

Nutanix Certified Professional - Unified Storage (NCP-US) v6.5

Nutanix NCP-US-6.5

Version Demo

Total Demo Questions: 13

Total Premium Questions: 137

Buy Premium PDF

<https://passqueen.com>

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Storage Concepts and Architecture	21
Topic 2, Configure and Manage Nutanix Volumes	6
Topic 3, Configure and Manage Nutanix Files	43
Topic 4, Configure and Manage Nutanix Objects	14
Topic 5, Mix Questions	53
Total	137

QUESTION NO: 1

An administrator is using Citrix Studio to configure policies for their existing CVAD environment on to a Nutanix Files share. The administrator would like to use Citrix Director to reset user profiles.

How should the user profiles be configured?

- A.** use Nutanix Files standard shares
Deploy Citrix Profile Management user stores inside the user's top-level directory
- B.** Redirect user's Desktop, Documents and Favorites to a Nutanix Files home share.
- C.** Redirect user's Desktop, Documents and Favorites to a Nutanix Files general share.
- D.** use Nutanix Files distributed shares.
Deploy Citrix Profile Management user stores inside the user's top-level directory.

ANSWER: A

Explanation:

Use Nutanix Files standard shares and deploy Citrix Profile Management user stores inside the user's top-level directory. This configuration provides a supported, straightforward location for the Citrix Profile Management user store while allowing Citrix Director to perform profile-reset operations. Citrix Profile Management stores each user's profile data in the configured user-store path, typically using a user-specific folder created from path variables such as the user name. Placing that store in each user's top-level directory on a standard Nutanix Files share gives the profile-management service and authorized administrators a consistent SMB path for profile lifecycle actions, including removal of the user's stored profile so it can be recreated at the next logon. Citrix Director's reset capability is intended to work with Citrix Profile Management and requires the relevant profile-management policies and permissions to be in place. Nutanix's CVAD guidance identifies standard shares as the appropriate Files share type when this Director-based profile reset workflow is required. For user-store configuration concepts and supported path variables, see [Citrix Profile Management user-store documentation](#). Nutanix CVAD design guidance is available from the [Nutanix Citrix Virtual Apps and Desktops best-practice guide](#).

QUESTION NO: 2

Which two steps are required for enabling Data Lens? (Choose two.)

- A.** In Prism, enable Pulse health monitoring.
- B.** Configure a MyNutanix account to access the Data Lens console.
- C.** Configure the Data Services IP in Prism Central.
- D.** Add File Services VM admin credentials to a MyNutanix account.

ANSWER: A B

Explanation:

Data Lens is a Nutanix cloud service that provides visibility, governance insights, anomaly detection, and ransomware-related analytics for Nutanix Files. Before its cloud-based analytics can be enabled and used, Prism Central must be able to send the required telemetry through Nutanix Pulse. Therefore, enabling Pulse health monitoring in Prism is a prerequisite: Pulse provides the secure outbound communication path used by Nutanix cloud services and does not require inbound Internet connectivity.

Configuring a MyNutanix account to access the Data Lens console is also required. The MyNutanix identity links the Prism Central environment to Nutanix cloud services and authorizes an administrator to open and manage the Data Lens service. After Pulse is enabled and the appropriate MyNutanix account is configured, an administrator can enable Data Lens for supported Nutanix Files deployments and use the Data Lens console for monitoring and investigation workflows.

These requirements align with Nutanix's Data Lens documentation, which identifies Pulse connectivity and MyNutanix authentication as prerequisites for onboarding the service. See the [Nutanix Data Lens Administration Guide](#) and the [Nutanix Data Lens product page](#).

QUESTION NO: 3

An administrator needs to create a new MCS Catalog, but is receiving a failure error, as shown below:

Acropolis _ Inventory: Getcontent Exception:system.ArgumentException: Error during serialization or deserialization using the JSON Java Scriptserializer. The length of the string exceeds the value set on the maxJsonLenth property.

