

Nutanix Certified Professional - Cloud Integration - AWS (NCP-CI-AWS) v6.7

Nutanix NCP-CI-AWS

Version Demo

Total Demo Questions: 16

Total Premium Questions: 162

Buy Premium PDF

<https://passqueen.com>

support@passqueen.com

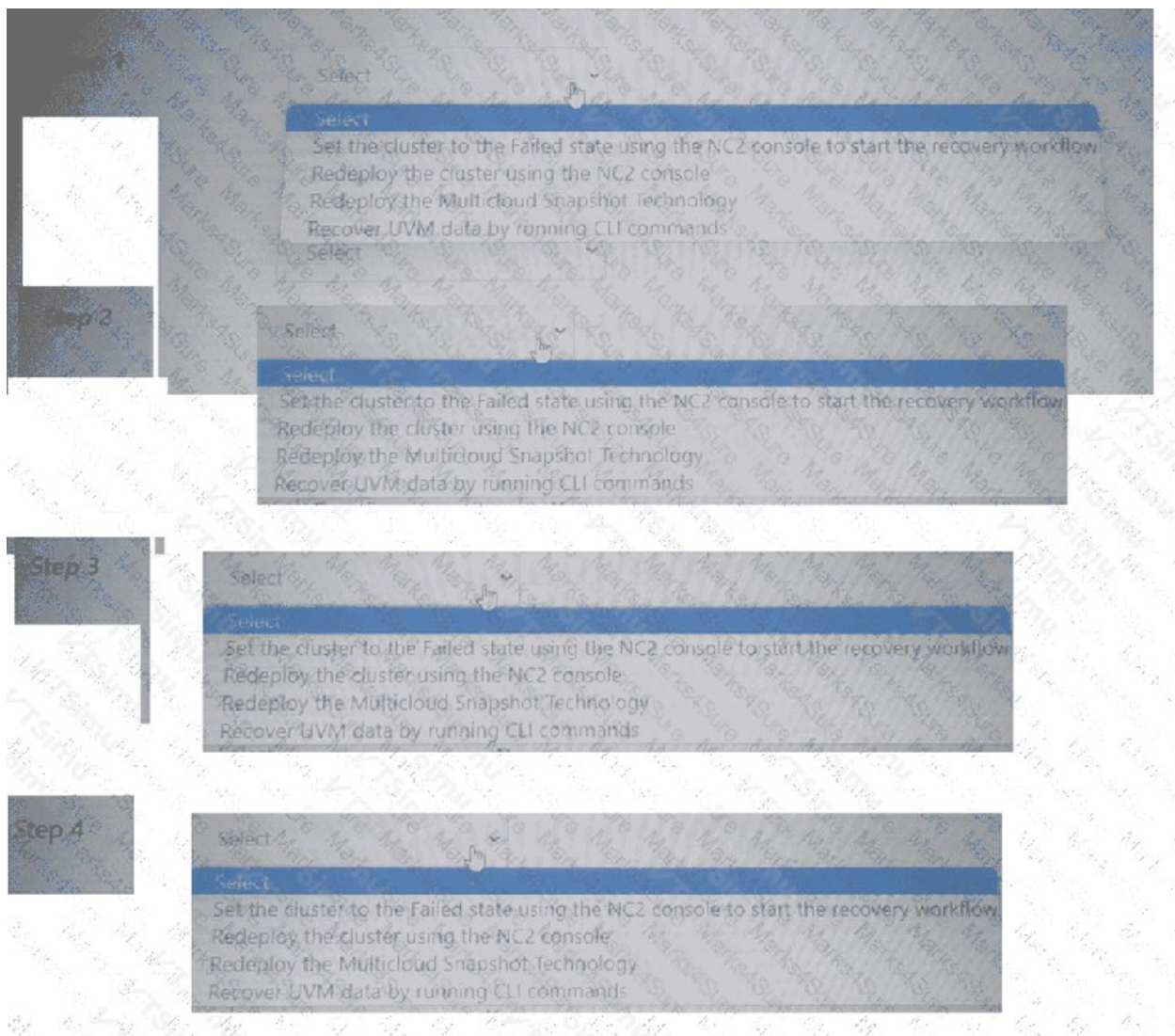
Topic Break Down

Topic	No. of Questions
Topic 1, Plan a Nutanix Cloud Clusters (NC2) on AWS Deployment	43
Topic 2, Deploy Nutanix Cloud Clusters (NC2) on AWS	19
Topic 3, Configure Network Connectivity	55
Topic 4, Manage Nutanix Cloud Clusters (NC2) on AWS	42
Topic 5, Migrate Workloads to Nutanix Cloud Clusters (NC2) on AWS	3
Total	162

QUESTION NO: 1 - (SIMULATION)

An administrator needs to recover a cluster protected using the Cluster Protect feature. The Prism Central instance was not on the failed cluster.

Which steps, in order, should the administrator perform to recover the cluster?



ANSWER: See the explanation for the answer

Explanation:

Correct recovery sequence:

Because Prism Central was not hosted on the failed cluster, it remains available to manage the recovery. First declare the original cluster failed, then deploy its replacement. After the replacement is available, redeploy MST so the snapshot-based recovery mechanism is available, and finally use the CLI recovery procedure to restore the user VM data.

QUESTION NO: 2

An administrator needs to deploy AWS networking resources for an NC2 cluster. Which option should the administrator consider to complete this task?

- A. Only NC2 can deploy the required AWS resources from the Portal.
- B. Allow NC2 to deploy the required AWS resource or use the Marketplace resource deployment.

C. Only BYO resources using the manual workflow is supported.

D. Allow NC2 to deploy the required AWS resource or BYO resource using the manual workflow.

ANSWER: D

Explanation:

Allow NC2 to deploy the required AWS resource or BYO resource using the manual workflow is correct because NC2 on AWS supports two valid approaches for the networking foundation needed by a cluster. During deployment, an administrator can authorize the NC2 service to create the required AWS networking components, allowing the deployment workflow to provision and configure the supported infrastructure automatically. Alternatively, organizations that require ownership of network design, existing