

Nutanix Certified Associate (NCA) v6.5 exam

Nutanix NCA-6.5

Version Demo

Total Demo Questions: 12

Total Premium Questions: 128

Buy Premium PDF

<https://passqueen.com>

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Describe the Nutanix Enterprise Cloud Platform	34
Topic 2, Manage the Nutanix Enterprise Cloud Platform	38
Topic 3, Configure the Nutanix Enterprise Cloud Platform	40
Topic 4, Troubleshoot the Nutanix Enterprise Cloud Platform	16
Total	128

QUESTION NO: 1

An administrator wants to reduce the risk of an unauthorized user accessing Prism Central.

Which two actions are recommended? (Choose two.)

- A. Configure role-based access control using least-privilege roles
- B. Integrate Prism Central with a directory service
- C. Use one shared administrator account for all operators
- D. Assign every user the Super Admin role

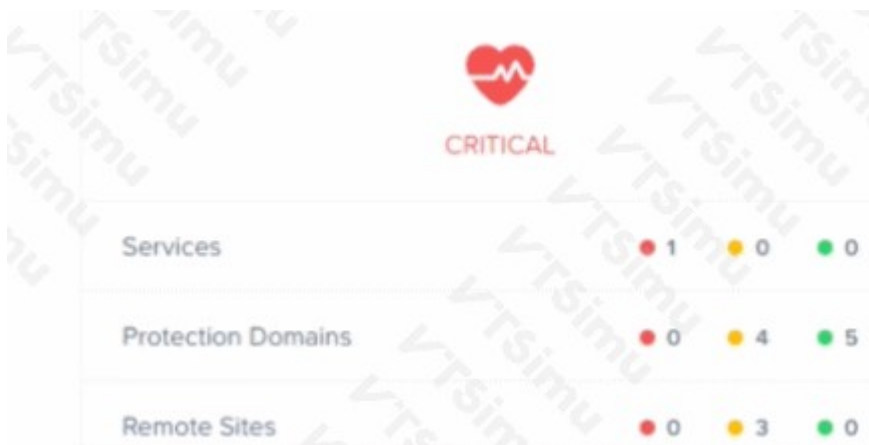
ANSWER: A B

Explanation:

Configure role-based access control using least-privilege roles and **integrate Prism Central with a directory service** are recommended actions. RBAC allows administrators to assign only the permissions required for each user or operational group, reducing the risk associated with broad administrative access. Directory-service integration centralizes identity management and allows organizations to apply established authentication and account-lifecycle processes.

These controls help organizations manage access consistently as administrators, operators, and application teams change over time. Shared administrator credentials and unrestricted roles reduce accountability and do not follow security best practices. See the [Nutanix Prism Central user management documentation](#) and the [Nutanix Security overview](#).

QUESTION NO: 2



Upon logging into Prism Element an administrator sees a red heart, as shown in the exhibit. Which dashboard in Prism will best help the administrator to isolate the cause of the red heart?

- A. Health
- B. Tasks
- C. Analysis
- D. Hardware

ANSWER: A

Explanation:

Health is the appropriate Prism Element dashboard for isolating the condition represented by a red heart status indicator. Prism uses the cluster health status to provide an at-a-glance indication of whether active alerts require attention. Selecting the Health dashboard exposes the underlying health checks and alerts that contribute to the overall state, allowing an

administrator to identify the affected service, host, storage component, or cluster condition. The dashboard organizes health information by severity and includes the alert details needed to begin remediation, such as the condition description, impacted entity, and relevant timestamps. This makes it the primary investigation point immediately after a degraded or critical cluster-health indicator appears. An administrator can then drill into the reported alert and follow its recommended resolution guidance or collect more detail from the relevant Prism view. Nutanix documents cluster monitoring and alert investigation as part of Prism Element administration; see the [Prism Element Web Console Guide](#) and the [Nutanix Support Portal documentation library](#).

QUESTION NO: 3

An administrator needs to present a Nutanix Volume Group to a Windows Server VM by using iSCSI.

Which two items are required for the VM to connect to the Volume Group? (Choose two.)

- A. Data Services IP
- B. iSCSI initiator access configuration
- C. Container whitelist
- D. Prism Central virtual IP

ANSWER: A B

Explanation:

A Data Services IP and an **iSCSI initiator access configuration** are required for a client VM to connect to a Nutanix Volume Group. The Data Services IP provides the client-facing iSCSI target portal for Nutanix storage services. The Windows Server VM uses this address when discovering and connecting to the Volume Group.

The VM iSCSI initiator must also be authorized for the Volume Group. Administrators configure the initiator IQN, or an appropriate initiator group, as part of the Volume Group access control configuration. This ensures that only approved clients can discover and attach the presented block storage. See the [Nutanix Volumes Guide](#) for Volume Group and iSCSI configuration information.

