

Nutanix.NCP-CI-AWS.by.Gano.55q

Number: NCP-CI-AWS
Passing Score: 800
Time Limit: 120
File Version: 5.0

Exam Code: NCP-CI-AWS

Exam Name: Nutanix Certified Professional - Cloud Integration - AWS V6.7



Exam A

QUESTION 1

An administrator has been tasked with performing a test migrating from an NC2 environment to a Nutanix on-premises environment.

Where should the administrator perform this task?

- A. NC2 Prism Element
- B. NC2 Prism Central
- C. Nutanix Cloud Services Portal
- D. On-premises Prism Central

Correct Answer: B

Section:

Explanation:

When performing a migration from an NC2 environment to a Nutanix on-premises environment, the task should be performed using the NC2 Prism Central. This is because NC2 Prism Central provides a centralized management interface that allows administrators to manage and migrate workloads between cloud and on-premises environments seamlessly.

Nutanix Cloud Clusters (NC2) Documentation

Nutanix Community Guide

QUESTION 2

An administrator is attempting to deploy an NC2 cluster.

The cluster configuration is as follows:

- * Name - Cluster-1
- * Nodes of type i4i.metal
- * Replication Factor 2
- * Existing VPC resources
- * VPC - 10.0.0.0/16
- * Subnets:
 - * Bare metal hosts: 10.0.1.0/24
 - * User VMs:10.0.2.0/24
 - * Public: 10.0.3.0/24

During the deployment process, the administrator notices the following alert:

```
System detected possible problems with Cluster Cluster-1 VPC/Subnet settings. Cluster nodes might not be able to contact Nutanix services
```

What should the administrator do to ensure the cluster deployment does not fail?

- A. Create a new VPC and modify the cluster configuration to use the new VPC.
- B. Check AWS VPC and subnet quotas for the cloud account.
- C. Ensure an outbound Internet connection exists from 10.0.1.0/24.
- D. Modify the administrator's RBAC permissions in the NC2 console.

Correct Answer: C

Section:

Explanation:



The alert indicates a potential issue with the VPC/Subnet settings, preventing the cluster nodes from contacting Nutanix services. To resolve this, the administrator needs to ensure that the subnet 10.0.1.0/24, which is assigned for Bare metal hosts, has an outbound Internet connection. This connection is necessary for the cluster nodes to communicate with external Nutanix services for updates, license validation, and other essential operations. Verify that there are appropriate route tables and security group rules allowing outbound traffic to the Internet from the 10.0.1.0/24 subnet. Ensure that there is either an Internet Gateway (IGW) attached to the VPC or a NAT Gateway configured if using private subnets. Reference: Refer to the Nutanix documentation and AWS VPC configuration guides to ensure proper Internet connectivity and routing setups.

QUESTION 3

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

Correct Answer: A

Section:

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 4

Which two features or services can an administrator ensure are protected by cluster protect within an NC2 environment? (Choose two.)

- A. Flow Network Security
- B. VM Templates
- C. Nutanix Files
- D. Virtual Machine Disks

Correct Answer: C, D

Section:

Explanation:

Within an NC2 environment, the Cluster Protect feature can ensure the protection of:

Nutanix Files: This provides file services within the Nutanix ecosystem, and Cluster Protect can safeguard the data stored in Nutanix Files.

Virtual Machine Disks: This ensures that the data stored on virtual machine disks is protected, providing backup and recovery options for the virtual machines running within the cluster.

Nutanix Cloud Clusters on AWS Administration

Nutanix AOS 6.7 Documentation

QUESTION 5

An administrator is planning a new NC2 on AWS deployment. The workload VMs to be deployed on the new cluster have low storage and memory, but high CPU frequency (>3.0 GHz) requirements. The administrator has also been tasked with ensuring that the cluster nodes have the lowest number of CPU cores to reduce application licensing requirements. Which node type will satisfy this new deployment?

- A. i3.metal
- B. z1d.metal
- C. i4i.metal
- D. m5d.metal

Correct Answer: A

Section:

Explanation:

For a new NC2 on AWS deployment where workload VMs have low storage and memory requirements but high CPU frequency (>3.0 GHz) requirements, and the goal is to minimize the number of CPU cores to reduce application licensing costs, the i3.metal instance type is the most suitable.

i3.metal:

High CPU Frequency: i3.metal instances offer high-frequency Intel Xeon processors (up to 3.1 GHz) which meet the high CPU frequency requirement.

Low Storage and Memory: These instances come with a balanced amount of storage and memory, suitable for workloads with low requirements in these areas.

Minimized CPU Cores: i3.metal instances have fewer CPU cores compared to other high-frequency instances like i4i.metal, making them ideal for minimizing application licensing costs.

Other Instance Types:

z1d.metal: While also offering high CPU frequency, these instances typically come with a higher core count and more memory, which may not be optimal for minimizing licensing costs.

i4i.metal: Designed for I/O intensive applications with higher core counts.

m5d.metal: Balanced instance type but with more cores and not as high CPU frequency as required.

[AWS EC2 Instance Types Documentation](#)

[Nutanix Cloud Clusters on AWS Administration Guide](#)

[Nutanix Best Practices for Instance Selection](#)

QUESTION 6

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.

