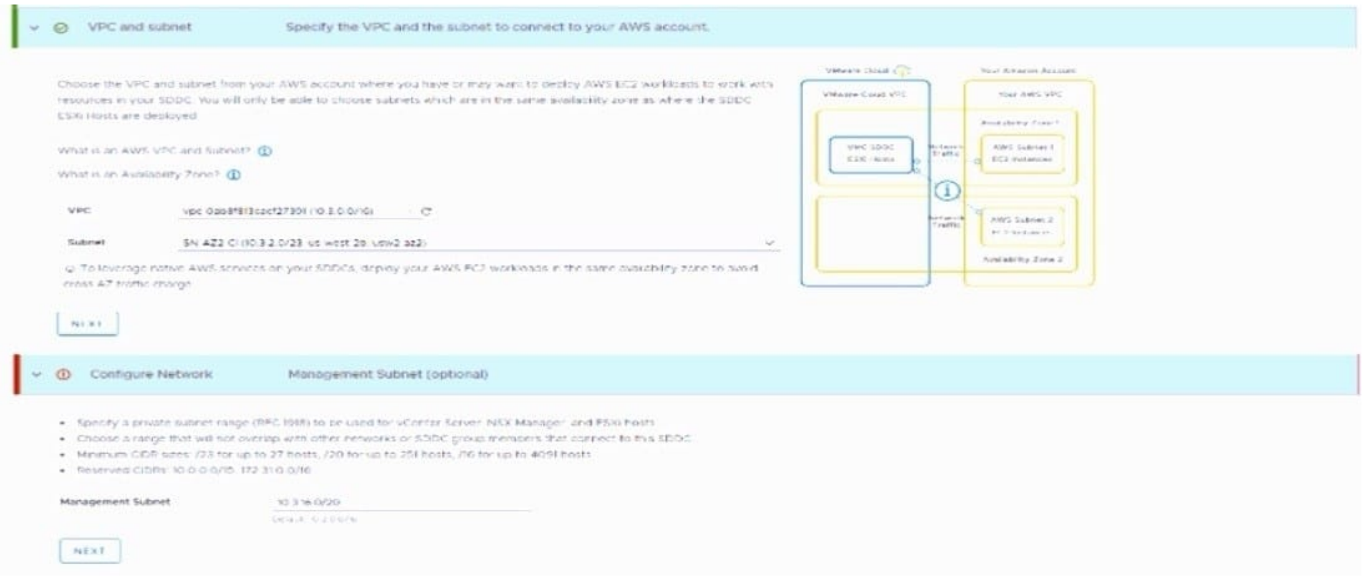
2V0-33.22$^{Q\&As}$

VMware Cloud Professional

Pass VMware 2V0-33.22 Exam with 100% Guarantee

QUESTION 1

Refer to the exhibit.



VPC and subnet — Specify the VPC and the subnet to connect to your AWS account.

Choose the VPC and subnet from your AWS account where you have or may want to deploy AWS EC2 workloads to work with resources in your SDDC. You will only be able to choose subnets which are in the same availability zone as where the SDDC ESXi Hosts are deployed

What is an AWS VPC and Subnet? ⓘ

What is an Availability Zone? ⓘ

VPC: vpc-0ab8f813cacf27301 (10.3.0.0/16)

Subnet: SN AZ2 C (10.3.2.0/23 us-west-2b usw2-az2)

To leverage native AWS services on your SDDCs, deploy your AWS EC2 workloads in the same availability zone to avoid cross AZ traffic charge

NEXT

Configure Network — Management Subnet (optional)

- Specify a private subnet range (RFC 1918) to be used for vCenter Server, NSX Manager and ESXi hosts
- Choose a range that will not overlap with other networks or SDDC group members that connect to this SDDC
- Minimum CIDR sizes: /23 for up to 27 hosts, /20 for up to 251 hosts, /16 for up to 4091 hosts
- Reserved CIDRs: 10.0.0.0/15, 172.31.0.0/16

Management Subnet: 10.3.16.0/20
Default: 10.2.0.0/16

NEXT

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

A. It overlaps with the AWS subnet.

B. It overlaps with the AWS VPC CIDR.

C. It is part of the reserved CIDRs.

D. It is an invalid size.

Correct Answer: A

https://docs.aws.amazon.com/whitepapers/latest/sddc-deployment-and-best- practices/deploying-vmware-cloud-on-aws-sddc.htmlThis must be a RFC1918 private address space (10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16) with CIDR block sizes of /16, /20, or /23. The management CIDR block cannot be changed after the SDDC is deployed. Choose a range of IP addresses that does not overlap with the AWS subnet you are connecting to. If you plan to connect the SDDC to an on-premises DC or another environment, the IP subnet must be unique within your enterprise network infrastructure. Choose a CIDR that will give you future scalability.

