?

- A. VMware vRealize Automation Cloud
- B. VMware vRealize Network Insight Cloud
- C. VMware vRealize Log Insight Cloud
- D. VMware vRealize Operations Cloud

Suggested Answer: A

Community vote distribution

D (100%)

🗳️ 👤 **SDDC_Guy** 2 years, 2 months ago

Selected Answer: D

vROps is the answer

upvoted 1 times

🗳️ 👤 **uchiken** 2 years, 5 months ago

I think D is correct

upvoted 2 times

🗳️ 👤 **BoDaddy** 2 years, 10 months ago

The answer is D - vROps

upvoted 4 times

🗳️ 👤 **Rabbit117** 3 years ago

Selected Answer: D

D is correct.

upvoted 3 times

🗳️ 👤 **MellasHellas** 3 years, 4 months ago

Selected Answer: D

These are vROps functions, vRLI is for log aggregation and analysis

<https://docs.vmware.com/en/vRealize-Operations/8.6/com.vmware.vcom.config.doc/GUID-9B27A50B-97AD-4B89-89D3-7BB515BD7394.html>

upvoted 3 times

The Tier-0 (T0) router will send northbound packets through which device?

- A. The AWS Elastic Network Adapter (ENA) of the VMware ESXi host that the active T0 Edge virtual machine is currently running on.
- B. The AWS Elastic Network Adapter (ENA) of the VMware ESXi host where the packet is originating from.
- C. The AWS Elastic Network Adapter (ENA) of the VMware ESXi host that the passive T0 Edge virtual machine is currently running on.
- D. The AWS Elastic Network Adapter (ENA) of the VMware ESXi host that is currently the least utilized.

Suggested Answer: C

Community vote distribution

A (100%)

🗲️ 👤 **gogo1** Highly Voted 3 years, 5 months ago

Correct answer is A
upvoted 9 times

🗲️ 👤 **SDDC_Guy** Most Recent 2 years, 2 months ago

Selected Answer: A

When the T0 Edge was Active/Passive, A would be the right answer. Now that it is active/active, that changes, but it is a new feature and not the way the test would see it.
upvoted 1 times

🗲️ 👤 **uchiken** 2 years, 5 months ago

I think A
upvoted 2 times

🗲️ 👤 **Blair77** 2 years, 6 months ago

Selected Answer: A

A is the good one
upvoted 2 times

🗲️ 👤 **BoDaddy** 2 years, 10 months ago

A is correct
upvoted 3 times

🗲️ 👤 **Rabbit117** 3 years ago

Selected Answer: A

A is correct.
upvoted 3 times

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.

Suggested Answer: D

Community vote distribution

C (100%)

🗳️ 👤 **MJ_PL** Highly Voted 👍 3 years, 4 months ago

C is right answer. this customer account does not need to be dedicated or special any way.
upvoted 6 times

🗳️ 👤 **SDDC_Guy** Most Recent 🕒 2 years, 2 months ago

Selected Answer: C

Existing Account... C
upvoted 1 times

🗳️ 👤 **Blair77** 2 years, 6 months ago

Selected Answer: C

C is good
upvoted 2 times

🗳️ 👤 **BoDaddy** 2 years, 10 months ago

C is correct
upvoted 3 times

🗳️ 👤 **Rabbit117** 3 years ago

Selected Answer: C

C is correct.
upvoted 4 times

An administrator is deploying a VMware Cloud on AWS software-defined data center (SDDC) in an AWS region and needs to plan for mission-critical application availability across availability zones. Which AWS Virtual Private Cloud (VPC) configuration needs to be in place in order to accomplish this?

- A. One AWS VPC with four subnets, one per availability zone
- B. Two AWS VPCs with two subnets, two per availability zone
- C. One AWS VPC with two subnets, one per availability zone
- D. Four AWS VPCs with two subnets, two per availability zone

Suggested Answer: B

Community vote distribution

C (100%)

  **MJ_PL**  3 years, 4 months ago

Mission critical means stretched cluster (among 2 AZs) and the requirement for stretched cluster is as follows:

You can create an SDDC with a cluster that spans two availability zones. A stretched cluster uses vSAN technology to provide a single datastore for the SDDC and replicate the data across both availability zones. If service in one availability zone is disrupted, workload VMs in the SDDC are brought up in the other availability zone.

The following restrictions apply to stretched clusters:

*The linked VPC must have two subnets, one in each AZ occupied by the cluster.

