Question 1

A company wants to start using Nutanix Cloud Clusters (NC2) in AWS. The company has large spend commitments as part of an AWS Enterprise Discount Program (EDP) totaling $15 million.

What approach should the administrator take to ensure that Nutanix licensing costs to the EDP commitment?

Options:

A- Purchase Nutaniz licenses through the AWS Marketplace.

B- Purchase Nutanix licenses directly from Nutanix and contact AWS support.

C- Leverage existing Nutanix licenses.

D- Request a trial license directly from Nutanix

Answer:

A

Explanation:

Given the company's large spend commitments as part of an AWS Enterprise Discount Program (EDP) totaling $15 million, purchasing Nutanix licenses through the AWS Marketplace ensures that the costs contribute to the EDP commitment.

This approach integrates the Nutanix license costs into the overall AWS spend, thereby maximizing the benefits of the EDP.

Purchasing directly from Nutanix or leveraging existing licenses might not count towards the AWS EDP commitment, and trial licenses are typically for evaluation purposes and do not contribute to the committed spend.

Reference: Refer to the Nutanix and AWS documentation on licensing and marketplace purchases, and EDP program details.

Question 2

Question Type: MultipleChoice

An administrator is deploying an NC2 cluster on AWS in the us-west-2 region. A VPC, management subnet, and a VM subnet are already created in the target region.

The management subnet has a local route and a route to the internet. The subnet has a route and a route to the NAT gateway. During the deployment, the management subnet appears in the drop-down list in the Create Cluster wizard, but cannot be selected.

What is the cause of this problem?

Options:

A- The subnet has both an IPv4 CIDR block and an IPv6 CIDR block.

B- The subnet has an IPv4 CIDR block but does not have an IPv6 CIDR block.

C- The subnet has a direct route to an Internet gateway.

D- The subnet does not have route to a Site-to-Site VPN connection through a virtual private gateway.

Answer:

A

Explanation:

The Nutanix Create Cluster wizard may not support selecting subnets that have both IPv4 and IPv6 CIDR blocks due to compatibility or configuration constraints.

When a subnet with both CIDR blocks is present, it can cause issues in the selection process during cluster creation, as the system might not be able to properly handle or recognize the dual-stack configuration.

Ensuring that the management subnet has only an IPv4 CIDR block, without an IPv6 CIDR block, could resolve this issue and allow for successful selection in the cluster creation wizard.

Reference: Refer to the Nutanix and AWS documentation on subnet configuration and requirements for NC2 cluster deployments, specifically addressing IPv4 and IPv6 compatibility and constraints.

Question 3

An administrator is tasked with deploying a VM in an NC2 cluster on AWS that needs to by accessed by resources within the on-premises datacenter.

The cluster has the following characteristics:

* 8 nodes

* Resides in the us-east-1a Availability Zone

* Contains 13 Subnets

* Has access to a Direct Connect connection

* Subnet that the User VM (UVM) is being deployed to:UserVM_subnet

There are multiple VMs within the cluster and the UserVM_subnet has access to the on-premises resources.

The administrator deploys the machine, but communication is not possible.

What is the most likely resolution for this situation?

Options:

A- The AWS User Management Security Group requires the new application's ports adding to and traffic

B- The AWS Internal Management Security Group requires the new application's ports adding to outbound traffic.

C- The AWS UVM Security Group requires the new application's ports adding to inbound traffic.

D- The AWS IGW requires the new application's ports adding to inbound traffic.

Answer:

C

Explanation:

For a VM deployed in an NC2 cluster on AWS to be accessed by resources within the on-premises datacenter, the security group associated with the User VM (UVM) subnet must allow inbound traffic on the specific ports required by the application.

If the security group rules do not permit inbound traffic on these ports, the communication will fail, even if other network configurations are correct.

The administrator should ensure that the UVM Security Group includes rules to allow inbound traffic for the application's required ports, facilitating proper communication between the VM and on-premises resources.

Reference: Refer to the AWS documentation on security group configurations and Nutanix NC2 documentation for details on configuring network access and security group rules.

Question 4

The cluster is configured as follows:

* 8 nodes

* Prism Central Deployed

* Files Deployed

Following the deployment, the administrator experiences network connectivity issues.

Which reason explains the connectivity issues?

Options:

A- The 192.168.5.0/24 range is not a valid CIDR range.

B- The 192.168.5.0/24 range is reserved for internal cluster usage.

C- The 192.168.5.0/24 range does not have enough IP addresses available.