Correct Answer: D

Section:

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.

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

QUESTION 7

Which interface must be used to deploy NC2?

- A. Cloud Provider portal
- B. NC2 Tile within the my.nutanix.com portal
- C. Prism Central Dashboard
- D. Foundation running in a Cloud Virtual Machine

Correct Answer: B

Section:**Explanation:**

The NC2 Tile within the my.nutanix.com portal is the correct interface to deploy NC2. This portal provides an integrated and user-friendly interface specifically designed for deploying and managing Nutanix Clusters on AWS. NC2 Deployment Interface:

NC2 Tile within the my.nutanix.com portal: This portal provides the necessary tools and options to deploy and manage NC2 clusters. It includes functionalities for setting up the clusters, configuring network settings, and managing resources.

Advantages:

User-Friendly Interface: Simplifies the deployment process with a guided setup.

Integrated Tools: Provides access to all necessary tools for managing the deployment and monitoring of NC2 clusters.

Nutanix Cloud Clusters on AWS Administration Guide

Nutanix my.nutanix.com Portal Documentation

Nutanix Best Practices for Cluster Deployment

QUESTION 8

Which entity should be contacted for AOS software supported related to NC2?

- A. Internal IT Operations team
- B. Nutanix
- C. Partner
- D. Public Cloud Vendor

Correct Answer: B

Section:**Explanation:**

For AOS software support related to NC2, the appropriate entity to contact is Nutanix. Nutanix provides comprehensive support for their software, including the Acropolis Operating System (AOS) used in NC2 deployments. Support Scope:

Nutanix offers support for the deployment, configuration, and management of NC2 clusters, including any issues related to AOS software.

This includes troubleshooting, updates, and technical assistance.

Why Not Other Options:

Internal IT Operations team: Typically handles internal issues but does not have the specialized knowledge or resources for AOS software support.

Partner: May provide support but would ultimately escalate issues to Nutanix for software-specific concerns.

Public Cloud Vendor: Manages infrastructure-related issues but does not provide support for Nutanix AOS software.

Nutanix Support Documentation

Nutanix Cloud Clusters on AWS Administration Guide

Nutanix Best Practices for AOS Support

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

Correct Answer: D

Section:**Explanation:**

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.

Nutanix Licensing Guide

Nutanix Cloud Clusters on AWS Administration Guide

Nutanix Best Practices for Advanced Features

QUESTION 10

What is an available log module when configuring a syslog server in the Prism Central Admin Center?

- A. API Audit
- B. Prism
- C. Zookeeper
- D. Acropolis

Correct Answer: D

Section:

Explanation:

When configuring a syslog server in the Prism Central Admin Center for Nutanix, one of the available log modules is Acropolis.

The Acropolis module logs system events related to the Nutanix Acropolis operating system, which is critical for monitoring and auditing system activities and performance.

Configuring syslog with the Acropolis module ensures that important events and issues related to the Acropolis environment are captured and can be forwarded to an external syslog server for centralized logging and analysis.

Reference: Refer to the Nutanix documentation on Prism Central and syslog configuration for the full list of available log modules and detailed steps for configuration.

QUESTION 11

What role is needed to create a cluster?

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

Correct Answer: C

Section:

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.

QUESTION 12

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.

Correct Answer: A

Section:

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.

Nutanix Cloud Clusters on AWS Administration Guide

AWS Security Group Documentation

Nutanix Best Practices for Security Groups

QUESTION 13

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

Correct Answer: A

Section:

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.

Nutanix Prism Central Administration Guide

Nutanix Support Documentation on Email Alert Configuration

Best Practices for Configuring SMTP Servers in Cloud Environments

QUESTION 14

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

Correct Answer: B

Section:

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.

Nutanix Cloud Clusters on AWS Administration Guide

AWS Security Group Documentation

Nutanix Best Practices for Secure Access



QUESTION 15

Which service enables the monitoring of key metrics on various AWS services, including EC2, EBS, and VPC for an NC2 cluster deployments?

- A. Amazon CloudWatch
- B. AWS CloudTrail
- C. AWS CloudFormation
- D. Amazon inspector

Correct Answer: A

Section:

Explanation:

Amazon CloudWatch is the service that enables the monitoring of key metrics on various AWS services, including EC2, EBS, and VPC, for NC2 cluster deployments.

Amazon CloudWatch:

Amazon CloudWatch provides monitoring for AWS cloud resources and applications. It collects and tracks metrics, collects and monitors log files, and sets alarms.

Specifically, for NC2 deployments, CloudWatch can be used to monitor key metrics such as CPU utilization, disk I/O, network I/O for EC2 instances, EBS volume performance, and VPC network traffic.

Features:

Metrics Monitoring: Collects and visualizes operational data in the form of metrics, including utilization, performance, and health.

Logs Monitoring: Collects log data, monitors it in real-time, and triggers alarms based on predefined thresholds.

Alarms: Notifies when operational performance thresholds are breached.

Integration with NC2:

By setting up CloudWatch, administrators can ensure they have visibility into the performance and health of their Nutanix clusters on AWS, aiding in proactive management and troubleshooting.