QUESTION 2

A cloud administrator wants to enable administrator wants to enable Enterprise Federation to the Cloud Services Portal in order to be able to authenticate with the on-premises Active Directory. The Administrator Already deployed the on-premises VMware Workspace One Access Connector. Through which port does the Cloud Service Portal communicate with Workspace ONE Access Connector?

A. ldaps/636

B. http/80

C. https/443

D. ldap/389

Correct Answer: C

https://docs.vmware.com/en/VMware-Workspace-ONE-Access/20.10/workspace_one_access_install/GUID-E81B6B1B-A3D1-40D0-806A-3D31502C53A5.html

The Cloud Services Portal communicates with the Workspace ONE Access Connector via port 443 (HTTPS). According to the VMware documentation [1], the Cloud Services Portal connects to the Access Connector on port 443 to authenticate users and authorize access to the cloud service. The Access Connector listens on port 443 and communicates with the Active Directory using LDAP over TLS (LDAPS) on port 636. Reference:

https://docs.vmware.com/en/VMware-Workspace-ONE-Access/services/com.vmware.access.admin.configure.doc/GUID-F5C6FD9E-36DA-4B1F-A7E7-CF8F64A81D78.html

QUESTION 3

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

A. Native cloud provider

B. Customer

C. VMware Cloud Provider Partner (VCPP)

D. VMware

Correct Answer: B

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

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

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

QUESTION 4

Which two steps does a cloud administrator need to take when protecting a VMware Cloud on AWS software-defined data center (SDDC) with VMware site Recovery? (Choose Two.)

A. Deploy the vSphere Replication virtual appliance.

B. Deploy the Site Recovery manager virtual Appliance.

C. Connect the Site Recovery manager instance on the protected recovery site.

D. Register the vSphere Replication appliance with vCenter Single Sign-On

E. Set the NSX-T Edge management gateway firewall rules.

Correct Answer: AC

A cloud administrator needs to deploy the vSphere Replication virtual appliance and the Site Recovery manager virtual appliance when protecting a VMware Cloud on AWS software-defined data center (SDDC) with VMware Site Recovery. The vSphere Replication virtual appliance is responsible for replicating the virtual machines from the source to the target site. Site Recovery Manager virtual appliance acts as the central management and orchestration platform for the entire disaster recovery process.

Reference:https://docs.vmware.com/en/VMware-Site-Recovery/index.html

In order to protect a VMware Cloud on AWS software-defined data center (SDDC) with VMware Site Recovery[1][2], a cloud administrator needs to take the following two steps:

A) Deploy the vSphere Replication virtual appliance - This can be done by logging into the vSphere Client, navigating to the vCenter Server, and then selecting the Deploy OVF Template option. From here, the cloud administrator can upload the OVF template for the vSphere Replication appliance and configure it.

B) Connect the Site Recovery manager instance on the protected recovery site - This involves logging into the Site Recovery Manager (SRM) and setting up the connection between the protected recovery site and the SRM instance. This can be done by going to the SRM dashboard and then selecting the Connect Remote Site option.

References: [1]https://docs.vmware.com/en/VMware-Site-Recovery/services/vmc-dr-deployment/GUID-DBF6CD69-6F7E-47E2-9417-91D5C5F5AC5E.html [2]https://docs.vmware.com/en/VMware-Site-Recovery/services/vmc-dr-deployment/GUID-1C8B7BCA-D4BE-4EAF-9A8A-4B42E2B7236A.html

QUESTION 5

Which hyperscaler partner is best suited for customers who need 100 GB bandwidth between SDDCs in the cloud? (Select one option)

A. VMware Cloud on AWS

B. Azure VMware Solution

C. Oracle Cloud VMware Solution

D. Google Cloud VMware Engine

Correct Answer: A

VMware Cloud on AWS provides the highest level of performance, reliability, and scalability for customers who need to move large amounts of data between their SDDCs in the cloud. It is also the only hyperscaler partner that has the ability to quickly and easily provision entire SDDCs in the cloud. In addition, VMware Cloud on AWS offers the most comprehensive enterprise-grade features, such as automated backups and disaster recovery, which provide customers with peace of mind that their data is always secure and protected.