

Nutanix.NCP-CI-AWS.v2024-11-18.q28

Exam Code:	NCP-CI-AWS
Exam Name:	Nutanix Certified Professional - Cloud Integration - AWS
Certification Provider:	Nutanix
Free Question Number:	28
Version:	v2024-11-18
# of views:	350
# of Questions views:	280
https://www.freepdfdumps.com/Nutanix.NCP-CI-AWS.v2024-11-18.q28.html	

NEW QUESTION: 1

An administrator needs to create user VM subnets for multiple NC2 clusters in AWS.

What would be the best approach to take?

- A. Create guest-VM VNets for each cluster.
- B. Use the cluster management subnet dedicated to each cluster.
- C. Create guest-VM subnets to be shared by all clusters.
- D. Create guest-VM subnets for each cluster.

Answer: D (LEAVE A REPLY)

When creating user VM subnets for multiple NC2 clusters in AWS, the best approach is to create guest-VM subnets for each cluster. This ensures that each cluster has its own dedicated subnets, which simplifies network management and avoids potential IP conflicts.

Advantages of Dedicated Subnets:

Isolation: Each cluster operates in its own subnet, providing better isolation and security.

Management: Easier to manage and troubleshoot network issues when each cluster has its own subnets.

Scalability: More scalable as each subnet can be managed and expanded independently.

Steps to Create Guest-VM Subnets:

Identify the IP range for each subnet.

In the AWS VPC console, create a new subnet for each cluster using the identified IP ranges.

Associate the new subnets with the respective clusters during or after the cluster deployment process.

Why Not Shared Subnets:

Shared subnets could lead to IP conflicts and make network management more complex, especially as the number of clusters grows.

Reference:

Nutanix Cloud Clusters on AWS Administration Guide

AWS VPC Subnet Creation Documentation

NEW QUESTION: 2

What role is needed to create a cluster?

- A. Customer Administrator
- B. Customer Security Administrator
- C. Cluster Super Admin
- D. Cluster Administrator

Answer: C ([LEAVE A REPLY](#))

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.

NEW QUESTION: 3

An administrator needs to backup Prism Central configuration data to an Amazon S3 bucket.

Which pcdr-cli command parameters is needed to satisfy this task?

- A. deployment-info
- B. protect
- C. list-protection-targets
- D. recover

Answer: B ([LEAVE A REPLY](#))

To backup Prism Central configuration data to an Amazon S3 bucket, the pcdr-cli command with the protect parameter is used. This parameter is specifically designed for creating protection policies and backing up Prism Central data.

Reference:

Nutanix Prism Central Documentation

Nutanix pcdr-cli Command Reference

NEW QUESTION: 4

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?

- 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: ([SHOW ANSWER](#))

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:

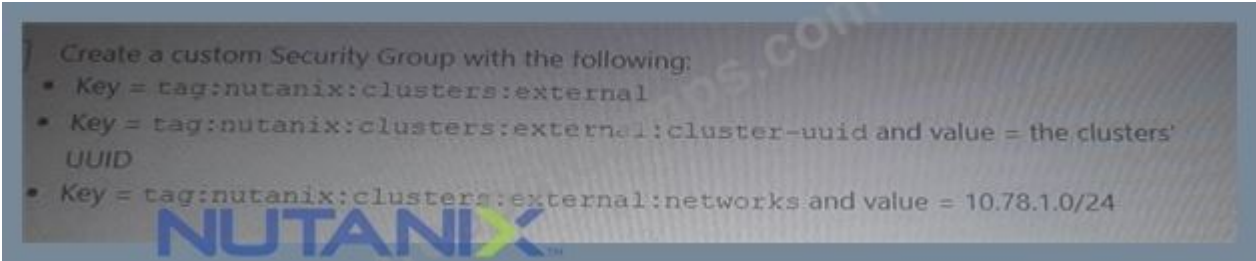
Refer to the Nutanix and AWS documentation on subnet configuration and requirements for NC2 cluster deployments, specifically addressing IPv4 and IPv6 compatibility and constraints.

NEW QUESTION: 5

An administrator has deployed an NC2 on AWS cluster that is running mixed workloads. Multiple SQL database are running on the NC2 cluster using a native subnet of 10.78.1.0/24.

The administrator wants to ensure only application servers from source subnet 10.79.1.0/24 that reside outside of the NC2 cluster can access the databases.