QUESTION NO: 4

An administrator wants to make an operating system ISO available for VM deployment on AHV.

Which two image types can be managed by the Nutanix Image Service? (Choose two.)

- A. ISO images
- B. Disk images
- C. Volume Groups
- D. Protection Domains

ANSWER: A B

Explanation:

ISO images and **disk images** can be managed by the Nutanix Image Service. An ISO image can be attached to a VM as virtual optical media for operating system installation. A disk image can be used as the source disk when deploying a VM from an existing operating system image.

Volume Groups provide externally accessible block storage and are not Image Service image types. A Protection Domain is a data-protection construct used to group entities for snapshots and replication. See the [Prism Element Web Console Guide: Image Configuration](#).

QUESTION NO: 5

Which address allows external connections to Nutanix storage presented by the Volumes feature?

- A. Prism Central IP
- B. Prism Central IP
- C. Data Services IP
- D. IPMI IP

ANSWER: C

Explanation:

Data Services IP is the dedicated address used for externally accessible Nutanix data services, including storage exposed through the Volumes feature. A Volume Group presents block storage from the Nutanix cluster to external clients through supported protocols such as iSCSI. For those clients to discover and connect to the presented storage, the cluster requires a Data Services IP on the appropriate storage network. This IP provides a stable, client-facing endpoint rather than tying external storage access to a Controller VM management address or another administrative interface. The Data Services IP is configured as part of the cluster storage-network setup and can also support other data-service workflows that require connectivity outside the cluster. In practice, an external host uses this address as the target portal when establishing its connection to a Volume Group, after the relevant initiator and access settings have been configured. Nutanix documentation describes the Data Services IP as the network address for external access to Nutanix storage services and documents its configuration in the storage-network workflow. See the [Nutanix Prism Administration Guide: Storage Networks](#) and the [Nutanix Prism Web Console Guide: Volume Groups](#).

QUESTION NO: 6

An administrator needs to use Flow Network Security to apply a common microsegmentation policy to a large set of application VMs.

Which two actions should the administrator perform? (Choose two.)

- A. Create categories for the application workloads
- B. Use the categories in the security policy
- C. Configure a container whitelist
- D. Assign a Data Services IP to every VM

ANSWER: A B

Explanation:

Create categories for the application workloads and **use the categories in the security policy** are the appropriate actions. Flow Network Security policies can use Prism Central categories to define the source and destination groups to which rules apply. Categorizing the application VMs allows the administrator to manage policy membership dynamically instead of selecting every VM individually.

When a new VM receives the relevant category, it becomes part of the policy scope automatically. Configuring a container whitelist controls external NFS client access and does not define VM-to-VM microsegmentation. See the [Nutanix Flow Network Security overview](#) and the [Prism Central Guide: Categories](#).

QUESTION NO: 7

Refer to the exhibit.

An administrator has configured Prism Central to email daily digests of alerts on a cluster. After a week, the administrator notices that digests are not being received.

What is the most likely cause of the issue?

- A. The recipient address is not registered with Nutanix.
- B. Nutanix support is not enabled as a recipient.
- C. The tunnel connection has not been enabled.
- D. The SMTP server is not configured properly.

ANSWER: D

Explanation:

The SMTP server is not configured properly. Prism Central uses the configured SMTP service to send alert notifications and scheduled alert digests to recipients. Creating a daily digest schedule and specifying recipient addresses determines what Prism Central should send and who should receive it, but successful delivery still depends on valid outbound email settings. These settings include a reachable SMTP server, the correct server address and port, any required authentication credentials, and appropriate TLS/SSL configuration. Network connectivity from Prism Central to the mail server must also be permitted, including firewall rules and DNS resolution where a hostname is used. A mail relay that rejects the sender address or requires authentication that has not been configured can likewise prevent messages from leaving Prism Central. The administrator should validate the SMTP configuration in Prism Central, use its email test capability if available, and review the mail server logs to confirm whether it receives and accepts the relay request. Nutanix documents email-alert configuration as a Prism Central service that relies on SMTP settings for notification delivery. See the [Nutanix Prism Central Guide: Configuring Email Alerts](#) and the [Nutanix Prism Central Guide: Configuring an SMTP Server](#).

QUESTION NO: 8

An administrator has received the following critical alert:

Node 192.168.148.172 is marked to be detached from metadata. The administrator has opened a case with Nutanix and the support engineer has requested more information about the error. Which two actions should the administrator take in the Health Check dashboard to collect the requested information? (Choose two.)