[Amazon CloudWatch Documentation](#)

[Nutanix Cloud Clusters on AWS Administration Guide](#)

[AWS Monitoring Best Practices](#)

QUESTION 16

An administrator needs the permissions to create and manage multiple organizations and clusters in NC2, as well as manage user access for the entire company.

What role should be assigned to meet the minimum requirements of this task?

- A. Organization Administrator
- B. Customer Administrator
- C. Customer Security Administrator
- D. Cluster Administrator

Correct Answer: B

Section:

Explanation:

The role of 'Customer Administrator' in Nutanix Cloud Integration with AWS (NC2) is designed to meet the requirements of creating and managing multiple organizations and clusters, as well as managing user access for the entire company.

Roles and Permissions:

Customer Administrator: This role has the broadest set of permissions, allowing the user to create and manage organizations, clusters, and user access across the entire company. It encompasses administrative control over multiple aspects of the NC2 environment.

Capabilities:

Organization Management: Ability to create and manage multiple organizations.

Cluster Management: Full control over creating, configuring, and managing clusters.

User Access Management: Manage user roles and permissions, ensuring that the right individuals have access to the necessary resources.

Why Not Other Roles:

Organization Administrator: Limited to managing organizations but not clusters and user access at the company level.

Customer Security Administrator: Focuses on security aspects, lacking broader administrative capabilities.

Cluster Administrator: Limited to managing clusters without the ability to manage organizations and user access comprehensively.

[Nutanix Cloud Clusters on AWS Administration Guide](#)

[Nutanix Role-Based Access Control Documentation](#)

QUESTION 17

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.

Correct Answer: D

Section:

Explanation:

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.

Nutanix Cloud Clusters on AWS Administration Guide

AWS VPC Subnet Creation Documentation

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 NCZ 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.

Correct Answer: B

Section:

Explanation:

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.

Nutanix Cloud Clusters on AWS Administration Guide

Nutanix Disaster Recovery Best Practices

AWS Availability Zones and Disaster Recovery Documentation

QUESTION 19

Exhibit.



Name	Cloud Provider	Cloud Account ID	Created On	Active	Status
D[REDACTED]	Azure	3c[REDACTED]	Apr 6th 2023 10:01 UTC	A	R
D[REDACTED]	AWS	3C[REDACTED]	Apr 6th 2023 09:56 UTC	A	U

An administrator is attempting, but failing to create an NC2 cluster in AWS. The administrator checks the configuration in the NC and notices the configuration shown in the exhibit. What action should the administrator take to resolve the issue?

- A. Recreate the AWS CloudFormation stack.
- B. Create a new cloud account in the organization.
- C. Restart Genesis on a Prism Central instance.
- D. Grant the administrator's account access to the NC2 organization.

Correct Answer: B

Section:

Explanation:

The exhibit shows two cloud accounts, one for Azure and one for AWS, with their statuses indicated. The AWS cloud account status is marked as 'U' (which likely stands for 'Unavailable' or 'Unreachable'). This indicates that the AWS cloud account configuration is not properly connected or accessible.

Status Check:

The AWS cloud account is marked with an 'U' status, meaning it is not active or accessible.

This status prevents the creation of an NC2 cluster because the necessary cloud resources cannot be allocated or managed without a proper connection.

Action:

The best course of action is to create a new cloud account in the organization. This involves setting up the cloud account details correctly and ensuring it is properly configured to communicate with Nutanix and AWS.

Steps to Create a New Cloud Account:

Log in to the Nutanix console.

Navigate to the 'Organizations' section.

Select 'Add Cloud Account' and provide the required AWS credentials and permissions.

Ensure the new cloud account is active and correctly configured.

[Nutanix Cloud Clusters on AWS Administration Guide](#)

[Nutanix Best Practices for Cloud Account Management](#)

QUESTION 20

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.

Correct Answer: C, D

Section:**Explanation:**

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.

[AWS VPC Peering Documentation](#)

[AWS Interface Endpoint Documentation](#)

[Nutanix Cloud Clusters on AWS Administration Guide](#)

QUESTION 21

An administrator is tasked with adding an AWS account to the NC2 console. A requirement is to configure an AWS IAM user with the appropriate permissions.

Which permission must be assigned to the user?

- A. IAMFullAccess
- B. IAMReadOnlyAccess
- C. AmazonEC2ReadOnlyAccess
- D. AmazonEC2FullAccess



Correct Answer: D

Section:**Explanation:**

To add an AWS account to the NC2 console, an AWS IAM user needs to be configured with the appropriate permissions to manage the EC2 resources. The required permission for the IAM user includes full access to manage EC2 instances, volumes, and related resources.

AmazonEC2FullAccess:

This permission grants full access to all EC2 resources, including the ability to create, modify, and delete instances, volumes, security groups, and more.

Essential for NC2 operations to manage the lifecycle of EC2 instances and associated components within the AWS environment.

Why Not Other Permissions:

IAMFullAccess: Grants full access to IAM resources but not specifically needed for EC2 operations.

IAMReadOnlyAccess: Only provides read access to IAM resources, insufficient for managing EC2 instances.

AmazonEC2ReadOnlyAccess: Provides read-only access to EC2 resources, insufficient for creating or modifying instances and other resources.