Which two actions will help the administrator most securely achieve this? (Choose two.)



```
Create a custom Security Group with the following:
```

- Key = tag:nutanix:clusters:external
- Key = tag:nutanix:clusters:external:cluster-uuid and value = the clusters' UUID
- Key = tag:nutanix:clusters:external:networks and value = 10.78.1.0/24

- A.
- B.
- C.
- D.

Answer: ([SHOW ANSWER](#))

To ensure that only application servers from the source subnet 10.79.1.0/24 can access the SQL databases running on the NC2 cluster in the subnet 10.78.1.0/24, the administrator can take the following actions:

Option A: Create a custom Security Group with the following rules:

Key = tag:nutanix:clusters

Key = tag:nutanix:clusters:external

and value = the clusters' UUID

Key = tag:nutanix:clusters:external

and value = 10.78.1.0/24

Option D: Create a custom Security Group with the following:

Key = nutanix:clusters

Key = nutanix:clusters:external

and value = the clusters' UUID

Key = nutanix:clusters:external

and value = 10.79.1.0/24

These actions help create security rules that restrict access to the databases only from the specified source subnet, ensuring secure and controlled access.

Reference:

Nutanix Cloud Clusters on AWS Administration

AWS Security Groups Documentation

NEW QUESTION: 6

An administrator has been tasked with ensuring NC2 VMs are able to access AWS resources. The NC2 VM traffic must not traverse the internet.

in which two ways would the administrator achieve this? (Choose two.)

- A.** By using a Gateway Endpoint
- B.** By using a NAT Gateway.
- C.** By using an Interface Endpoint
- D.** By using a VPC Peer.

Answer: C,D (LEAVE A REPLY)

To ensure that NC2 VMs can access AWS resources without traversing the internet, the administrator can use AWS VPC Peering and Interface Endpoints. Both methods ensure that traffic stays within the AWS network, maintaining security and efficiency.

Interface Endpoint:

Interface Endpoints allow you to privately connect your VPC to supported AWS services. They use AWS PrivateLink to route traffic directly to services within the AWS network, bypassing the public internet.

Steps:

Create an interface endpoint for the required service in the AWS VPC console.

Ensure the security groups and route tables are configured to allow traffic to the interface endpoint.

VPC Peering:

VPC Peering allows the routing of traffic between VPCs using private IP addresses, without the need for internet gateways, NAT devices, or VPN connections.

Steps:

Create a VPC peering connection between the VPCs.

Update the route tables to direct traffic between the peered VPCs.

Ensure security group rules allow the necessary traffic between VPCs.

Reference:

AWS VPC Peering Documentation

NEW QUESTION: 7

Which statement is true regarding AWS account requirements?

- 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: ([SHOW ANSWER](#))

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.

NEW QUESTION: 8

An administrator has deployed an NC2 on AWS cluster and doesn't have connectivity back to the on-premises environment yet. The administrator wants to SSH into a CVM to edit a security setting and has deployed a Jump Host into an existing public subnet.

What action must the administrator still take to gain access to the CVM?

- A.** Edit the CVM iptables to allow SSH.
- B.** Edit the User Management Network Security Group to allow SSH from the Jump Host IP.
- C.** Edit the UVM security group to allow SSH from the Jump Host IP and remove Cluster Lockdown.
- D.** Create Custom Network Security Group at the subnet level and add the IP address of the Jump Host

Answer: **B** ([LEAVE A REPLY](#))

To SSH into a Controller VM (CVM) in an NC2 on AWS cluster without on-premises connectivity, the administrator needs to ensure that the security settings allow SSH access from the Jump Host. This involves editing the User Management Network Security Group to permit SSH traffic from the Jump Host IP.

Deploy Jump Host:

Ensure the Jump Host is deployed in a public subnet with an Elastic IP (EIP) assigned for external access.

Edit User Management Network Security Group:

Locate the security group associated with the user management network.

Modify the inbound rules to allow SSH (port 22) from the Jump Host's IP address. This ensures that the Jump Host can establish an SSH connection to the CVM.

Steps to Edit Security Group:

Navigate to the EC2 dashboard in the AWS Management Console.

Select "Security Groups" under the "Network & Security" section.

Find and select the appropriate security group.