connectivity, naming standards, routing, security controls, or IP addressing can bring their own AWS networking resources. In that model, the administrator prepares the required environment and uses the manual workflow to supply the relevant existing-resource details for the cluster deployment. This flexibility lets NC2 fit both greenfield deployments and enterprise AWS environments with centrally governed networking. The AWS networking components involved are based on the Amazon VPC model, including the virtual network and its associated connectivity and address-planning constructs. Refer to the [Nutanix documentation portal](#) for the NC2 on AWS deployment documentation and to the [Amazon VPC User Guide](#) for AWS networking fundamentals.

QUESTION NO: 3

An administrator has noticed the company's NC2 free trial expired 60 days ago.

What should the administrator do to continue using all of the NC2 features on existing clusters?

A. Switch to a paid subscription plan.

B. Nothing. The clusters will have full feature support.

C. Contact Nutanix support to redeploy the cluster.

D. Contact the AWS cloud vendor.

ANSWER: A

Explanation:

Switch to a paid subscription plan. An NC2 free trial is intended for evaluation and does not provide an ongoing entitlement to use the full NC2 service after its expiration. To retain full functionality for the company's existing NC2 clusters, the organization must obtain the appropriate NC2 subscription and associate the available entitlement with its cloud deployment. A paid subscription establishes the licensing basis for continued operation of NC2 and its supported capabilities, including ongoing cluster management through the Nutanix cloud platform. The administrator should work through the organization's Nutanix account team or approved purchasing channel to select and activate the subscription capacity that matches the deployed NC2 environment. This conversion allows the existing deployment to remain licensed rather than treating the expired evaluation period as a renewable operating state. Nutanix describes NC2 on AWS as a subscription-based hybrid multicloud service; its product information is available at [Nutanix Cloud Clusters on AWS](#). Additional subscription and entitlement resources are available through the [Nutanix Support Portal](#).

