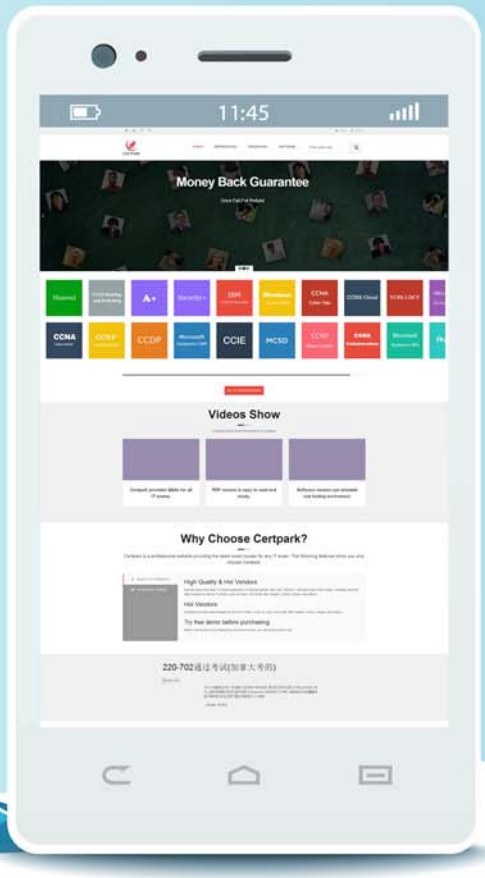
CERTPARK

QUESTION & ANSWER

CERTPARK.COM

Accurate Study Guides,
High Passing Rate!
provides update
free of charge
in one year!



https://www.certpark.com

Exam : **NCP-CI-AWS**

Title : Nutanix Certified Professional - Cloud Integration - AWS v6.7

Version : DEMO

1.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:

Subnet Name	IPv4/CIDR	Availability Zone
VDI	10.78.130.0/22	us-east-1z
SQL	10.78.3.0/24	us-east-1a
Server01	10.78.2.0/24	us-east-1z
Server02	10.79.120.0/24	us-east-1z
Tier01	10.19.101.0/24	us-east-1a

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: AB
Explanation:
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

2.preparing the landing zone networking resources for a Nutanix cluster on AWS. The administrator has created a VPC with two private subnets: one for cluster management and one for user VMs.
What additional subnet must the administrator create?
A. Public subnet for S3 access
B. Public subnet for Internet access
C. Private subnet for VPN gateway
D. Private subnet for Prism Central
Answer: B
Explanation:
When setting up a landing zone for Nutanix clusters on AWS, having only private subnets for cluster management and user VMs is not sufficient for full cluster functionality. Nutanix clusters often need to communicate with the internet for updates, patches, and other cloud services. VPC Configuration:
The VPC already has two private subnets (one for cluster management and one for user VMs).
Additional Requirements:
To access public services like S3 or for the cluster nodes to reach Nutanix services for updates, a public subnet is essential.
Why Public Subnet for Internet Access?:
A public subnet allows resources within it to communicate directly with the internet, which is necessary for accessing Nutanix's update servers, applying patches, and other maintenance tasks.
This subnet typically includes an internet gateway, enabling instances in the public subnet to receive and send traffic directly to the internet.
Reference: Nutanix Cloud Clusters on AWS Administration Guide
AWS Networking Best Practices
Nutanix Networking and Subnet Configuration Guidelines

3.An organization wants to control network traffic at the individual User VM (UVM) subnet level.
Which action will help achieve this goal?

A. Create a custom security group.
B. Modify the default UVM security group.
C. Modify the user management security group.
D. Modify the internal management security group.
Answer: A
Explanation:
To control network traffic at the individual User VM (UVM) subnet level, creating a custom security group is the appropriate action. This approach allows for fine-grained control over inbound and outbound traffic rules that can be applied to specific subnets or individual instances within those subnets.
Custom Security Group:
Custom security groups enable administrators to define specific traffic rules tailored to the needs of individual subnets or VMs. This includes specifying allowed IP ranges, ports, and protocols.
By applying these custom security groups to the UVMs, the organization can control access and enhance security according to their policies and requirements. Steps to Create a Custom Security Group:
Navigate to the AWS Management Console and go to the VPC service.
Select "Security Groups" under the "Security" section.
Click on "Create Security Group" and define the name, description, and VPC. Add inbound and outbound rules according to the desired traffic control policies. Attach the custom security group to the UVMs or subnets in question.
Reference: Nutanix Cloud Clusters on AWS Administration Guide
AWS Security Group Documentation
Nutanix Best Practices for Security Groups

4.When configuring an alert email in Prism Central deployed within an NC2 environment, what is required in order for the emails to be sent properly?
A. SMTP server configured in Prism Central settings
B. Cluster Super Admin permissions
C. Name servers configured in Prism Central
D. A whitelisted public cloud console endpoint
Answer: A
Explanation:
To ensure that alert emails are sent properly from Prism Central within an NC2 environment, configuring an SMTP server in the Prism Central settings is required. The SMTP server facilitates the sending of email notifications for alerts and other communications.
SMTP Configuration:
Prism Central requires an SMTP server to send email alerts. This involves specifying the SMTP server address, port, and authentication details if needed.
The configuration must include the email address from which the alerts will be sent and the recipient addresses.
Steps to Configure SMTP Server in Prism Central:
Log in to Prism Central.
Navigate to the "Settings" menu.
Select "Email Server" under the "Alerts" section.

Enter the SMTP server details, including the server address, port, and authentication credentials.
Test the configuration to ensure emails are sent correctly.
Reference: Nutanix Prism Central Administration Guide
Nutanix Support Documentation on Email Alert Configuration Best Practices for Configuring SMTP Servers in Cloud Environments

5.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
Explanation:
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