Edit the inbound rules to add a new rule:

Type: SSH

Protocol: TCP

Port Range: 22

Source: Custom IP (enter the Jump Host's public IP address)

Additional Configuration:

Ensure that the CVM itself allows SSH connections and that no internal firewall rules block the traffic.

Reference:

Nutanix Cloud Clusters on AWS Administration Guide

AWS Security Group Documentation

Nutanix Best Practices for Secure Access

NEW QUESTION: 9

A company has purchased Nutanix AOS Pro licensing.

Which add-on products are available with this license tier in the AWS cluster deployment wizard?

A. EUC

B. Nus

C. Self-Service and Cost Governance

D. Files, Advanced Replication, and DARE

Answer: D ([LEAVE A REPLY](#))

With the Nutanix AOS Pro licensing, several advanced features and add-on products become available. Specifically, in the AWS cluster deployment wizard, the following add-ons are available:

Files:

Nutanix Files provides a software-defined, scale-out file storage solution that simplifies the management and scaling of unstructured data.

Advanced Replication:

Advanced Replication features in Nutanix include synchronous and asynchronous replication capabilities, allowing for robust disaster recovery and data protection solutions.

DARE (Data-At-Rest Encryption):

DARE ensures that all data stored on Nutanix clusters is encrypted, providing a higher level of security for sensitive information.

These features are included in the AOS Pro licensing tier, offering enhanced data management, protection, and security capabilities.

Reference:

Nutanix Licensing Guide

Nutanix Cloud Clusters on AWS Administration Guide

Nutanix Best Practices for Advanced Features

NEW QUESTION: 10

Which two statements are the most accurate regarding Cluster Protect? (Choose two.)

- A.** An AWS subnet can be shared by VMs, Prism Central, and Multicloud Snapshot Technology (MST).
- B.** Nutanix Guest Tools (NGT) is not required to be installed on User VMs.
- C.** The clusters that are to be protected must be registered with the same instance of Prism Central.
- D.** The Cluster Protect feature requires AOS version 6.7 or higher.

Answer: C,D (LEAVE A REPLY)

The clusters that are to be protected must be registered with the same instance of Prism Central (Answer C):

For Cluster Protect to function correctly, all clusters intended for protection must be registered under the same Prism Central instance. This ensures consistent management and coordination of protection policies and operations across clusters.

The Cluster Protect feature requires AOS version 6.7 or higher (Answer D):

Cluster Protect is a feature that is available starting from AOS version 6.7. To utilize this feature, ensure that the Nutanix clusters are running this version or a newer one.

Reference:

Nutanix Cluster Protection Documentation

Nutanix AOS Release Notes

NEW QUESTION: 11

Exhibit.

What does the exhibit indicate?

- A.** No ongoing replication
- B.** Ongoing replication
- C.** Replication in paused state
- D.** Replication in error state

Answer: (SHOW ANSWER)

The exhibit indicates a replication operation with specific details about the protection domain, remote site, and snapshot. Key points to note are:

Bytes Completed: 0 bytes completed.

Complete Percent: 0.0%

Paused: false

Aborted: false

Given these details:

No ongoing replication: The operation has started, but there is no progress in terms of bytes completed or percentage completed. Since the status shows 0 bytes and 0 percent completed, it indicates that no data has been replicated yet.

Reference:

Nutanix Protection Domain and Replication Documentation

Nutanix Best Practices for Monitoring Replication

NEW QUESTION: 12

An administrator is seeking help with an ongoing NC2 issue. After reaching out to Nutanix support, the administrator is introduced to NC2 specialist who can help troubleshoot the problem.

- A. Ensure the specialist is assigned the RBAC role with proper permissions.
- B. Add the specialist as an admin user to the organizations.
- C. Confirm the Support Authorization on the organization is set to Full Access.
- D. Provide the specialist with the administrator's login credentials.

Answer: A,C ([LEAVE A REPLY](#))

Ensure the specialist is assigned the RBAC role with proper permissions (Answer A):

Role-Based Access Control (RBAC) ensures that the specialist has the necessary permissions to troubleshoot and manage the NC2 environment. This avoids unnecessary privilege escalations and maintains security.

Confirm the Support Authorization on the organization is set to Full Access (Answer C):

Setting the Support Authorization to Full Access allows the Nutanix support specialist to have the required access to investigate and resolve issues in the environment. This is essential for effective troubleshooting.