QUESTION NO: 4

An administrator has deployed an NC2 cluster on AWS to an existing environment for VDI.

Afterwards, the corporate security teams direct the administrator to reuse an existing AWS subnet, 10.79.4.0/24 that has two EC2 instances: EC2-1 (10.79.4.200) and EC2-2 (10.79.4.201). The security team indicates that this directive is to avoid overlap with the AHV IPAM.

Which two configuration actions should the administrator take to ensure there are no configuration issues? (Choose two.)

A. aCLI > net.add_to_ip_blacklist 10.79.4.200 aCLI > net.add_to_ip_blacklist 10.79.4.201

- B. Deploy two VMs on the NC2 cluster and assign 10.79.4.200 and 10.79.4.201 as the assigned IPs in Prism Element
- C. aCLI > net.de/ete_from_ip_blacklist 10.79.4.200 aCLI > net.defete_fromjp_blacklist 10.79.4.201
- D. Configure the AHV IPAM to use DHCP range 10.79.4.2 -10.79.4.253.

ANSWER: A D

Explanation:

Using aCLI > net.add_to_ip_blacklist 10.79.4.200 aCLI > net.add_to_ip_blacklist 10.79.4.201 reserves the two addresses already used by EC2-1 and EC2-2 from the AHV IPAM allocation process. IP blacklisting is important when AHV IPAM serves a subnet containing addresses assigned outside the Nutanix cluster, because it prevents AHV from dynamically leasing those addresses to guest VMs. The commands should be issued separately, once for each existing EC2 address.

Configuring AHV IPAM to use the DHCP range 10.79.4.2 - 10.79.4.253 establishes the pool from which AHV can provide addresses on the reused /24 network. Combined with the blacklist entries, this lets IPAM manage valid guest addresses in the subnet while retaining the EC2 addresses as exclusions. The configuration therefore avoids duplicate use of the existing AWS workload addresses while allowing VDI guests to receive IP configuration through the AHV-managed network. Nutanix documents IP address management and address-exclusion concepts in the [AHV Administration Guide](#); AWS also documents the reserved-address behavior applicable to VPC subnets in its [VPC subnet sizing documentation](#).

QUESTION NO: 5

Which address must AWS Directory Service be able to resolve when deploying a new NC2 cluster?

- A. gateway-internal-api.cloud.nutanix.com
- B. gateway-external-api. cloud, nutanix.com
- C. dovvnloads.cloud.nutanix.com
- D. apikeys.nutanix.com

ANSWER: B

Explanation:

The required address is **gateway-external-api.cloud.nutanix.com**, represented by “gateway-external-api. cloud, nutanix.com” in the question. During an NC2 on AWS deployment, Nutanix Cloud Clusters uses the external Nutanix gateway API endpoint for cloud-control-plane communication. AWS Directory Service DNS must be able to resolve this fully qualified domain name so the deployment workflow and the resulting cluster can establish the required connectivity to Nutanix cloud services. This requirement is especially important when the AWS environment uses custom DNS, restrictive outbound DNS rules, conditional forwarding, or network security controls that limit name resolution to approved destinations. Ensure that the DNS servers used by AWS Directory Service can recursively resolve the endpoint through the configured DNS path and that associated network policies permit the necessary outbound service communication. Nutanix documents the DNS and connectivity prerequisites as part of NC2 on AWS deployment planning in the [NC2 on AWS Deployment Guide](#). Additional NC2 on AWS product documentation is available through the [Nutanix Support Portal](#).

QUESTION NO: 6

An administrator needs to configure Cross Cluster Live Migration for an NC2 on AWS deployment. Which networking configuration is supported for this task?

- A. Standard AWS networking is deployed.
- B. Between an on-premises cluster and NC2 on AWS.
- C. Between an NC2 on Azure and NC2 on AWS cluster.