A. Running the below command on CVM shows the following output:

B. nutanix@cvm: ~\$ acli snapshot.list | wc -l

C. 1919

D. nutanix@cvm: ~\$ acli snapshot.list | wc -l

E. 4787

ANSWER: B E

Explanation:

The relevant validation is to determine whether the cluster has accumulated a very large number of snapshots, because MCS inventory collection can retrieve snapshot metadata as part of its Acropolis inventory request. The intended command, `acli snapshot.list | wc -l`, lists the snapshots known to the cluster and counts the resulting entries. A count of 4787 identifies an unusually large snapshot inventory that can cause the serialized inventory response to exceed the JSON serializer's maximum string-length setting. This directly aligns with the reported GetContent serialization failure during catalog creation.

In practice, the administrator should identify snapshots that are no longer required by protection policies, backup workflows, test activities, or prior provisioning operations, then remove them using the appropriate retention and change-control process. Snapshot cleanup reduces metadata returned by inventory queries and allows MCS catalog creation to proceed without producing an oversized JSON response. Snapshot operations and lifecycle management should be performed carefully because snapshots can be dependencies for recovery and replication workflows. Nutanix documents snapshot administration in its [Prism documentation](#); Citrix also describes MCS catalog creation and its dependency on the selected hosting resource in its [machine catalog documentation](#).

QUESTION NO: 4

An administrator has performed an upgrade to Files. After upgrading, the file server cannot reach the given domain name with the specified DNS server list.

Which two steps should the administrator perform to resolve the connectivity issues with the domain controller servers? (Choose two.)

A. Verify the DNS settings in Prism Element.

B. Verify the DNS entries for the given domain name.

C. Verify the DNS settings in Prism Central.

D. DNS server addresses of the domain controllers.

ANSWER: A B

Explanation:

Verify the DNS settings in Prism Element and verify the DNS entries for the given domain name. Nutanix Files relies on the DNS configuration supplied by the Nutanix cluster to locate and communicate with Active Directory domain controllers. After an upgrade, the administrator should first confirm in Prism Element that the configured DNS server IP addresses and search-domain configuration are still present, reachable, and appropriate for the Active Directory environment. This ensures that the Files deployment is using the intended resolvers rather than stale, unavailable, or incorrectly ordered DNS servers.

The administrator should also validate that the domain's DNS records resolve correctly through those configured servers. Active Directory operations depend on DNS resolution not only for the domain name itself, but also for the service-location records used to discover domain controllers and related directory services. Confirming that the required records are available and return reachable domain-controller addresses helps restore the discovery path that Files uses for domain communication. These checks align with Nutanix guidance to validate cluster DNS configuration and Active Directory name resolution when troubleshooting Files directory connectivity. See the [Nutanix Files documentation](#) and the [Nutanix Support Portal documentation library](#).

QUESTION NO: 5

An administrator has received an alert A130358 - ConsistencyGroupWithStaleEntities with the following details:

Block Serial Number: leswxxxxxxxx

Alert Time: Thu Jan 19 2023 21:56:10 GMT-0800 (PST)

Alert Type: ConsistencyGroupWithStaleEntities

Alert Message: A130358:ConsistencyGroupWithStaleEntities

Cluster ID: xxxxx

Alert Body: No alert body available Which scenario is causing the alert and needs to be addressed to allow the entities to be protected?

- A. One or more VMs or Volume Groups belonging to the Consistency Group contains stale metadata.
- B. One or more VMs or Volume Groups belonging to the Consistency Group may have been deleted.
- C. The logical timestamp for one or more of the Volume Groups is not consistent between clusters.
- D. One or more VMs or Volume Groups belonging to the Consistency Group is part of multiple Recovery Plans configured with a Witness.

ANSWER: B

Explanation:

“One or more VMs or Volume Groups belonging to the Consistency Group may have been deleted.” is correct because this alert identifies stale entity references in a consistency group. A consistency group retains its configured membership so that its member objects can be protected together in a crash-consistent or application-consistent recovery point. If a referenced VM or Volume Group is deleted, the consistency group can retain a reference to an object that is no longer available on the cluster. That unresolved reference is considered stale and prevents Nutanix from completing protection for the group's configured entities.

