DUMPSARENA

Nutanix Certified Professional - Data Services

Nutanix NCP-DS

Version Demo

Total Demo Questions: 14

Total Premium Questions: 145

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Nutanix Files	70
Topic 2, Nutanix Objects	40
Topic 3, Nutanix Volumes	29
Topic 4, Mix Questions	6
Total	145

QUESTION NO: 1

An administrator would like to convert an existing Volume Group with an attached external

Windows client to use Volumes

The administrator has taken these actions

. Disconnect any existing SCSI targets

Remove targets from the Favorite Targets tab

• Remove targets from the Discovery tab

Which action must the administrator take next to complete this task?

A. Connect with MPIO to the ISCSI Data Services IP

B. Connect without MPIO to the Cluster Virtual IP

C. Connect without MPIO to the iSCSI Data Services IP

D. Connect with MPIO to the Cluster Virtual IP

ANSWER: A

Explanation:

Connect with MPIO to the ISCSI Data Services IP is correct. Nutanix Volumes presents Volume Groups to external hosts through the cluster's iSCSI Data Services IP address. After removing the prior target discovery and persistent target entries from the Windows iSCSI Initiator, the Windows host must rediscover and reconnect to the Volume Group through that Data Services IP. This ensures that the client uses the Nutanix Volumes access method rather than its previous target configuration.

For a Windows client, Multipath I/O must be used for the iSCSI connection. MPIO provides multiple iSCSI paths to the Volume Group, allowing Windows to maintain storage access if an individual path becomes unavailable and enabling the supported resilient connectivity model for Nutanix Volumes. The administrator should therefore ensure the Windows MPIO feature and iSCSI device support are configured, then establish the target session using the iSCSI Data Services IP with multipathing enabled.

Nutanix documents external-host access and iSCSI client configuration for Volume Groups in the Nutanix Volumes Guide: Windows Clients. General Volume Group and external-client concepts are also covered in the Nutanix Data Services documentation.

QUESTION NO: 2

A company has a number of thin clients which need to boot over the network. The company is

using Volumes for this project.

Which two components are needed to meet these requirements? (Choose two.)

A. A VG per client with a Disk for boot

B. A compatible Ethernet adapter per client

C. A DHCP server pointing to the Nutanix cluster

D. A client with MPIO access to the VG

ANSWER: B C

Explanation:

Network boot with Nutanix Volumes relies on iSCSI boot capability at the endpoint and network-delivered boot configuration. A compatible Ethernet adapter per client is required because the client NIC must support the applicable network/iSCSI boot functionality, allowing firmware to establish storage connectivity before the operating system is running. This is what enables the thin client to reach the boot volume over the network rather than requiring a locally installed boot disk.

A DHCP server pointing to the Nutanix cluster is also required to provide the client's initial network configuration and the boot-target information needed during the pre-OS boot sequence. The DHCP-based configuration directs the boot-capable adapter toward the Nutanix Volumes iSCSI service so that the client can discover and connect to its assigned boot storage. Together, compatible boot-capable NIC hardware and DHCP-delivered target configuration provide the essential client-side and network-side elements for this workflow. Nutanix Volumes provides block storage to external clients through iSCSI; see the Nutanix Volumes overview and the Nutanix Documentation Portal for Volumes deployment and client-connection guidance.

QUESTION NO: 3 - (SIMULATION)

A developer requires API access to a S3 destination for storage. The environment is currently

configured as:

• 4 node Nutanix cluster

• Both Files and Objects have been deployed

• Active Directory access has been configured for Files and Objects

How would an administrator grant Read-Write access for the developer?

A • Create a new Share/Export within Files supporting multi-protocol access.

• Check the checkbox to Enable API Access

B. Click + Add People under User Accounts within Objects and add the developer account

• Click the checkbox to enable Kerberos Token Authentication

• Create a new Bucket and add the user.

C. Create a new Share/Export within Files supporting multi-protocol access.

• The developer can utilize the REST API to write to the destination.

D. Click + Add People under Access Keys within Objects and add the developer account.

Download the Access Key and provide it to the developer.

• Create a new Bucket and add the user.

ANSWER: See the explanation for the answer

Explanation:

Correct answer: D.

The developer needs S3 API access, which is provided by **Nutanix Objects**, not Files. Create credentials for the Active Directory user under **Objects > Access Keys**:

Click **+ Add People** under **Access Keys**.
Select/add the developer's account.
Download and securely provide the generated access key credentials to the developer.
Create the required Objects bucket and grant the developer read-write permissions to that bucket (using the appropriate bucket access/policy settings).

The developer can then configure their S3-compatible client or application with the Nutanix Objects endpoint, access key, and secret key to read from and write to the bucket.