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-operations/GUID-BC0EC6C5-9283-4679-91F8-87AADF89E116.html>

Then C is the answer

upvoted 8 times

  **MJ_PL**  3 years, 4 months ago

Selected Answer: C

The linked VPC must have two subnets, one in each AZ occupied by the cluster.



upvoted 5 times

  **Blair77**  2 years, 6 months ago

Selected Answer: C

C two subnets, one in each AZ occupied by the cluster

upvoted 2 times

  **BoDaddy** 2 years, 10 months ago

Agree with C

upvoted 2 times

  **Rabbit117** 3 years ago

Selected Answer: C

I agree with MJ_PL, correct answer is C.

upvoted 2 times

Which two VMware Cloud on AWS maintenance tasks are the responsibility of AWS personnel? (Choose two.)

- A. Back up and restore VMware appliances and infrastructure.
- B. Patch VMware Cloud on AWS components.
- C. Refresh hardware and replace failed components.
- D. Upgrade workload VMware Tools.

Suggested Answer: BC

Reference:

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/vmw-cloud-aws-service-description.pdf>

Community vote distribution

C (100%)

🗳️ 👤 **nemis95** Highly Voted 3 years, 4 months ago

- A - VMware
- B - VMware
- C - AWS
- D - Customer

Poor question imo. It's definitely C and probably B is the better choice than A. The question should really state "responsibility of VMware personnel?" (as per the VMware sample exam in Question 10)

<https://vmc.techzone.vmware.com/vmcrf/vmcaws-shared-responsibility-model#shared-responsibility-matrix>

upvoted 8 times

🗳️ 👤 **me4or** Highly Voted 2 years, 8 months ago

Selected Answer: C

C & E - Update BIOS firmware was on the exam too

upvoted 7 times

🗳️ 👤 **handraco** Most Recent 2 years, 1 month ago

Selected Answer: C

C: The hardware is belonged to AWS

upvoted 1 times

🗳️ 👤 **SDDC_Guy** 2 years, 2 months ago

Selected Answer: C

Exam has BIOS/Firmware as an answer as well... C is correct

upvoted 1 times

🗳️ 👤 **garfieldca** 2 years, 10 months ago

one option is missing from the actual exam

E Patches BIOS and firmware which is correct

so final answer should be C and E

upvoted 6 times

🗳️ 👤 **NikTheFlash** 2 years, 8 months ago

it make sense - in all VMware exams, when you have '(choose two)' you always have 5 options.

upvoted 2 times

🗳️ 👤 **BoDaddy** 2 years, 10 months ago

Agreed , poor wording of the question and I would select B & C

upvoted 3 times

A user with an Organization Member role would like to add another user to an organization. How would this be accomplished?

- A. Only users with an Organization Owner role can invite and add users to the organization.
- B. The user with an Organization Member role needs to have CloudAdmin permissions in order to add a new user.
- C. The user with an Organization Member role will be able to add a new user through the Identity and Access Management page.
- D. Users with an Organization Member role are automatically granted access to all roles within VMware Cloud on AWS.

Suggested Answer: A

A -

Reference:

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.getting-started/GUID-9CAB2B3E-42D5-44A1-9428-E8FFD22BDD01.html> -

VMware Cloud accounts are based on an Organization, which corresponds to a group or line of business subscribed to VMware Cloud services.

Each Organization has one or more Organization Owners, who have access to all the resources and services of the Organization and can invite additional users to the account. By default, these additional users are Organization Users, who can create, manage, and access resources belonging to the Organization, but cannot invite new users.

Community vote distribution


A (100%)

 **SDDC_Guy** 2 years, 2 months ago

Selected Answer: A

Go AAAA

upvoted 1 times

 **Blair77** 2 years, 6 months ago

Selected Answer: A

100% A

upvoted 2 times

 **briansbums** 2 years, 10 months ago

VMware has management and operational responsibilities for the infrastructure, cloud SDDC software components, and the VMware Cloud on AWS console:

- vCenter, NSX, vSAN
- ESXi hosts
- AWS infrastructure: Servers and provider networking
- Management activities: Host and SDDC management, components updates, configuration, monitoring, and logging

Partners and customers are responsible for managing and operating their workloads:

- VM, VM Tools, guest OS, applications
- Management activities: Deployment, updates, and configuration
- Monitoring activities: Logging, backup and DR, migration, and hybrid management

Both VMware and the customer are responsible for management and compute network gateways.

For more information about management and operational responsibilities, see Managing the VMware Cloud on AWS Data Center at <https://docs.vmware.com/en/VMware-Cloud-on-AWS/index.html>.

upvoted 1 times

 **BoDaddy** 2 years, 10 months ago

A is correct

upvoted 2 times

 **Mellashellas** 3 years, 4 months ago

Selected Answer: A

<https://docs.vmware.com/en/VMware-Cloud-services/services/Using-VMware-Cloud-Services/GUID-C11D3AAC-267C-4F16-A0E3-3EDF286EBE53.html>

upvoted 2 times