D- The 192.168.5.0/24 range is reserved by IANA,

Answer:

B

Explanation:

The 192.168.5.0/24 range is often reserved for internal cluster communication within Nutanix deployments.

Using this CIDR range for other purposes could lead to network conflicts and connectivity issues, as it might interfere with the internal operations and communication channels of the Nutanix cluster.

Ensuring that the CIDR range is not overlapping with any reserved ranges is crucial for maintaining proper network connectivity and cluster functionality.

Reference: Refer to the Nutanix documentation on network configuration and best practices for NC2 deployments to confirm reserved IP ranges and their appropriate use.

Question 5

Question Type: **MultipleChoice**

Which statement is true regarding AWS account requirements?

Options:

A- IAMFullAccess permission gets configuration details for supported AWS resources.

B- AWSCloudFormationFullAccess role is required to create a CloudFormation stack.

C- An AWS root user can be used for any deployment or operations related to NC2.

D- NC2 on AWS uses AWS Secrets Manager for maintaining any stored secrets.

Answer:

B

Explanation:

To create a CloudFormation stack, the AWSCloudFormationFullAccess role is required.

This role grants the necessary permissions to create, update, and delete CloudFormation stacks, which are essential for deploying and managing AWS infrastructure using CloudFormation templates.

CloudFormation stacks are often used to automate the deployment of complex infrastructures, including those required for NC2 on AWS.

Proper permissions ensure that the deployment process is seamless and adheres to the security and operational policies of the organization.

Reference: Refer to the AWS IAM documentation for details on the AWSCloudFormationFullAccess role and Nutanix documentation on prerequisites for deploying NC2 on AWS.

Question 6

An administrator is creating and destroying multiple clusters daily for a test/dev environment. The administrator wants ensure that every NC2 on AWS cluster deployed will allow full access from the on-premises CVM subnet.

What is most-efficient way to achive this?

Options:

A- Modify the UVM Network Security Group of each cluster by setting the inbound allow address of the on-premises subnet.

B- Modify the UVM Network Security Group of each cluster by setting the outbound allow address of the on-premises subnet.

C- Create a Custom AWS Network Security Group using a key value of tag:nutanix:clusters:external and set the inbound allow address of the on-premises subnet.

D/ Create a Custom AWS Network Security Group using a key of tag:nutanix: clusters:external:cluster-uuid and set the value of the UUID for each deployed cluster. Set the inbound allow address of the on-premises subnet.

Answer:

C

Explanation:

To ensure that every NC2 on AWS cluster deployed allows full access from the on-premises CVM subnet efficiently, the administrator should create a custom AWS Network Security Group.

Use a key value of tag:nutanix:clusters:external for the security group, and set the inbound allow address to the on-premises subnet.

This approach leverages AWS tags to manage security group rules dynamically and ensures that the necessary access permissions are applied automatically to all clusters with the specified tag.

This method reduces the need for manual configuration of each cluster's security group, streamlining the process for a test/dev environment where clusters are frequently created and destroyed.

Reference: Refer to the AWS documentation on Network Security Groups and Nutanix documentation on best practices for securing NC2 clusters.

Question 7

A company has just adopted Nutanix as their technology of choice and is preparing to deploy Nutanix Cloud Clusters (NC2).

Which step must be taken first to again access to the CN2 console?

Options:

A- Navigate to cloud.nutanix.com

B- Start a free trial via Billing Portal.

C- Open a support case with Nutanix.

D- Create a My Nutanix account

Answer:

D

Explanation:

Before accessing the Nutanix Cloud Clusters (NC2) console, the first step is to create a My Nutanix account.

This account serves as the primary gateway for managing and accessing Nutanix services, including NC2.

Once the account is created, users can log in to the Nutanix portal, where they can manage their subscriptions, start trials, and access various Nutanix services, including the NC2 console.

Reference: Refer to the Nutanix documentation on getting started with NC2 and the My Nutanix account creation process.

Question 8

Question Type: **MultipleChoice**

When selecting the NC2 subscription plan from the Nutanix Billing portal, which options are available.

Options:

A- Pay-as-you-Go (PayG), Cloud Provider Credits, Bring your own License (BYOL)

B- Reserved Instances, Cloud Provider Credits, Bring your own License (BYOL)

C- Pay-as-you-Go (PayG), Bring your own License (BYOL)

D- Reserved Instances, Bring your own License (BYOL)

Answer:

C

Explanation:

When selecting the NC2 subscription plan from the Nutanix Billing portal, the available options include:

Pay-as-you-Go (PayG): A flexible payment option where users are billed based on their actual usage, providing cost efficiency for variable workloads.