[AWS IAM Policies Documentation](#)

[Nutanix Cloud Clusters on AWS Administration Guide](#)

[Nutanix Best Practices for IAM User Permissions](#)

QUESTION 22

An administrator has created an NC2 cluster on AWS, but the NC2 console has issued this alert:


```
Cluster failed to create. Max retries for provisioning cluster nodes reached. Deleting cluster.
Refer to KB 9774 (https://portal.nutanix.com/kb/9774) to understand possible causes for the cluster
creation failures.
```

Which two scenarios could have resulted in the cluster creation failure? (Choose two.)

- A. Bad Terraform (TF) state in provisioning
- B. Insufficient permissions
- C. No available AWS credits
- D. AWS Quota exceeded/instance limit exceeded

Correct Answer: B, D

Section:

Explanation:

The error message in the image indicates that the cluster creation failed due to reaching the maximum retries for provisioning cluster nodes. Here are two possible scenarios that could lead to this issue:

Insufficient Permissions (Answer B):

If the AWS user or role used to create the cluster does not have sufficient permissions, it can result in failures during the provisioning process. Proper IAM policies must be attached to ensure that the necessary actions can be performed, such as launching instances, creating VPCs, or managing networking components.

AWS Quota Exceeded/Instance Limit Exceeded (Answer D):

AWS imposes quotas and limits on the number of instances and other resources that can be created within an account. If these quotas are exceeded, new instances cannot be provisioned, causing the cluster creation to fail.

This can be resolved by requesting a quota increase from AWS.

Nutanix Knowledge Base Article 9774

AWS Service Quotas

Nutanix NC2 on AWS Documentation



QUESTION 23

Administrator has recently deployed an NC2 cluster on AWS in the North Virginia region in availability zone us-east-1d. 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:

Subnet Name	IPv4/CIDR	Availability Zone
VDI	10.78.130.0/22	us-east-1d
SQL	10.78.3.0/24	us-east-1a
DR01	10.78.2.0/24	us-east-1d
DR02	10.79.120.0/24	us-east-1d
L2stretch	10.19.101.0/24	us-east-1a

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

Correct Answer: A, B

Section:

Explanation:

For the NC2 cluster deployed in the North Virginia region (us-east-id), consuming IPs from the 10.78.2.0/24 range, the subnets configured within the same CIDR range of 10.78.0.0/16 will be recognized.

The subnet DR01 (10.78.2.0/24) is directly within the range of the deployed cluster.

The subnet L2stretch (10.19.101.0/24) is also configured in the NC2 AWS VPC, although not in the immediate range of the cluster, it may show up due to broader network configurations for stretched L2 operations.

Subnets VDI (10.78.130.0/22) and DR02 (10.79.120.0/24), although part of the same VPC, are not directly within the immediate CIDR range or may not be recognized in this specific configuration scenario.

Reference: Refer to the Nutanix documentation on NC2 AWS VPC subnet configurations and Prism Element settings for detailed guidelines on network visibility and configuration.

QUESTION 24

An administrator has deployed an NC2 cluster in AWS.

The following configuration decisions were made:

Created a new VPC from the NC2 console as part of the deployment

Selected the Public option for prism access policy

Host type selected was i3en,metal

The administrator now has a goal of provision public internet access to a user VM (UVM),web-1, on the Nutanix cluster. The admin can access Prism Element via the public DNS of the Auto-created load balancer.

The administrator tries to create another network load balancer for the web server access. After creating the load balancer and registering web-1's IP address as a target, the administrator finds that the health check for the VM target is failing and the DNS returns as NOT Found message in the browser.

Why is the issue happening?

- A. The load balancer is still in a Provisioning state.
- B. The administrator has not modified the inbound rules under the UVM security group to allow the network load balancer to access the UVM subnet.
- C. The administrator has not assigned a public IP to web-1.
- D. The administrator needs to provision an application load balancer instead of a network load balancer to allow Internet traffic to access the UVM subnet.

Correct Answer: C

Section:

Explanation:

For a VM to be accessible over the internet through a load balancer, the VM itself must have a public IP address.

In this case, the health check for the VM target is failing and the DNS returns a 'NOT Found' message because web-1 does not have a public IP assigned.

Without a public IP, the load balancer cannot route traffic to web-1 from the internet.

Assigning a public IP to web-1 ensures that the VM can be accessed via the load balancer, resolving the connectivity issue.

Reference: Refer to the AWS documentation on network load balancers and public IP assignments, and Nutanix documentation on VM network configurations.

QUESTION 25

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

Correct Answer: B, C

Section:

Explanation:

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.

QUESTION 26

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. downloads.cloud.nutanix.com
- D. apikeys.nutanix.com

Correct Answer: B

Section:

Explanation:

When deploying a new NC2 cluster, the AWS Directory Service must be able to resolve the address gateway-external-api.cloud.nutanix.com.

This external API gateway is critical for the NC2 cluster to communicate with Nutanix services for operations such as management, updates, and licensing.

Ensuring that this address can be resolved allows the cluster to interact properly with the Nutanix cloud infrastructure and services.

Reference: Refer to the Nutanix documentation on network and DNS requirements for NC2 deployments, specifically the addresses that need to be resolvable for proper functionality.

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

Correct Answer: A

Section:

Explanation:

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.