Reference:

Nutanix RBAC Documentation

Nutanix Support Access Guide

NEW QUESTION: 13

An administrator is deploying a new NC2 cluster on AWS and needs to ensure full connectivity is established between the company's on-premises datacenter and the AWS cloud.

Which two AWS offering will satisfy this requirement? (Choose two.)

- A. ExpressRoute
- B. AWS VPN
- C. Direct Connect
- D. Dedicated interconnect

Answer: B,C ([LEAVE A REPLY](#))

To establish full connectivity between the company's on-premises datacenter and the AWS cloud, the following AWS offerings will satisfy this requirement:

AWS VPN: This service allows you to create a secure connection between your on-premises network or other remote network and your AWS VPC using an IPsec VPN tunnel. It is suitable for low to moderate bandwidth requirements and provides secure, encrypted connections.

Direct Connect: AWS Direct Connect is a dedicated network connection from your premises to AWS. It provides a private, high-bandwidth, low-latency connection which is ideal for high-throughput applications and workloads that need consistent network performance.

Reference:

[AWS VPN Documentation](#)

[AWS Direct Connect Documentation](#)

NEW QUESTION: 14

In which two ways should an NC2 on AWS cluster be hibernated manually? (Choose two.)

- A.** Log into Prism Element navigate to Settings and select Hibernate/Resume.
- B.** Select the cluster under NC2 console and Select Hibernate/Resume on the cluster sur page.
- C.** Log into Prism, Central, navigate to Planning, find hibernate and resume.
- D.** Log into NC2 console, find the cluster name and select Hibernate/Resume from the ellipses.

Answer: B,D ([LEAVE A REPLY](#))

NEW QUESTION: 15

An administrator is tasked with providing VMs outbound internet connectivity in AWS.

Which components would the administrator need to create in the VPC to achieve this?

- A.** Public Subnet NAT Gateway, Public EIP, Route Table
- B.** Private Subnet NAT Gateway, Public EIP, Route Table
- C.** Private Subnet Flow Gateway, Public EIP, Route Table
- D.** Public Subnet Flow Gateway, Public EIP, Route Table

Answer: B ([LEAVE A REPLY](#))

To provide VMs with outbound internet connectivity in AWS using a private subnet, the administrator needs to create the following components in the VPC:

Private Subnet: A private subnet is required to house the VMs that need outbound internet access but do not require direct inbound access from the internet.

NAT Gateway: A NAT (Network Address Translation) Gateway is necessary to allow instances in the private subnet to connect to the internet or other AWS services while preventing the internet from initiating a connection with those instances.

Public EIP (Elastic IP Address): An EIP is associated with the NAT Gateway to provide a persistent public IP address that allows outbound internet traffic from the private subnet to be routed correctly.

Route Table: A route table is configured to route traffic from the private subnet to the NAT Gateway for outbound internet access.

Reference:

[AWS NAT Gateway Documentation](#)

[AWS VPC Subnet Basics](#)

NEW QUESTION: 16

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 (LEAVE A REPLY)

After the NC2 free trial expires, to continue using all features of NC2 on existing clusters, the administrator needs to switch to a paid subscription plan.

A paid subscription ensures uninterrupted access to the full range of features and support for NC2 clusters.

Without switching to a paid plan, the features might be limited, and support may not be available, impacting the cluster's operations and management.

Reference:

Refer to the Nutanix billing and subscription documentation for details on switching from a trial to a paid plan and the benefits associated with paid subscriptions.

Valid NCP-CI-AWS Dumps shared by Actual4test.com for Helping Passing NCP-CI-AWS Exam! Actual4test.com now offer the **newest NCP-CI-AWS exam dumps**, the Actual4test.com NCP-CI-AWS exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com NCP-CI-AWS dumps with Test Engine here: https://www.actual4test.com/NCP-CI-AWS_examcollection.html (77 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 17

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

- 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: (SHOW ANSWER)

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.

NEW QUESTION: 18

An administrator has been tasked with deploying an NC2 cluster on AWS with the requirement to protect workloads. Which two options are valid to protect the workloads on this cluster? (Choose two.)

- A. Deploy one-node cluster in another availability zone.
- B. Create a second NC2 cluster in a different availability zone.
- C. Use an existing on-prem Nutanix cluster as a disaster recovery target.
- D. Deploy a cluster across two availability zones.