D. Flow Virtual Networking is deployed.

ANSWER: D

Explanation:

Flow Virtual Networking is deployed. is the supported configuration for Cross Cluster Live Migration in an NC2 on AWS environment. Cross Cluster Live Migration moves the execution of a running VM between Nutanix clusters while preserving the workload's network identity and connectivity. Flow Virtual Networking supplies the software-defined overlay networking required for that mobility. Its virtual networks are decoupled from the underlying AWS physical and native network constructs, allowing the VM's network attachment to remain available as the VM transitions to the destination cluster. This overlay-based design is what enables a consistent tenant network across participating clusters and supports the continuity required by a live migration workflow.

Administrators should ensure that Flow Virtual Networking has been configured on the participating NC2 on AWS clusters and that the relevant virtual network and associated policy configuration are available where the workload will run. This is an architectural prerequisite rather than merely a VM-level migration setting: the destination cluster must be able to provide the same overlay-network connectivity to the migrated VM. Nutanix documentation for Flow describes its role in creating virtualized, software-defined network environments, while NC2 documentation covers supported cloud deployment and networking capabilities. See the [Nutanix Flow Virtual Networking overview](#) and the [Nutanix Cloud Clusters on AWS overview](#).

QUESTION NO: 7

During the deployment of the first NC2 cluster on AWS, Flow Virtual Networking automatically creates a transit VPC that contains a subnet. By default, what is the name of this subnet?

- A. overlay-external-subnet-nonat
- B. overlay-external-subnet-nat
- C. overlay-internal-subnet-nonat
- D. overlay-internal-subnet-nat

ANSWER: A

Explanation:

overlay-external-subnet-nonat is the default subnet name created in the transit VPC when Flow Virtual Networking is enabled during initial NC2 on AWS deployment. Flow Virtual Networking extends networking capabilities to NC2 environments and uses AWS networking constructs to provide connectivity between the overlay-based virtual networks and external destinations. The transit VPC is created as part of this infrastructure, and the non-NAT external subnet provides the default path for overlay workloads that require routed connectivity without source-address translation. Preserving the original source address is especially important for communication with connected enterprise networks, including networks reached through hybrid connectivity such as AWS Transit Gateway or VPN connections. The naming convention explicitly identifies both the subnet's external-overlay role and its non-NAT behavior, making **overlay-external-subnet-nonat** the expected default resource name. Nutanix NC2 documentation provides the AWS deployment and networking context for these automatically provisioned components, while the Flow Virtual Networking documentation describes the overlay networking architecture and external connectivity model. See [Nutanix Cloud Clusters on AWS documentation](#) and [Nutanix Flow Virtual Networking](#).

QUESTION NO: 8

An administrator is planning an NC2 deployment and wants to connect to AWS Services privately from the corporate VPC without going through the public internet.

Which connectivity solution should the administrator use?

- A. Point-to-Site VPN

- B. Gateway Endpoint
- C. VTEP Gateways
- D. Site-to-Site VPN

ANSWER: B

Explanation:

Gateway Endpoint is the appropriate solution when the required private AWS-service access is to Amazon S3 or Amazon DynamoDB. A gateway endpoint is created within a VPC and provides a private route to the supported service without requiring an internet gateway, NAT device, VPN connection, or public IP addressing. Traffic remains on the AWS network, and endpoint policies can be used to control which principals and resources may use the endpoint. Route tables associated with the endpoint receive the relevant service prefix-list route, so workloads in the VPC can reach the service privately and transparently. This is useful for an NC2-related design that must access supported AWS storage or database services while maintaining a private network path and avoiding public-internet traversal. AWS documents gateway endpoints as a VPC endpoint type specifically available for Amazon S3 and DynamoDB; other AWS services generally require interface endpoints instead. See the [AWS VPC endpoint documentation](#) and the [Amazon S3 gateway endpoint documentation](#) for endpoint behavior, routing, and supported-service details.

QUESTION NO: 9

What happens if there are not enough AWS bare-metal nodes available in the selected region during an NC2 cluster expansion?