QUESTION 28

How many Amazon Elastic Block Store(EBS) volumes are attached to each node within an AWS NC2 cluster upon creation.

- A. 1
- B. 2
- C. 3
- D. 4

Correct Answer: C

Section:

Explanation:

Upon creation, each node within an AWS NC2 cluster has 3 Amazon Elastic Block Store (EBS) volumes attached.

These volumes are used for different purposes, such as operating system storage, Nutanix services, and user data storage.

The number of EBS volumes is designed to ensure adequate storage performance and capacity for the NC2 cluster's operations and workload demands.

Reference: Refer to the Nutanix documentation on NC2 cluster setup and AWS EBS volume configurations to confirm the details on the number and purpose of EBS volumes attached to each node.

QUESTION 29

An administrator has deployed NC2 on AWS. The cluster deployment completed successfully.

After deployment, the administrator created a subnet in AWS, added it as a network in Prism Element, deployed Prism Central using the newly-configured network, and registered the cloud cluster with it.

The on-premises network and AWS are connected via a Site-to-Site VPN. Cluster nodes, CVM, and Prism Central can communicate with each other, but cannot be accessed from the on-premises network.

What two issues might be the cause of this problem? (Choose two.)

- A. AWS Direct Connect must be used to establish connection between AWS and on-premises
- B. Traffic from the on-premises network is not permitted by VM and Management security groups.
- C. The AHV firewall is blocking traffic from the on-premises network.
- D. The AWS VPC traffic is blocked by a firewall in the on-premises network.

Correct Answer: B, D

Section:

Explanation:

Traffic from the on-premises network is not permitted by VM and Management security groups:

Ensure that the security groups assigned to the VMs and management interfaces in AWS allow inbound traffic from the on-premises network. Without appropriate security group rules, the traffic will be blocked.

The AWS VPC traffic is blocked by a firewall in the on-premises network:

Check if the firewall on the on-premises network is configured to allow traffic from the AWS VPC. Firewalls may have restrictive rules that block incoming traffic, preventing communication.

Reference: Refer to AWS documentation on security groups and firewalls and Nutanix documentation on configuring networking for NC2 clusters.

QUESTION 30

An administrator is investigating reports of network congestion on their NC2 deployment.

As part of the investigation, a packet capture is taken from a group of user VMs. During the analysis of the packet capture, it is observed that user VMs are receiving multicast traffic unexpectedly.

What action should the administrator take to resolve the issue?

- A. Disable DHCP snooping on the upstream network
- B. Enable IGMP snooping on the AHV hosts
- C. Enable DHCP snooping on the upstream network
- D. Disable IGMP snooping on the AHV hosts

Correct Answer: B

Section:

Explanation:

Enable IGMP snooping on the AHV hosts:

IGMP (Internet Group Management Protocol) snooping is a feature that listens to IGMP traffic between hosts and routers. By enabling IGMP snooping on the AHV (Acropolis Hypervisor) hosts, the switch can intelligently forward multicast traffic only to the ports that have requested it.

This reduces unnecessary multicast traffic on the network and prevents congestion by ensuring that multicast packets are only delivered to the appropriate endpoints.

Reference: Refer to the Nutanix documentation on network configuration and best practices for managing multicast traffic.

QUESTION 31

An administrator is deploying an NC2 cluster into an existing AWS VPC.

The cluster deployment fails, with the following error message:

```
Failed to create network interface due to the following error: Must provide a security group when creating interfaces in a shared subnet
```

Why has the deployment failed?

- A. The administrator has not created the necessary Security Group.
- B. The administrator has not configured the Security Group to manage the shared subnet.
- C. Shared subnets are not supported for Nutanix clusters.
- D. Outbound Internet access is not configured on the VPC.

Correct Answer: A

Section:

Explanation:

The administrator has not created the necessary Security Group:

The error message indicates that the creation of network interfaces in a shared subnet requires specifying a security group. This means that the necessary security group has not been created or assigned to the network interfaces.

Creating the appropriate security group and ensuring it is associated with the network interfaces during cluster deployment should resolve this issue.

Reference: Refer to AWS documentation on security groups and network interface configuration and Nutanix documentation on prerequisites for deploying NC2 clusters in an existing AWS VPC.

QUESTION 32

An administrator is experiencing problems with several operations, including VM IP address assignment validations, VM power-on and VM power-off operations.

Whenever a related operation is performed, an alert is generated in the NC2 console indicating that the Cloud API endpoints are unavailable.

The issue was further investigated and it was determined that NC2 is unable to make API calls to the underlying cloud infrastructure due to network connectivity misconfigurations.

Which two connectivity misconfigurations could be causing this issue? (Choose two.)

- A. AWS VPC endpoints are used for connectivity to AWS services.
- B. Subnets are connected to the Internet via NAT gateways.
- C. Route tables for cloud subnets contain incorrect route entries.
- D. IAM roles and policies are incorrectly configured.

Correct Answer: C, D

Section:

Explanation:

Route tables for cloud subnets contain incorrect route entries:

If the route tables associated with the cloud subnets contain incorrect route entries, the NC2 cluster might not be able to reach the necessary AWS services or endpoints. Correct route entries are crucial for ensuring proper communication between the NC2 cluster and the underlying AWS infrastructure.