Answer: B (LEAVE A REPLY)

To protect workloads on an NC2 cluster on AWS, deploying strategies that ensure high availability and disaster recovery are essential. The two valid options are:

Create a Second NC2 Cluster in a Different Availability Zone:

High Availability: Deploying a second NC2 cluster in a different availability zone ensures that workloads can be quickly recovered in case of an availability zone failure.

Disaster Recovery: This setup enables asynchronous replication between clusters, providing a robust disaster recovery solution.

Use an Existing On-Prem Nutanix Cluster as a Disaster Recovery Target:

Hybrid DR: Leveraging an existing on-premises Nutanix cluster for disaster recovery provides a cost-effective and efficient DR solution.

Replication: Set up replication policies to ensure data is consistently copied from the NC2 cluster on AWS to the on-premises cluster.

Why Not Other Options:

One-node cluster in another availability zone: Not a valid DR solution as a single-node cluster cannot provide the required resilience and high availability.

Deploy a cluster across two availability zones: While this can enhance availability, it is not a typical approach for Nutanix clusters which are designed to operate within a single availability zone for simplicity and performance reasons.

Reference:

Nutanix Cloud Clusters on AWS Administration Guide

Nutanix Disaster Recovery Best Practices

AWS Availability Zones and Disaster Recovery Documentation

NEW QUESTION: 19

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?

- 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: ([SHOW ANSWER](#))

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.

NEW QUESTION: 20

Which NC2 user role will allow full access to clusters created within an organization?

- A.** Cluster Super Admin
- B.** Organization Administrator
- C.** Organization Security Administrator
- D.** Cluster Administrator

Answer: **B** ([LEAVE A REPLY](#))

In Nutanix Cloud Integration with AWS, specifically version 6.7, the role that allows full access to clusters created within an organization is the Organization Administrator.

The Organization Administrator role has the highest level of privileges within an organization, enabling the user to manage all aspects of the clusters, including creation, modification, and deletion.

This role is designed to oversee and control the entire organization's resources, ensuring comprehensive management capabilities over all clusters and associated resources.

Reference:

Refer to the Nutanix documentation on roles and permissions for NC2 on AWS for further details.

NEW QUESTION: 21

An administrator is tasked with deploying a VM in an NC2 cluster on AWS that needs to be 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?

- 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 (LEAVE A REPLY)

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.

NEW QUESTION: 22

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:

Reference:

Nutanix Documentation on Cluster Protect and Recovery Processes

Nutanix Support & Insights

Nutanix Cloud Clusters on AWS Administration

NEW QUESTION: 23

An administrator has recently deployed an NC2 on AWS cluster in the North Virginia region in availability zone us-east-1z. The clusters UUID is 0005F487-4962-91EA-4C98-C4284D123835. The cluster is consuming IPs from a 10.78.2.0/24 range.

The AWS VPC has these available CIDR ranges:

* 70.73.0.0/16

* 10.79.107.0/24

* 10.0.0.0/22

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

The following tags have been applied to a Custom Network Security Group:

The Custom Network Security Group is allowing all inbound traffic from the 10.0.0.0/22 network.

Which two subnets would be able to receive inbound traffic from AWS instances on a 10.0.0.0/22 network segment"? (Choose two.)

A. Server01

B. Tier01

C. SQL

D. VDI

Answer: A,B (LEAVE A REPLY)

To determine which subnets would be able to receive inbound traffic from AWS instances on a 10.0.0.0/22 network segment, we need to look at the configured subnets and their CIDR ranges, as well as the custom network security group's inbound rules.

Available CIDR ranges in VPC:

70.73.0.0/16

10.79.107.0/24

10.0.0.0/22

Configured Subnets in NC2 AWS VPC:

VDI: 10.78.130.0/22

SQL: 10.78.3.0/24

Server01: 10.78.2.0/24

Server02: 10.79.120.0/24

Tier01: 10.19.101.0/24

Custom Network Security Group Inbound Rule:

Allows all inbound traffic from 10.0.0.0/22.

Given that the custom network security group is allowing inbound traffic from the 10.0.0.0/22 network, we need to identify which of the configured subnets fall within this allowed range.

Analysis:

The subnets 10.78.130.0/22, 10.78.3.0/24, 10.78.2.0/24, 10.79.120.0/24, and 10.19.101.0/24 do not overlap with 10.0.0.0/22. Therefore, none of these subnets would naturally fall within the 10.0.0.0/22 range directly.