Files shares/exports do not provide an S3 destination, and Kerberos token authentication is not the required credential mechanism for normal S3 API access in this scenario.

QUESTION NO: 4

An organization requires browsers and S3 API clients to trust the HTTPS endpoint of a new Objects deployment.

The organization has issued a certificate from its internal Certificate Authority.

Which two files must the administrator provide when configuring the Objects certificate? (Choose two.)

A. The certificate file or certificate chain

B. The matching private key file

C. The Objects Data Services IP address

D. An S3 access key for the Objects administrator

ANSWER: A B

Explanation:

The certificate file or certificate chain is required so Objects can present the certificate issued by the trusted internal CA to browsers and API clients. The certificate must contain the DNS name used to access the Objects endpoint.

The matching private key file is also required because it is the private component of the certificate key pair. Objects uses the private key to establish TLS sessions and prove possession of the certificate identity. Where applicable, the certificate chain should include required intermediate CA certificates so clients can validate the full chain to the internal root CA.

A Data Services IP address and an S3 access key are unrelated to installing a trusted TLS certificate. See the Nutanix Objects product page and the Nutanix Objects documentation.

QUESTION NO: 5

Refer to the exhibit.



An administrator has been informed that a new workload will be deployed in six months with these characteristics.

• CPU: 210 GHz

• Memory: 600 GiB

• Storage:11.72 TiB

Upon receiving the new project notification, the administrator creates a scenario to determine whether or not the Nutanix cluster has enough space capacity to properly handle the new workload.

Why is the Overall Cluster runway showing that cluster resources are not exhausted (red color)?

A. Target analysis timeframe starts after additional resources are added.

B. There are enough available resources to support the new workload.

C. Additional resources will be added before the new workload is added

D. Target analysis timeframe ends before the new workload is added.

ANSWER: D

Explanation:

Target analysis timeframe ends before the new workload is added. Prism Central Runway evaluates projected resource consumption only within the configured analysis window. A scenario change, such as adding a workload with defined CPU, memory, and storage requirements, affects the runway calculation beginning at the workload's specified effective date. If that date is six months in the future but the target analysis timeframe finishes earlier, the projected demand from that workload is outside the period being evaluated.

Consequently, the Overall Cluster runway does not include the workload's resource requirements when determining whether CPU, memory, or storage will reach exhaustion. The runway can therefore remain non-red even though the workload may create a capacity concern after the configured analysis period. To assess the planned deployment accurately, the administrator should extend the target analysis timeframe so that it includes the workload's deployment date and sufficient time afterward to observe its projected effect on cluster capacity. Nutanix documents that Runway planning uses scenario-based projections and a selected timeframe to forecast resource exhaustion. See the Nutanix Prism Central Runway view documentation and the Nutanix documentation portal.

QUESTION NO: 6

An administer has a new requirement to separate management and block storage network traffic for bare-metal workloads. What should the administrator do to satisfy this requirement?

A. Add a second virtual NIC to CVMs, configure them in prism.

B. Configure Backplane LAN to isolate hypervisor traffic

C. Configure Management LAN to segment internal communication.

D. Enable Volumes network segmentation

ANSWER: D

Explanation:

Enable Volumes network segmentation is the appropriate configuration because it provides a dedicated network path for Nutanix Volumes iSCSI block-storage traffic, separate from the management network used for administrative and cluster-management communications. For bare-metal workloads, the physical host acts as an iSCSI initiator and requires connectivity to the storage service presented by the CVMs. Enabling this feature allows the administrator to assign that storage-facing traffic to a distinct VLAN or subnet, so iSCSI data does not share the management network.

This separation is valuable for both operational and security reasons: management access remains isolated from application storage I/O, and storage traffic can be routed, monitored, and protected according to its own network policy. The network design must ensure that each bare-metal initiator can reach the segmented Volumes network and that the required iSCSI

connectivity is permitted. Nutanix Volumes is Nutanix's block-storage service and supports using dedicated networking for its storage data path. See the Nutanix Volumes product overview and the Nutanix documentation portal for the applicable Volumes and Prism configuration guidance for the deployed AOS release.

QUESTION NO: 7

An administrator manages a vSphere-based Nutanix cluster and has enabled Flash Mode for

extremely latency sensitive The administrator recently migrated several workloads from this

cluster to another cluster with higher CFU and migration, users complained about the VM

performance of the latency sensitive workloads.What must the administrator to resolve this issue?