IAM roles and policies are incorrectly configured:

Incorrectly configured IAM roles and policies can prevent NC2 from making API calls to AWS services. These roles and policies must be properly set up to allow the necessary permissions for NC2 to interact with AWS resources and perform required operations.

Reference: Refer to the AWS documentation on route table configuration and IAM roles and policies, and Nutanix documentation on NC2 cloud connectivity and permissions.

QUESTION 33

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

Correct Answer: B

Section:

Explanation:

Gateway Endpoint:

A Gateway Endpoint in AWS allows you to connect to supported AWS services privately without going through the public internet. This setup provides secure and efficient connectivity directly from the corporate VPC to the required AWS services.

Gateway Endpoints support services such as Amazon S3 and DynamoDB and are ideal for scenarios where private connectivity to these services is needed.

Reference: Refer to the AWS documentation on VPC endpoints, specifically Gateway Endpoints, and the Nutanix documentation on configuring private connectivity for NC2 deployments.

QUESTION 34

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.delete_from_ip_blacklist 10.79.4.200 aCLI > net.delete_from_ip_blacklist 10.79.4.201
- D. Configure the AHV IPAM to use DHCP range 10.79.4.2 -10.79.4.253.

Correct Answer: A, D

Section:

Explanation:

To avoid IP address conflicts and ensure there are no configuration issues when reusing an existing AWS subnet, the administrator should take the following actions:

aCLI > net.add_to_ip_blacklist 10.79.4.200 aCLI > net.add_to_ip_blacklist 10.79.4.201 (Answer A):

This command adds the specified IP addresses to the blacklist, preventing AHV IPAM from assigning these addresses to any VMs. This ensures that the existing EC2 instances with IPs 10.79.4.200 and 10.79.4.201 are not allocated to other VMs in the NC2 cluster.

Configure the AHV IPAM to use DHCP range 10.79.4.2 -10.79.4.253 (Answer D):

By configuring the AHV IPAM to use a specific DHCP range, you ensure that the IP addresses assigned to the EC2 instances (10.79.4.200 and 10.79.4.201) are not included in the DHCP pool. This prevents IP address conflicts within the subnet.

Nutanix aCLI Reference

Nutanix NC2 on AWS Documentation

AWS VPC and Subnet Basics

QUESTION 35

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.

Correct Answer: C, D

Section:



Explanation:

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):

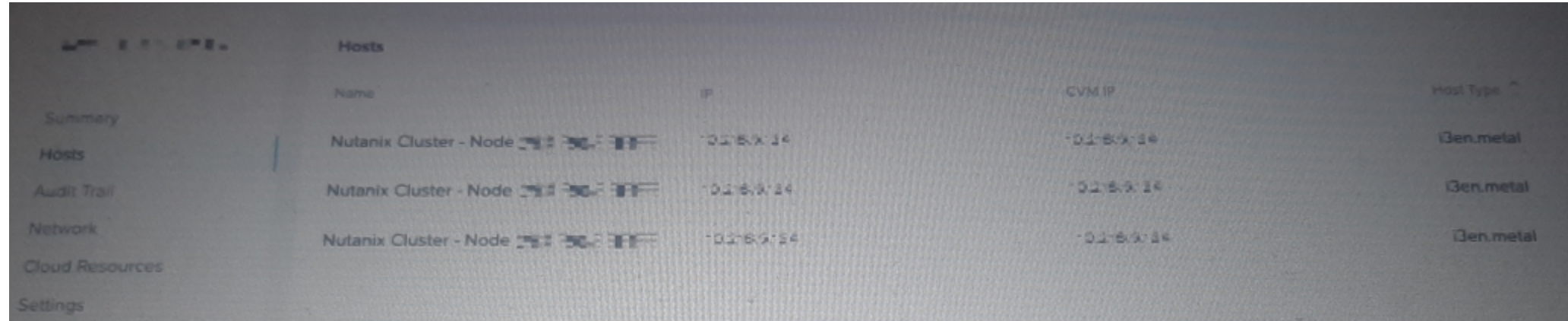
Cluster Protect is a feature that is available starting from AOS version 6.7. To utilize this feature, ensure that the Nutanix clusters are running this version or a newer one.

Nutanix Cluster Protection Documentation

Nutanix AOS Release Notes

QUESTION 36

Exhibit.



	Name	IP	CVM IP	Host Type
Summary				
Hosts	Nutanix Cluster - Node [Status]	10.10.10.10	10.10.10.10	Gen.metal
Audit Trail	Nutanix Cluster - Node [Status]	10.10.10.10	10.10.10.10	Gen.metal
Network	Nutanix Cluster - Node [Status]	10.10.10.10	10.10.10.10	Gen.metal
Cloud Resources				
Settings				

What action is taken against the Condemned node shown in the exhibit?

- A. The node has a power reset sent to it.
- B. The node is restarted.
- C. The node is powered off.
- D. The node is automatically replaced.



Correct Answer: A

Section:

Explanation:

When a node is marked as 'Condemned,' it indicates that the system has determined that the node is no longer reliable for operations. As part of the automated recovery and protection process, the following action is typically taken:

The node has a power reset sent to it (Answer A):

In most cases, a condemned node undergoes a power reset as an initial recovery attempt. This action attempts to reboot the node to bring it back to a healthy state. If the reset fails, further manual or automated steps may be required to address the hardware or software issue.