- A. Create an Entity chart
- B. Open a remote support tunnel.
- C. Run the Log Collector
- D. Run the Nutanix Cluster Check

ANSWER: C D

Explanation:

Running the Log Collector and running the Nutanix Cluster Check provide the diagnostic material Nutanix Support needs to investigate a metadata-detach alert. The Log Collector gathers relevant cluster logs and configuration information into a support bundle. This preserves the event context, service messages, and other artifacts needed to analyze the node and metadata condition at the time of collection. The resulting bundle can be supplied through the support case as requested by the support engineer.

The Nutanix Cluster Check (NCC) performs Nutanix health and configuration checks and produces results that identify detected cluster issues, warnings, and failures. Its output gives Support a current health assessment and can expose related conditions affecting metadata services, node communication, storage, or cluster resiliency. Collecting both the log bundle and NCC results from the Health Check dashboard gives the case a combination of detailed diagnostic evidence and a structured health-check report. Nutanix documents Health dashboard operations, including log collection and NCC execution, in the [Prism Health Dashboard documentation](#). Additional official guidance and support resources are available through the [Nutanix Support Portal](#).

QUESTION NO: 9

Which Nutanix storage service can store Petabytes of unstructured data and supports S3 APIs?

- A. DSF
- B. Files
- C. Volumes
- D. Objects

ANSWER: D

Explanation:

Objects is Nutanix's scale-out object-storage service for large volumes of unstructured data. It presents an Amazon S3-compatible API, allowing applications that use the S3 protocol to store, retrieve, and manage data without requiring application changes for a proprietary storage interface. This makes it suitable for workloads such as backup repositories, archives, media assets, application data lakes, and cloud-native applications that require durable, massively scalable object storage.

Nutanix Objects is designed to scale capacity across cluster nodes and support petabyte-scale deployments. Data is organized as objects in buckets rather than as files in a hierarchical file system or as block devices attached to hosts. Its S3 compatibility includes the familiar bucket- and object-based access model used by many modern applications and data-protection products. Objects also provides enterprise capabilities such as access controls, encryption, replication options, and lifecycle-oriented data management, depending on the configured version and environment. Nutanix identifies Objects as its software-defined, S3-compatible object-storage offering for unstructured data at scale. See the [Nutanix Objects product page](#) and the [Nutanix data protection solutions overview](#).

QUESTION NO: 10

How is the destination cluster determined when uploading images from the local workstation to Prism Central?

- A. Selected randomly
- B. Selected manually
- C. Selected alphabetically
- D. Selected sequentially

ANSWER: B

Explanation:

Selected manually is correct because Prism Central requires the administrator to choose the target cluster when uploading an image from a local workstation. In the image-upload workflow, the selected cluster is the location where Prism Central initially places and stores the uploaded image. This selection is important because image data consumes storage capacity on that cluster and is written to a container available on the selected target. Prism Central then manages the image as part of its centralized image services, allowing the administrator to use it for VM provisioning and other supported operations across the Prism Central environment as applicable. The administrator should therefore select a cluster with appropriate available capacity, connectivity, and a suitable storage container for the image type being uploaded. This explicit placement choice provides predictable control over where the upload is staged rather than relying on an automatic naming-based or rotation-based selection process. Nutanix documents image management and upload operations in its Prism Central documentation; see the [Nutanix Prism Central documentation portal](#) and the [Nutanix Product Documentation page](#).

QUESTION NO: 11

An administrator is configuring a Protection Domain for a group of related application VMs.

Which two capabilities are provided by a Protection Domain? (Choose two.)

- A. Create crash-consistent snapshots
- B. Replicate protected data to a remote site
- C. Apply VM anti-affinity rules
- D. Increase vCPU allocation automatically

ANSWER: A B

Explanation:

Create crash-consistent snapshots and **replicate protected data to a remote site** are capabilities provided by a Protection Domain. A Protection Domain groups entities that require a common data-protection policy. Snapshot schedules can create recovery points for the protected VMs, and replication schedules can transfer those recovery points to a configured remote site for disaster recovery.

A Protection Domain does not provide host-level placement rules or automatically increase VM compute resources. Those functions are handled by AHV placement capabilities and VM configuration workflows. See the [Prism Element Web Console Guide: Data Protection](#).

QUESTION NO: 12

Which component is required to create application-consistent snapshots of supported guest operating systems?

- A. Nutanix Guest Tools
- B. Prism Central

C. Lifecycle Manager

D. Data Services IP

ANSWER: A

Explanation:

Nutanix Guest Tools is correct because application-consistent snapshots require in-guest coordination. Nutanix Guest Tools includes the guest agent used to communicate with the guest operating system and quiesce supported applications before the snapshot is created.

Without this guest-level integration, Nutanix can still create crash-consistent VM snapshots, but it cannot coordinate application writes in the guest before capturing the recovery point. The guest operating system and installed applications must also support the required quiescing mechanism. See the [Prism Element Web Console Guide: Guest Tools](#).