The administrator should review the consistency group membership and identify the deleted or otherwise unavailable object. Removing the stale entry from the group, or restoring and correctly re-adding the intended entity where appropriate, returns the group to a valid protectable state. This is important before relying on scheduled snapshots or replication, because protection operations require every configured group member to resolve successfully. Nutanix documents consistency groups as the mechanism used to group related VMs and Volume Groups for coordinated data protection; their membership must remain valid for protection workflows to proceed. See the [Nutanix Prism documentation](#) and the [Nutanix documentation portal](#) for product documentation and alert guidance.

QUESTION NO: 6

When creating a Frame account, which two are valid Network Type options? (Choose two.)

- A. Public Network
- B. Private Network
- C. Private Network with VPN

D. Express Route

ANSWER: A C

Explanation:

When a Nutanix Frame account is created, the network type establishes how users and workloads communicate with the Frame environment. **Public Network** is a valid choice for environments in which Frame workloads and end users use public Internet connectivity. This model supports access to Frame resources without requiring a private site-to-site network connection to an organization's internal network.

Private Network with VPN is also a valid network type. It is intended for deployments that require private connectivity between the Frame environment and organizational network resources. The VPN connection provides the protected network path needed for Frame workloads to reach private services, such as internal applications, authentication services, file shares, or other resources that are not exposed to the public Internet. Selecting the appropriate type during account creation is important because it aligns the Frame account's connectivity model with the organization's security and application-access requirements. Nutanix documents these network-type selections as part of the Frame account-creation workflow. See the [Nutanix Frame account creation documentation](#) and the [Nutanix Frame documentation portal](#).

QUESTION NO: 7

An administrator is using a mix of full clones and non-persistent desktops deployed via Citrix MCS on a three-node cluster. The full clone and non-persistent desktops are managed using separate storage containers.

Which two Storage Efficiency features will provide better storage efficiency and performance improvement? (Choose two.)

- A. Compression
- B. Erasure Coding
- C. Deduplication
- D. RDMA

ANSWER: A C

Explanation:

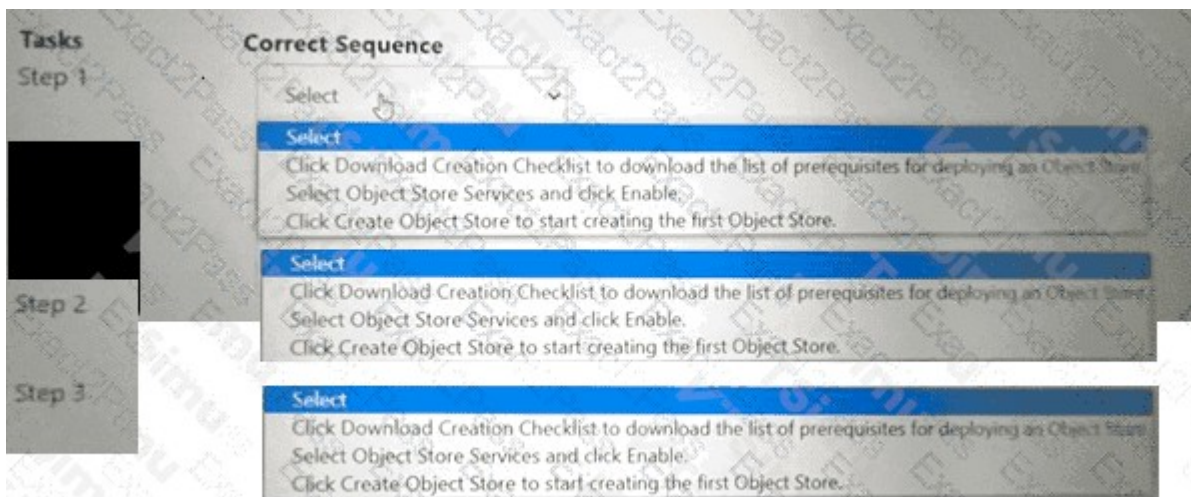
Compression and Deduplication are the appropriate storage-efficiency features for this Citrix MCS virtual-desktop deployment. Desktop images and their clones commonly contain highly repetitive operating-system files, application binaries, and common configuration data. Deduplication identifies identical data extents and stores a single physical copy, while preserving the logical data presented to each desktop. This can substantially reduce the capacity consumed by full clones and by the repeated base-image content associated with non-persistent desktops.