Nutanix Cluster Management Documentation

Nutanix Support Knowledge Base

QUESTION 37

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

Correct Answer: B

Section:

Explanation:

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.

[AWS NAT Gateway Documentation](#)

[AWS VPC Subnet Basics](#)

QUESTION 38

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

Correct Answer: B

Section:

Explanation:

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.

[Nutanix Prism Central Documentation](#)

[Nutanix pcdr-cli Command Reference](#)

QUESTION 39

An administrator has been tasked with deploying a new production NC2 cluster on AWS and is studying the deployment..

AWS supports EC2 bare-metal instances in regions with at least how many partitions?

- A. 1
- B. 3
- C. 5
- D. 6

Correct Answer: B

Section:

Explanation:

AWS supports EC2 bare-metal instances in regions with at least 3 partitions. Partitions in AWS provide high availability and fault tolerance by distributing instances across different hardware to minimize the impact of hardware failures.

[AWS EC2 Bare Metal Instances Documentation](#)

[AWS Regions and Availability Zones](#)

QUESTION 40

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.

Correct Answer: A, C

Section:

Explanation:

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.

[Nutanix RBAC Documentation](#)

[Nutanix Support Access Guide](#)

QUESTION 41

A company needs to create virtual interfaces directly to public AWS S3 services. The company also wants to bypass any internet service providers in the network path.

Which method will best satisfy this requirement?

- A. VPN
- B. Bastion Host
- C. SSH
- D. Direct Connect

Correct Answer: D

Section:

Explanation:

AWS Direct Connect allows companies to create private, dedicated connections between their data centers and AWS. This bypasses the internet and provides a more reliable and faster network connection directly to AWS services, including S3.

[AWS Direct Connect Documentation](#)

[AWS S3 Access over Direct Connect](#)

QUESTION 42

Regarding a cloud cluster, which two upgrades can be performed using LCM? (Choose two.)

- A. AHV
- B. NBA
- C. BIOS
- D. NCC

Correct Answer: A, C

Section:

Explanation:

AHV (Answer A):

AHV (Acropolis Hypervisor) can be upgraded using Lifecycle Manager (LCM). LCM simplifies the upgrade process and ensures that all components are updated in a coordinated manner.

BIOS (Answer C):

BIOS upgrades can also be performed using LCM. This helps in maintaining hardware compatibility and performance by ensuring that the latest firmware is installed.

[Nutanix Lifecycle Manager \(LCM\) Documentation](#)



QUESTION 43

If an administrator deploys an NC2 cluster using an existing AWS network, in which type of subnet should the administrator deploy the NAT Gateway?

- A. Isolated subnet
- B. Private subnet
- C. VPN-only subnet
- D. Public subnet

Correct Answer: D

Section:

Explanation:

To deploy an NC2 cluster using an existing AWS network, the NAT Gateway should be placed in a public subnet. A public subnet is one that has a route to an Internet Gateway, allowing the NAT Gateway to provide outbound internet access for resources in private subnets. The NAT Gateway is used to enable instances in private subnets to access the internet while keeping them secure by not exposing them directly to the public internet.

Nutanix Cloud Clusters (NC2) on AWS Documentation

QUESTION 44

A company wants to use Nutanix NC2 to burst VDI resources to the AWS cloud. The VDI workloads requires GPU accelation.

Which solution meets the company's requirements?

- A. AN36P nodes
- B. m6g.metal nodes
- C. g4dn.metal nodes
- D. AN36 nodes



Correct Answer: C

Section:

Explanation:

For VDI workloads that require GPU acceleration, the g4dn.metal nodes are the appropriate choice. These instances are equipped with NVIDIA T4 GPUs, which are well-suited for graphics-intensive applications such as VDI workloads that need GPU acceleration. Other node types like AN36P, m6g.metal, or AN36 do not provide the necessary GPU capabilities.

Nutanix Support & Insights - GPU support in AWS

QUESTION 45

An organization plans to use the Cluster Protect feature to protect the cluster data.

Which license will satisfy this requirement?

- A. AOS Ultimate or NCI Ultimate
- B. AOS Pro or AOS Ultimate
- C. AOS Pro or NCI Pro
- D. NCI Pro or AOS Ultimate

Correct Answer: A

Section:

Explanation:

The Cluster Protect feature, which provides data protection and disaster recovery capabilities for Nutanix clusters, requires either the AOS Ultimate or NCI Ultimate license. These licenses include the necessary features to leverage Cluster Protect for ensuring data resilience and recovery.

QUESTION 46

An administrator planned to create a new NC2 cluster and chose the existing AWS VPC infrastructure in the workflow. The administrator needs two private subnets to complete the configuration.

- A. For user VMs and cluster management
- B. For Prism Element and Prism Central management
- C. For DNS and NJP management
- D. For private NAT and Elastic IP management

Correct Answer: A

Section:

Explanation:

When creating a new NC2 cluster using an existing AWS VPC infrastructure, two private subnets are needed. These subnets are used as follows:

One private subnet for user VMs, which houses the virtual machines that users interact with.