Bring your own License (BYOL): Allows users to utilize existing Nutanix licenses they have purchased, offering a cost-effective way to leverage existing investments in Nutanix software.

Reference: Refer to the Nutanix billing and subscription documentation for detailed descriptions of subscription plans and their benefits.

Question 9

Question Type: **MultipleChoice**

An administrator seeks to ensure that the newly created NC2 organization named Finance can only deploy clusters into certain cloud regions.

What action should the administrator take to do this?

Explanation:

To ensure that the newly created NC2 organization named Finance can only deploy clusters into certain cloud regions, the administrator should specify the allowed regions during the cloud account configuration.

This action restricts the regions available for cluster deployment, ensuring compliance with organizational policies or regulatory requirements.

The allowed regions can be set in the cloud account settings associated with the Finance NC2 organization, defining the geographical scope of operations.

Question 10

Question Type: **MultipleChoice**

To manually create an AWS VPC with Public access to Prism Element for testing purposes, Which components must be created?

Options:

A- VPC, Delegated Subnets, Route Tables, NAT Gateway, Internet Gateway, Load balancer

B- VPC, Delegated Subnets, Route Tables, NAT Gateway, vNets, Load balancer

C- VPC Subnets Route Tables NAT Gateway, Internet Gateway, Load balancer

D- VPC Subnets Route subnets, Route Tables, NAT Gateway, Internet Gateway, VPN

Answer:

A

Explanation:

To manually create an AWS VPC with Public access to Prism Element for testing purposes, the following components must be created:

VPC: A Virtual Private Cloud to provide an isolated network for the resources.

Delegated Subnets: Subnets within the VPC to segment the network and allocate IP ranges.

Route Tables: To define routing rules for the subnets to ensure proper traffic flow.

NAT Gateway: To enable instances in the private subnets to access the internet.

Internet Gateway: To allow direct internet access to instances in the public subnets.

Load Balancer: To distribute traffic across multiple instances for improved availability and redundancy.

Reference: Refer to the AWS documentation on VPC creation and Nutanix documentation on network setup for Prism Element access.

Question 11

Question Type: **MultipleChoice**

An administrator is tasked with enabling inbound internet access to two Virtual Servers in an NC2 cluster on AWS for the HTTPs protocol.

The cluster is configured with:

* 8 nodes

* Prism Central

* 3 x User VM subnets

All subnets have been configured and can communicate with Internet-based resources as well as on-premises servers. The company d to allow Internet access, so the administrator must implement an AWS solution.

Which approach will enable the necessary communication?

Options:

A- Create a WS Network Load Balancer, configure the listener TCP port as 80, create a target groud and register the servers as the endpoint

B- Create a AWS Network Load Balancer, configure the listener TCP port as 443, create a target group and register an HP as the endpoint.

C- Create a AWS Network Load Balancer, configure the lister TCP port as 433, create a target group and register an EIP as the Endpoint.

D- Create a AWS Network Load Balancer, configure the listener TCP port as 80, create a target group and register the servers as targets.

Answer:

B

Explanation:

To enable inbound internet access to Virtual Servers in an NC2 cluster on AWS for the HTTPS protocol, the administrator should use an AWS Network Load Balancer (NLB).

Configure the NLB listener to listen on TCP port 443, which is the standard port for HTTPS traffic.

Create a target group in AWS, and register the servers (Virtual Servers in the NC2 cluster) as targets within this group.

Ensure the NLB is properly configured with an Elastic IP (EIP) if required, to provide a static IP address for the load balancer.

Verify that the security groups and network ACLs associated with the load balancer and the target group allow inbound traffic on port 443.

Reference: Refer to AWS documentation on Network Load Balancers and Nutanix NC2 on AWS integration guides for step-by-step instructions on setting up and configuring the necessary components for enabling HTTPS access.

Question 12

Question Type: **MultipleChoice**

What role is needed to create a cluster?

Options:

A- Customer Administrator

B- Customer Security Administrator

C- Cluster Super Admin

D- Cluster Administrator

Answer:

C

Explanation:

To create a cluster in Nutanix Cloud Integration with AWS, the role needed is Cluster Super Admin.

The Cluster Super Admin role provides the highest level of privileges required to perform critical operations such as creating, managing, and deleting clusters.

This role is essential for overseeing the cluster setup and configuration processes, ensuring the user has full control over the cluster lifecycle.

Reference: Refer to the Nutanix documentation on roles and permissions for NC2 on AWS for further details on the capabilities and required permissions for cluster creation.