Compression reduces the physical space required for data that remains after deduplication by encoding compressible data more efficiently. In addition to lowering capacity use, reducing the amount of data written to and read from storage can improve effective I/O efficiency for VDI workloads. Nutanix applies these data-reduction capabilities at the storage-container level, which is especially relevant here because the persistent/full-clone and non-persistent desktop populations use separate containers. The administrator can therefore configure the appropriate data-reduction settings for each workload independently, based on its data pattern and expected savings.

Nutanix documents storage efficiency as a core platform capability for reducing physical capacity requirements while supporting workload performance. See [Nutanix Unified Storage](#) and the [Nutanix Prism storage-efficiency documentation](#).

QUESTION NO: 8 - (SIMULATION)

Within the Prism Central Entity > Services > Objects menu option, what is the correct task order for creating an object storage?



ANSWER: See the explanation for the answer

Explanation:

Correct sequence:

1. Select **ObjectStore Services** and click **Enable**.
2. Click **Download Creation Checklist** to obtain and validate the prerequisites for the Object Store deployment.
3. Click **Create Object Store** to begin creating the first Object Store.

The Objects service must be enabled in Prism Central before Object Store functions are available. The checklist should then be reviewed/completed before starting the Object Store creation workflow.

QUESTION NO: 9

Which port is required between a CVM or Prism Central to insights.nutanix.com for Data Lens configuration?

- A. 80
- B. 443
- C. 8443
- D. 9440

ANSWER: B

Explanation:

443 is required because Nutanix Data Lens is a cloud service accessed through `insights.nutanix.com` using HTTPS. During Data Lens configuration, the Nutanix environment needs outbound, secure HTTPS connectivity from the relevant cluster component—either the Controller VM (CVM) or Prism Central—to the Data Lens service. TCP port 443 is the standard port used by HTTPS and provides the encrypted transport required for service authentication, configuration requests, and the exchange of Data Lens analytics-related information.

Allowing this outbound connection is therefore an important network prerequisite before enabling or operating Data Lens for Nutanix Files. The firewall rule should permit the applicable CVM or Prism Central source to reach `insights.nutanix.com` on TCP 443; the requirement concerns outbound service connectivity rather than inbound access from the Internet. Nutanix documentation for Data Lens and Nutanix Files provides the service configuration and networking guidance: [Nutanix Data Lens Administration Guide](#) and [Nutanix Files documentation](#). HTTPS port usage is also standardized as TCP 443 by the Internet Assigned Numbers Authority: [IANA Service Name and Port Number Registry](#).

QUESTION NO: 10

How should an administrator protect Writable AppVolumes during a disaster in a Nutanix environment?

- A. Create a storage container in both the primary and DR data centers for the Writable AppVolumes. Set up asynchronous DR between the two sites.
- B. Enable HA reservations on the cluster to ensure there is capacity in case of failure.
- C. Disable HA reservations to ensure that VMS are powered on using best effort during a disaster,
- D. Create a protection domain and add the AppVolumes VM entities to it. Set up a schedule to replicate the VMS every 60 minutes.

ANSWER: A

Explanation:

Create a storage container in both the primary and DR data centers for the Writable AppVolumes, then set up asynchronous DR between the two sites. Writable AppVolumes are user-specific VMDK-based disks that retain user-installed applications and profile-related data. Because these disks reside on Nutanix storage, their recovery depends on replicating the storage container data to the recovery site rather than relying only on the availability configuration of the compute cluster.