Another private subnet for cluster management, which is used for internal cluster operations and management tasks, ensuring that management traffic is isolated from user traffic for security and performance reasons.

Nutanix Support & Insights

Nutanix Cloud Clusters on AWS Administration

QUESTION 47

An administrator planned to create a new NC2 cluster and chose the existing AWS VPC infrastructure in the workflow. The administrator need two private subnets to complete the configuration.

What are these two private subnets used for..

- A. For user VMs and cluster management
- B. For Prism Element and Prism Central management
- C. For DNS and NTP management
- D. For private NAT and Elastic IP management

Correct Answer: A

Section:

Explanation:

The requirement for two private subnets in the NC2 cluster configuration workflow serves the same purposes:

One subnet is designated for user VMs, ensuring user workloads are separated from management operations.

The other subnet is designated for cluster management, maintaining the integrity and security of management processes and internal communications.

Nutanix Clusters on AWS Deployment Guide

Nutanix Cloud Clusters on AWS Administration

QUESTION 48

An administrator is deploying a new cluster on AWS and would like to ensure the data is encrypted. Due to cost constraints, the deployment will leverage the native local key manager (LKM).

What is the minimal number of nodes needed to support the Nutanix native LKM?

- A. 1
- B. 2
- C. 3
- D. 4

Correct Answer: C



Section:**Explanation:**

To support Nutanix's native Local Key Manager (LKM) for data encryption in a cost-effective manner, a minimum of three nodes is required. This ensures that there is enough redundancy and reliability for the encryption services to function properly, complying with best practices for distributed key management.

Nutanix Support & Insights

Nutanix Cloud Clusters on AWS Administration

QUESTION 49

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

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

Correct Answer: B, D

Section:**Explanation:**

To manually hibernate an NC2 on AWS cluster, the administrator can use the following methods:

Select the cluster under NC2 console and Select Hibernate/Resume on the cluster sur page: Navigate to the specific cluster in the NC2 console and use the provided Hibernate/Resume option.

Log into NC2 console, find the cluster name and select Hibernate/Resume from the ellipses: Access the NC2 console, locate the cluster name, and select the Hibernate/Resume option from the ellipses (three dots) menu.

These options allow for the manual control of the cluster's hibernation state directly within the NC2 console interface.

Nutanix Cloud Clusters on AWS Administration

Nutanix Support & Insights

**QUESTION 50**

What is the purpose of an organization in the NC2 console?

- A. To link with NC2 subscription plans
- B. To map the on-premises Prism Central environment
- C. To segregate clusters based on specific requirements
- D. To Link with a Public Cloud account

Correct Answer: C

Section:**Explanation:**

In the NC2 console, an organization is used to segregate clusters based on specific requirements. This segregation allows administrators to manage clusters more effectively by grouping them according to business units, projects, or other criteria. This organizational structure helps in maintaining clear boundaries and applying specific policies or permissions to different clusters within the same NC2 environment.

Nutanix Cloud Clusters on AWS Administration

Nutanix Certified Professional - Cloud Integration - AWS

QUESTION 51

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.

Correct Answer: A

Section:

Explanation:

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.

Nutanix Cloud Clusters on AWS Deployment Guide

Nutanix Support & Insights

QUESTION 52

To deploy NC2 in AWS using an existing VPC, which two AWS resources should be configured beforehand? (Choose two.)

- A. NAT Gateway
- B. Public and Private Subnets
- C. Placement Group
- D. Bare-metal EC2 Instance

Correct Answer: A

Section:

Explanation:

To deploy NC2 in AWS using an existing VPC, the following AWS resources should be configured beforehand:

NAT Gateway: This allows instances in the private subnet to connect to the internet or other AWS services, while preventing the internet from initiating connections with those instances.

Public and Private Subnets: These are necessary to segregate the network traffic. Public subnets provide a direct route to the internet gateway, while private subnets are used for internal resources that do not need direct access to the internet.

Nutanix Cloud Clusters on AWS Deployment Guide

Nutanix Support & Insights

QUESTION 53

Which entity should be contacted for cloud hardware supported (EC2 instances, VPC, etc) related to NC2?

- A. Partner
- B. Public Cloud Vendor
- C. Internal IT Operations team
- D. Nutanix

Correct Answer: B

Section:

Explanation:

For issues related to cloud hardware support such as EC2 instances, VPC, etc., the public cloud vendor (AWS in this case) should be contacted. AWS provides support and documentation for their infrastructure and services, ensuring that users can get assistance for any hardware or cloud-specific queries.

Nutanix Support & Insights



QUESTION 54

Exhibit.

```
Id : 56447579 Protection Domain : pd_1621856221288635_555 Replication Operation : Sending Start Time : 05/24/2021
14:23:15 UTC Remote Site : remote_10_xx_xx_22_000xx00f-xxxx-0659-xxxx-xxx0006095 Snapshot Id : 56004377 Aborted :
false Paused : false Bytes Completed : 0 bytes Complete Percent : 0.0
```

What does the exhibit indicate?

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

Correct Answer: A

Section:

Explanation:

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.

Nutanix Protection Domain and Replication Documentation

Nutanix Best Practices for Monitoring Replication

QUESTION 55

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.

Correct Answer: C

Section:

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.