- A. Cluster enters maintenance mode until nodes are available.
- B. Expansion continues with fewer nodes than requested.
- C. NC2 retries provisioning and may fail, so the administrator must verify node availability with AWS.
- D. The NC2 console will retry the deployment until suitable nodes are available.

ANSWER: C

Explanation:

NC2 retries provisioning and may fail, so the administrator must verify node availability with AWS. An NC2 on AWS expansion requires AWS to allocate the requested supported bare-metal EC2 capacity in the selected deployment location. Bare-metal capacity is physical, location-specific AWS infrastructure, rather than capacity that NC2 can reserve or create independently. When AWS cannot fulfill the EC2 request because sufficient capacity is not available, the node-provisioning workflow can retry the request, but it cannot complete the expansion unless AWS returns the required instances. After the retry process is exhausted, the expansion can fail and requires administrator action. The appropriate next step is to validate capacity and service conditions with AWS, then retry when capacity is available or use an appropriate alternative deployment location or supported configuration if operational requirements permit. AWS documents that an *InsufficientInstanceCapacity* condition occurs when it cannot provide the requested instance capacity in the requested Availability Zone, and recommends modifying the request or trying again later. See [AWS EC2 launch-capacity troubleshooting](#). NC2 AWS requirements and supported infrastructure details are maintained in the [Nutanix Cloud Clusters on AWS Deployment Guide](#).

QUESTION NO: 10

Where can the status of a Layer 2 Extension be checked within the management interface?

- A. Prism Central > Network and Security > Network Services > Subnet Extensions
- B. Prism Central > Network and Security > Connectivity > Subnet Extensions
- C. Prism Central > Network and Security > Virtual Private Clouds > Subnet Extensions
- D. Prism Central > Network and Security > Subnets > Subnet Extensions

ANSWER: A

Explanation:

Prism Central > Network and Security > Network Services > Subnet Extensions is the correct management path for checking a Layer 2 Extension. Subnet Extensions are the Prism Central feature used to present and manage stretched Layer 2 networks between an on-premises Nutanix environment and an NC2 on AWS environment. The Subnet Extensions view provides the operational context administrators need for each configured extension, including its connectivity and status information. This makes it the appropriate place to confirm that an extension is available before relying on it for workload mobility or communication between virtual machines across the connected environments.

Checking the extension from this view also supports day-to-day hybrid-cloud operations: an administrator can identify the extension associated with a particular subnet, validate its state, and investigate the relevant network-service configuration when connectivity needs attention. Layer 2 extension is specifically managed as a network service rather than as a generic subnet or VPC object, so the Network Services area is the relevant Prism Central workflow. Nutanix describes NC2 on AWS networking and its supported hybrid-cloud connectivity capabilities in its [NC2 on AWS product documentation](#) and provides product documentation through the [Nutanix Support Portal](#).

QUESTION NO: 11

An administrator needs to understand which of the services implemented on their NC2 AWS deployment will be protected with Cluster protect.

Which service of feature is Cluster Protect able to both protect and recover its associated metadata?

- A. Object
- B. VM templates
- C. Files
- D. Categories

ANSWER: B C

Explanation:

VM templates and **Files** are supported by Cluster Protect for protection and recovery with their associated metadata in an NC2 on AWS environment. Protecting VM templates preserves the reusable VM definitions and configuration information needed to restore and continue using those templates after recovery. This is important because templates commonly provide standardized operating-system images and baseline VM settings for deployments.

For Nutanix Files, Cluster Protect safeguards the file-service data together with the metadata required to restore the protected file-service workload in a usable state. Recovering the associated metadata ensures that the recovered Files deployment retains the information necessary for the service and its protected content to be correctly reconstructed, rather than restoring data without its related service context.

These capabilities are part of Nutanix data-protection workflows for cloud deployments, where protection domains, schedules, snapshots, and recovery operations are managed through the Nutanix platform. See the [NC2 on AWS Administration Guide: Cluster Protect](#) and the [Nutanix Files documentation](#) for supported protection and recovery workflows.