Nutanix asynchronous disaster recovery replicates protected data from a primary site to a configured remote site on a schedule. This establishes recovery copies of the Writable AppVolumes at the DR location and provides a defined recovery point objective based on the replication frequency. During a site disaster, the administrator can activate the replicated data at the remote site so the App Volumes environment can access the recovered writable disks when the corresponding desktop resources are brought online. Creating the appropriate storage containers at both sites and configuring asynchronous replication therefore aligns the AppVolumes storage layout with Nutanix's native cross-site DR workflow. Nutanix discusses App Volumes storage on Nutanix in its [VMware App Volumes on Nutanix](#) overview, and its [VMware App Volumes best-practices guide](#) documents the relevant deployment considerations.

QUESTION NO: 11

An administrator is configuring an application server to access a Nutanix Volume Group by using iSCSI. The application requires resilient storage connectivity from the guest operating system.

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

- A. Configure MPIO in the guest operating system
- B. Connect the iSCSI initiator through multiple available target paths
- C. Create a distributed Files share for the application
- D. Install the Nutanix AHV MCS Plug-in on the application server

ANSWER: A B

Explanation:

Configure MPIO in the guest operating system and **connect the iSCSI initiator through multiple available target paths** are correct. Multipath I/O allows the guest operating system to use more than one path to the presented Volume Group. If an individual path becomes unavailable, I/O can continue over another configured path.

The iSCSI initiator must be configured with the target information supplied for the Volume Group, and all intended paths should be discovered and connected. Creating a Files share or installing the AHV MCS Plug-in does not establish resilient iSCSI access for a Volume Group. Nutanix describes Volume Group and iSCSI configuration in the [Prism Web Console Guide](#).

QUESTION NO: 12

After configuring Smart DR, an administrator is unable to see the policy in the Policies tab. The administrator has confirmed that all FSVMs are able to connect to Prism Central via port 9440 bidirectionally. What is the possible reason for this issue?

- A. The primary and recovery file servers do not have the same version.
- B. Port 7515 should be open for all External/Client IPs of FSVMs on the Source and Target cluster.
- C. The primary and recovery file servers do not have the same protocols.
- D. Port 7515 should be open for all Internal/Storage IPs of FSVMs on the Source and Target cluster.

ANSWER: B

Explanation:

Port 7515 should be open for all External/Client IPs of FSVMs on the Source and Target cluster. Smart DR requires communication between the FSVMs at both sites in addition to each file server's connectivity with Prism Central. Port 9440 provides the Prism Central management/API path, so successful bidirectional communication on that port confirms only one part of the Smart DR connectivity prerequisites. It does not establish the required FSVM-to-FSVM Smart DR communication path.

The Smart DR service uses TCP port 7515 through the FSVM external/client network addresses. Therefore, firewall or network-security rules must permit bidirectional TCP 7515 connectivity between every source FSVM external IP address and every target FSVM external IP address. If that connectivity is unavailable, policy-related operations cannot be completed and synchronized correctly, which can result in the configured policy not being displayed in the Policies tab. Administrators should validate the complete mesh of required flows—not merely a single FSVM pair—and ensure that intermediate firewalls, ACLs, and security groups allow the traffic in both directions. Nutanix publishes Files networking and feature requirements in its [product documentation](#) and maintains current product documentation through the [Nutanix Support Portal documentation library](#).

QUESTION NO: 13

An administrator is configuring a Nutanix Files share that will contain financial records subject to a regulatory retention requirement. Files written to the share must not be modified or deleted until the configured retention period expires.

Which Files capability should the administrator enable?

- A. File Lock
- B. Advanced File Replication
- C. Distributed share
- D. Shadow Copies

ANSWER: A

Explanation:

File Lock is correct because it provides write-once, read-many (WORM) protection for files stored on a Nutanix Files share. After a file is locked, users cannot alter or delete it until its retention period has expired. This helps organizations preserve records in an immutable state to meet retention and compliance requirements.

Share permissions continue to determine who can access the files, but permissions alone do not prevent authorized users from changing or deleting data. File Lock adds the retention enforcement needed for this use case. Nutanix Files documentation is available from the [Nutanix Files documentation portal](#).