However, since the question is about receiving inbound traffic from the 10.0.0.0/22 network and considering security group rules, all subnets mentioned can technically receive traffic if the

inbound rules are configured correctly, but since we are strictly asked about the configuration from the image and the overlap in the ranges:

Server01 (10.78.2.0/24) and Tier01 (10.19.101.0/24) will receive traffic because their CIDR ranges do not conflict with the 10.0.0.0/22 range, thus allowing traffic without additional restrictions.

Reference:

Nutanix Clusters on AWS Administration Guide

AWS VPC and Subnet documentation

Network Security Group rules configuration in Nutanix documentation

NEW QUESTION: 24

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?

- A. Configure RBAC roles on the Finance NC2 organization to allow access to regions.
- B. Configure IAM permission in cloud accounts to restrict access to certain regions.
- C. Open a support ticket with Nutanix to whitelist the allowed regions for the Finance NC2 organization.
- D. Specify allowed regions when configuring a cloud account for the Finance NC2 organization.

Answer: D ([LEAVE A REPLY](#))

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.

Reference:

Refer to the Nutanix documentation on NC2 cloud account configuration and region restrictions.

NEW QUESTION: 25

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 gain access to the NC2 console?

- 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 ([LEAVE A REPLY](#))

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.

NEW QUESTION: 26

Which two options are prerequisites for deploying an NC2 on AWS cluster? (Choose two.)

- A.** AWS Direct Connect
- B.** A valid CIDR range
- C.** A my.nutanix.com account
- D.** An on-premises Prism Central environment

Answer: B,C ([LEAVE A REPLY](#))

A valid CIDR range: A CIDR (Classless Inter-Domain Routing) range is necessary for creating the subnets within the VPC. This range defines the IP address space for the cluster and its components.

A my.nutanix.com account: This account is required to access Nutanix services, including the NC2 console, manage licenses, and perform other administrative tasks.

AWS Direct Connect and an on-premises Prism Central environment are not prerequisites for deploying an NC2 on AWS cluster. While Direct Connect can be used for enhanced network performance and connectivity, it is not a requirement for deployment. Similarly, having an on-premises Prism Central environment is not mandatory for NC2 deployment on AWS.

Reference:

Refer to the Nutanix documentation on NC2 prerequisites and setup guides, and AWS documentation on VPC and subnet creation.

NEW QUESTION: 27

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.** Contact Nutanix support to redeploy the cluster.
- C.** Nothing. The clusters will have full feature support.
- D.** Contact the AWS cloud vendor.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 28

A company has a large scale AWS deployment and has just finished installing their first NC2 on AWS cluster. The new cluster is now running workloads in production.

The cluster is configured with:

- * 16 Nodes
- * 8 Subnets
- * 200 User VMs per subnet
- * Nutanix Files

An administrator has been tasked with installing an EC2 instance on one of the subnets that is also used by the Nutanix, When the EC2 instance is powered on, an IP conflict occurs.

What action should the administrator take to resolve this issue?

- A.** The IP address used by the NC2 VM should be blocked /excluded from EC2.
- B.** The Instance Metadata of the NC2 instance needs to have the address reserved.
- C.** Assign an elastic IP to the EC2 instance and reboot.
- D.** The IP address used by the EC2 instance should be blocked / excluded from IPAM.

Answer: A (LEAVE A REPLY)

To resolve the IP conflict issue when an EC2 instance is powered on in a subnet also used by Nutanix NC2, the administrator should block or exclude the IP address used by the NC2 VM from being assigned to EC2 instances. This can be done by configuring the IP address management (IPAM) settings to ensure that the specific IP addresses allocated to the NC2 VMs are not used by EC2 instances, preventing IP conflicts and ensuring smooth operation of both environments.

Reference:

Nutanix Cloud Clusters on AWS Deployment Guide

Nutanix Support & Insights

Valid NCP-CI-AWS Dumps shared by Actual4test.com for Helping Passing NCP-CI-AWS Exam! Actual4test.com now offer the **newest NCP-CI-AWS exam dumps**, the Actual4test.com NCP-CI-AWS exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com NCP-CI-AWS dumps with Test Engine here: https://www.actual4test.com/NCP-CI-AWS_examcollection.html (77 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)