QUESTION NO: 12

Which two actions are exclusive to the "Bring Your Own" (BYO) deployment of AWS resources for an NC2 cluster? (Choose two.)

- A. Set up the AWS account permissions.
- B. Configure an AWS IAM user.
- C. Create an AWS VPC.

D. Create the required subnets.

ANSWER: C D

Explanation:

Creating an AWS VPC and creating the required subnets are the actions that characterize a Bring Your Own deployment for an NC2 cluster on AWS. In this deployment model, the customer prepares the networking foundation in AWS before beginning cluster creation. That foundation includes a VPC with the network layout needed by the cluster and appropriately configured subnets for NC2 components and workload connectivity. The deployment workflow then consumes those pre-existing networking resources rather than creating a new network environment on the customer's behalf.

This approach is useful when an organization needs the NC2 cluster integrated into an established AWS network design, including existing routing, connectivity, address-space governance, and security controls. Nutanix documents that deployments can use existing AWS networking resources, with the required VPC and subnets supplied as part of the cluster-deployment configuration. The AWS VPC documentation also describes VPCs and subnets as the fundamental resources used to define isolated virtual networks and their IP address ranges. See the [Nutanix Cloud Clusters on AWS Deployment Guide](#) and [AWS VPC User Guide](#).

QUESTION NO: 13

An administrator desires to add a node to an existing 3-node NC2 cluster on AWS. After 40 minutes, an alert indicates that a "boot timeout" has been reached. Proper credentials and account settings have been verified. Which two other options might be the cause of this alert? (Choose two.)

- A. A network cannot be reached due to the wrong VPC settings.
- B. <https://downloads.cloud.nutanix.com> is not allowed through the firewall.
- C. There is a quota configured on the cloud account.
- D. There is an instance limit configured on the cloud account.

ANSWER: A B

Explanation:

A network cannot be reached due to the wrong VPC settings. is a valid cause because a newly added NC2 node must be deployed into a VPC with the required routing, subnet configuration, security-group access, and connectivity to the existing cluster services. If the selected VPC or its associated networking configuration prevents the new instance from reaching required endpoints or cluster components during initialization, the node cannot complete its startup workflow. NC2 continues waiting for the node to become available until the configured boot-time limit is reached, resulting in a boot-timeout alert.

<https://downloads.cloud.nutanix.com> is not allowed through the firewall. is also a valid cause. During node deployment and initialization, NC2 requires access to Nutanix-hosted download services for required software artifacts and bootstrapping content. Firewall, proxy, network ACL, route-table, or egress policy rules that block this endpoint can prevent the node from completing initialization even though AWS credentials and cloud-account configuration are valid. Nutanix deployment planning therefore requires outbound connectivity to the documented Nutanix endpoints, as well as correctly configured AWS VPC networking. See the [NC2 on AWS Administration Guide](#) and [Amazon VPC documentation](#).

QUESTION NO: 14

An administrator is planning to update from using native AWS subnets to using an overlay network in the currently deployed NC2 clusters on AWS. Which two prerequisites should the administrator validate to ensure a seamless migration? (Choose two.)

- A. External IPAM is properly configured for cloud subnets.
- B. AWS subnets must already be created and attached to the target AWS VPC.

- C. Corresponding cloud subnets must be added in the Prism Element UI and mapped to AWS subnets.
- D. Ensure Prism Central and Prism Element are running AOS 7.3 or later.