A. Manually fingerprint the migrated

B. Flash Mode can only be enabled on the VM curing the world

C. Flash usage exceeds 20% of the new SSD capacity tier

D. Manually enable Flash Mode on the migrated workloads

ANSWER: D

Explanation:

Manually enable Flash Mode on the migrated workloads. Flash Mode is a per-VM setting that keeps a VM's data preferentially in the Nutanix SSD tier to provide the consistently low latency required by highly latency-sensitive applications. When a workload is moved to a different Nutanix cluster, the destination cluster must apply its own local storage and VM data-placement configuration. The administrator should therefore verify the migrated virtual machines' Flash Mode status in the destination environment and explicitly enable Flash Mode for each applicable workload. This restores the intended SSD-tier placement behavior and helps return storage latency and application performance to the expected level. Flash Mode should be reserved for workloads with a demonstrated low-latency requirement and monitored after activation so that SSD-tier capacity remains appropriately sized. Nutanix describes Flash Mode as a VM-level capability for prioritizing storage performance, and its operation depends on the destination cluster's available SSD resources and configuration. See the Nutanix Prism Web Console Guide: Flash Mode and the Nutanix Prism Web Console Guide: Managing VMs.

QUESTION NO: 8

An administrator needs to configure Windows Server Failover Clustering (WSFC) in a

Nutanix

environment using storage provided by the Nutanix cluster.

Which two prerequisites are required to accomplish this task? (Choose two.)

A. Configure a Data Services IP on the Nutanix cluster.

B. Record the IQNs or IPs of the WSFC virtual machines

C. Ensure the WSFC clients are on the same subnet as the Nutanix cluster

D. Verify that the WSFC clients have one-way CHAP configured

ANSWER: A B

Explanation:

Configuring a Data Services IP on the Nutanix cluster is required because Nutanix Volumes presents a volume group as an iSCSI target through a Data Services IP address. The WSFC nodes use this address as the target portal when discovering

and connecting to the shared storage. The Data Services IP must therefore be configured and reachable from every cluster node that will consume the volume group.

Recording the IQNs or IPs of the WSFC virtual machines is also required before granting the nodes access to the volume group. Nutanix uses iSCSI client identification, based on an initiator IQN or an IP address, to define which guests are permitted to connect to a volume group. Each intended WSFC node must be added as an authorized iSCSI client so that all nodes can access the same shared disks. This shared, consistently presented storage is fundamental to a WSFC deployment using Nutanix Volumes.

For implementation details, see the Nutanix Volumes Guide: Add an iSCSI Client and the Nutanix Volumes overview.

QUESTION NO: 9

Which two network requirements must an administrator take into consideration when configuring and defining client and storage networks? (Choose two.)

A. Ensure there is one IP address available for the storage network

B. Ensure there is one IP address available for client network

C. The Client and storage networks must have separate subnets.

D. Ensure the client and storage networks use a tagged VLAN

ANSWER: B D

Explanation:

Ensure there is one IP address available for client network is required because the client network supplies the address through which users and applications access the data service. This client-facing IP is a fundamental part of establishing client connectivity and must be available in the selected network during configuration. Ensure the client and storage networks use a tagged VLAN is also required because VLAN tagging identifies the intended Layer-2 network for each service network and keeps traffic mapped to the administrator-defined network segment. Correct VLAN configuration is particularly important where client access and storage communication traverse shared physical switching infrastructure; it enables the platform to attach its interfaces to the appropriate logical networks reliably. Administrators should therefore confirm that the required VLANs are configured consistently on the Nutanix hosts and the connected physical switch ports before deployment or network changes. Nutanix Files documentation describes the network configuration workflow and the required client and storage network settings in its Network Configuration documentation. Nutanix also provides deployment and networking guidance through the Nutanix Support Portal documentation library.

QUESTION NO: 10

Due to a new IP addressing plan for the Desktops network, an administrator needs to change

the Files client-side network

Which action should the administrator perform first?

A. Power off the FSVMS

B. Stop the Files service

C. Create a new managed virtual network

D. Remove existing DNS entries

ANSWER: B

Explanation:

Stop the Files service is the required first action before changing a Nutanix Files client-side network. The client-side network supplies the addresses through which SMB and NFS clients access the file server. Stopping the service places the file server into the required maintenance state so its client-network configuration can be safely modified without active file-serving operations using the existing network configuration.

After the service is stopped, the administrator can update the client-network settings in the Files management interface, including the applicable VLAN, subnet, gateway, and IP-address allocation details for the new addressing plan. Nutanix Files then applies the revised configuration to the file server components when the service is brought back online. This sequencing is important because the client-access addresses are integral to the Files service and are not simply guest-level network settings on individual FSVMs. The expected maintenance impact should be communicated to users because client access to shares is unavailable while the Files service is stopped and the network change is applied.

See the Nutanix Files documentation and the Nutanix Files product overview for Files architecture and administration resources.

QUESTION NO: 11

The administrator is migrating users' home directories from a legacy SAN to Files. The

administrator wants to make sure that the users can only access their home directory, and that

when a new employee logs in for the first time, a home directory is automatically created.