ANSWER: A C

Explanation:

External IPAM must be properly configured for the cloud subnets, and corresponding cloud subnets must be added in Prism Element and mapped to the AWS subnets. During migration to Flow Virtual Networking, the cloud subnet provides the relationship between the virtual overlay environment and the AWS VPC subnet used for underlay connectivity. The mapping ensures that overlay-network traffic can be routed through the appropriate AWS subnet while preserving the required connectivity for AHV hosts, Controller VMs, and guest workloads. External IPAM is required so that address allocation for these cloud subnets is governed by the configured external address-management source rather than relying on an unavailable or unsuitable local allocation method. Validating both items before migration establishes the required underlay association and IP-address lifecycle management, reducing the risk of address conflicts or workload connectivity interruptions as virtual networks are moved onto the overlay. Nutanix documents cloud-subnet configuration as part of NC2 on AWS networking and describes Flow Virtual Networking as the overlay networking capability used to create and manage virtual networks independently of the physical network. See the [NC2 on AWS Administration Guide](#) and the [Flow Virtual Networking documentation](#).

QUESTION NO: 15

Refer to Exhibit:

An administrator is deploying an NC2 cluster on AWS that has been sized for performance applications. The cluster has two node types: i4i.metal and i7ie.metal-48xl. When the administrator attempts to deploy the cluster, the option to add EBS storage volumes is not available. How would the administrator add additional EBS volumes for storage capacity to the cluster? (Choose two.)

- A. Add an additional i7ie.metal-48xl node so that it 's a multiple of the RF.
- B. Add a host type that supports EBS volumes.
- C. EBS storage can be added in the next step of the deployment wizard.
- D. Use only a single node type within the cluster.

ANSWER: A B

Explanation:

Adding an additional i7ie.metal-48xl node so that it is a multiple of the RF is required because EBS-backed capacity in a heterogeneous NC2 cluster must be provisioned in a manner that preserves the cluster's configured replication-factor resilience. Capacity contributions from a given node type need to align with the replication factor; this lets Nutanix distribute protected data consistently across the applicable nodes and maintain the expected failure tolerance. Adding the necessary i7ie.metal-48xl node therefore makes the node-type count eligible for the EBS-capacity configuration.

Adding a host type that supports EBS volumes is also required when the selected instance configuration lacks the required EBS-volume support. NC2 deployment validates the AWS instance types selected for the cluster before exposing supplemental EBS storage configuration. The administrator must include an eligible host type so the deployment workflow can offer EBS volumes as capacity resources. This validation reflects both the NC2 deployment design and AWS's EBS attachment capabilities for supported EC2 instances. Nutanix NC2 deployment documentation is available through the [Nutanix Cloud Clusters on AWS documentation portal](#); AWS also documents [Amazon EBS volume attachment](#) requirements and behavior.

QUESTION NO: 16

Administrator has recently deployed an NC2 cluster on AWS in the North Virginia region in availability zone us-east-id. The consuming IPS from a 10.78.2.0/24 range.

The AWS VPC has two available CIDR ranges:

10.78.0.0/16

10.19.101.0/24

The following subnet have been configured in the NC2 AWS VPC:

Which two subnet will show up in the Network configuration of the Prism Element Settings page? (Choose two.)

- A. DR01
- B. L2stretch
- C. VDI
- D. DR02

ANSWER: A B

Explanation:

DR01 and **L2stretch** will be available in Prism Element network configuration. NC2 on AWS exposes AWS subnets that are usable by the cluster, which includes validating that the subnet belongs to the cluster VPC and is in the Availability Zone used by the NC2 cluster. DR01 uses the 10.78.2.0/24 range, which is contained within the VPC's 10.78.0.0/16 CIDR and corresponds to the cluster's stated IP range. It is therefore an eligible subnet for network configuration and VM connectivity.

L2stretch uses 10.19.101.0/24, the VPC's additional CIDR range. AWS VPCs can have secondary IPv4 CIDR blocks, and subnets created from an associated secondary CIDR block are part of that VPC. Consequently, a subnet from this associated range can be presented to the NC2 cluster when it meets the cluster Availability Zone requirement. This capability is particularly useful when extending address space without changing the original VPC CIDR allocation.

For NC2 networking concepts and AWS VPC/subnet behavior, see the [Nutanix Cloud Clusters documentation](#) and the [AWS documentation for adding IPv4 CIDR blocks to a VPC](#).