What should the administrator do to satisfy these requirements?

A. Create a Standard SMB share and edit folder permissions using the MMC plugin.

B. Create a Standard NFS share and set the default access to Read-only.

C. Create a Distributed NFS share and set the default access to No Access

D. Create a Distributed SMB share and edit folder permissions using the MMC plugin.

ANSWER: A

Explanation:

Create a Standard SMB share and edit folder permissions using the MMC plugin. Nutanix Files supports SMB home-directory use cases through a standard SMB share, where the administrator can use the Microsoft Management Console MMC plug-in to manage the share's NTFS-style permissions and ACLs. This lets the administrator apply permissions so that each user is granted access only to that user's assigned home folder. The home-directory capability can create the appropriate user directory when the user initially accesses the share, avoiding the need to manually provision a folder for every new employee.

This approach is appropriate for Windows user home directories because SMB integrates with Active Directory identities and Windows security descriptors. Managing ACLs through the MMC plug-in provides the familiar Windows administrative workflow needed to set ownership and access controls on the automatically provisioned folders. Nutanix Files documents SMB shares, Active Directory integration, and Windows-compatible permission management as core Files capabilities. See the Nutanix Files product overview and the Nutanix documentation portal for the Files administration documentation applicable to the deployed Files version.

QUESTION NO: 12

An administrator is notified by a user about a problem regarding a file within a Files share.

The file AIC.docx is being periodically deleted by another user. The administrator is asked to

collect information about who is deleting this file.

How should the administrator collect the required information in File Analytics

A. Use File Operations on the dashboard for the docx

B. Use Audit Trails and search for file AIC.docx

C. Configure Alert Notification for file and does

D. Configure Anomaly Rules for file ARC, docx

ANSWER: B

Explanation:

Use **Audit Trails and search for file AIC.docx**. File Analytics audit trails provide an event-level record of activity performed against files and folders in Nutanix Files shares. For a recurring deletion, the administrator can search or filter the audit data using the affected file name and then review the matching delete events. Each audit event supplies the context needed for an investigation, including the user identity associated with the operation, the action performed, the relevant path or object, and the event time. This lets the administrator establish who deleted the file and correlate repeated deletion events over a selected time range. Audit data is intended to support operational investigation, accountability, and forensic review of file activity, rather than merely showing aggregate usage trends. Nutanix describes Files as providing file services with governance and analytics capabilities, including visibility into file activity. See the Nutanix Files product overview and access the applicable Files administration documentation through the Nutanix Support Portal documentation portal.

QUESTION NO: 13

Which two configuration elements can an administrator find in the File Server -> FILE

SERVER DETAILS tab? (choose two.)

A. Share/Export Count.

B. Total Number of Files.

C. DNS Domain Name.

D. Quarantined Files.

ANSWER: A C

Explanation:

The File Server Details tab provides an at-a-glance view of the selected Nutanix Files instance, including its identity and key service inventory. **Share/Export Count.** is shown as a summary value, enabling an administrator to see how many SMB shares and/or NFS exports are configured for the file server without opening each individual share or export configuration. This is useful for quickly validating the file service footprint and identifying the scope of hosted file access resources.

DNS Domain Name. is also a file-server configuration attribute displayed in the details view. The DNS domain is fundamental to name resolution and, for an Active Directory-integrated deployment, helps identify the domain context in which the file server operates. Administrators use this information when confirming that a file server has been deployed with the intended DNS and directory-service settings.

Nutanix Files documentation describes using the Files management interface to inspect file-server configuration and operational details, including identity, network, directory, and share-related information. See the Nutanix Files documentation and the Nutanix Files product overview for additional context on Files management and supported SMB/NFS services.

QUESTION NO: 14

An administrator is migrating a Windows file server to Nutanix Files across an unreliable WAN connection.

The administrator must preserve NTFS security information and ensure that interrupted copy operations can resume.

Which two Robocopy options should the administrator use? (Choose two.)

A. Use the `/Z` option

B. Use the `/SEC` option

C. Use the `/L` option

D. Use the `/MOV` option

ANSWER: A B

Explanation:

Use the `/z` option because it enables restartable mode. If the WAN connection is interrupted, Robocopy can resume the copy operation rather than requiring the administrator to restart the transfer from the beginning.

Use the `/SEC` option because it copies NTFS security information along with file data, attributes, and timestamps. This preserves the source access control lists on the destination Files SMB share, subject to the migration account having the required permissions.

The `/L` option only lists the files that would be copied and does not transfer data. The `/MOV` option removes source files after a successful copy and is not appropriate for an initial staged migration. Microsoft documents these options in the Robocopy command reference. Nutanix Files provides SMB file services suitable for Windows file-server migrations; see Nutanix Files.