

Nutanix Certified Professional Unified Storage (NCP-US) v6.10

Nutanix NCP-US-6.10

Version Demo

Total Demo Questions: 9

Total Premium Questions: 97

Buy Premium PDF

<https://passqueen.com>

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Nutanix Unified Storage	8
Topic 2, Nutanix Files	20
Topic 3, Nutanix Objects	5
Topic 4, Nutanix Volumes	4
Topic 5, Data Protection	9
Topic 6, Mix Questions	51
Total	97

QUESTION NO: 1

What are the two types Of Launchpads that exist in Frame? (Choose two.)

- A. Application Launchpad
- B. user Launchpad
- C. Desktop Launchpad
- D. VDI Launchpad

ANSWER: A C

Explanation:

Nutanix Frame provides two Launchpad types: Application Launchpad and Desktop Launchpad. An Application Launchpad presents users with a curated set of published applications. After authentication, users select an available application tile and Frame starts that application in a provisioned workload session. This model is suited to delivering individual business applications while maintaining centralized administration of the applications, images, and capacity used to run them.

A Desktop Launchpad provides access to a full desktop experience rather than an application-selection portal. It is used when users need a complete Windows desktop session, including the desktop environment and the applications made available through the underlying Frame workload configuration. Both Launchpad types are configured and managed in the Frame administration console and provide the user-facing entry point for the associated account and its capacity resources. Nutanix Frame documentation describes these Launchpad types and their intended user experiences in its Launchpads administration guide: [Frame Launchpads documentation](#). For broader Frame product and deployment information, see [Nutanix Frame](#).

QUESTION NO: 2

A new client has just deployed a new Frame account, During the testing phase, the security team found that they had bidirectional clipboard, capabilities, the ability to transfer files, and connectivity to unauthorized external storage devices.

What should the administrator do to secure the environment, based on the security team's feedback?

- A. Apply Group Policies to limit the end users abilities.
- B. Implement a Mobile Device Management solution.
- C. Disable unauthorized storage providers and features.
- D. Deploy a device visibility & control platform.

ANSWER: C

Explanation:

Disable unauthorized storage providers and features. In a Nutanix Frame environment, clipboard redirection, file transfer, and external-storage access are user-session capabilities that must be governed through Frame's account and workload security configuration. The findings show that data can move both into and out of the hosted desktop or application session through several channels. The administrator should therefore apply a least-privilege configuration: disable bidirectional clipboard access where it is not required, restrict file-upload and download functionality, and allow only approved storage-provider integrations. This directly reduces the risk of unapproved data exfiltration, malware introduction, and use of personal or unmanaged storage services while preserving access paths specifically approved by the organization. These controls should be set at the appropriate Frame account or workload scope and validated using a standard user session after the policy is applied. Nutanix Frame is designed to deliver apps and desktops securely from centralized infrastructure, making session-control settings an important part of the organization's overall data-protection posture. See the [Nutanix Frame documentation](#) and the [Nutanix Frame product overview](#) for Frame administration and security information.

QUESTION NO: 3

A group of developers are migrating from physical computers to persistent virtual desktops.

What is the recommended migration path?

- A. Deploy a base image and provision required hosted applications
- B. Deploy non-persistent desktops and install required applications.
- C. Convert the physical computers to virtual desktops,
- D. Convert the developers profile to a roaming profile.

ANSWER: C

Explanation:

Convert the physical computers to virtual desktops, is the recommended path when developers move from physical endpoints to persistent virtual desktops and need continuity of their established workstation environments. A physical-to-virtual conversion captures the operating system, installed development tools, local configuration, user customizations, and project-related settings in a virtual-machine disk. That disk can then be prepared as a supported virtual desktop image and used to deliver a persistent desktop, where the assigned user retains changes across sessions. This approach is especially appropriate for developers because their workstations commonly contain specialized IDEs, SDKs, compilers, dependencies, extensions, and individualized configuration that would be time-consuming and potentially disruptive to recreate manually. After conversion, administrators should validate the guest operating system and drivers for the target hypervisor, install the required virtual desktop/Frame guest components, and confirm that the resulting image meets organizational security and image-management standards. Nutanix Frame documents the persistent-desktop model and its use for desktops that preserve user-installed applications and changes; its image-management guidance also describes preparing and maintaining workload images. See the [Nutanix Frame persistent desktops documentation](#) and [Nutanix Frame image management documentation](#).

QUESTION NO: 4

An administrator wants to allow Citrix MCS integration with AHV.

Which component needs to be installed and where should it be deployed?

- A. Nutanix AHV MCS Plug-in on Citrix XenDesktop DC
- B. Citrix Desktop DC Plug-in on Prism Element
- C. Nutanix AHV MCS Plug-in on Prism Central
- D. Citrix MCS AHV Plug-in on AHV

ANSWER: A

Explanation:

Nutanix AHV MCS Plug-in on Citrix XenDesktop DC is correct. Citrix Machine Creation Services requires the Nutanix AHV plugin to be installed on each Citrix Delivery Controller that will create or manage machine catalogs using Nutanix AHV. In current Citrix terminology, XenDesktop Delivery Controllers are called Citrix Virtual Apps and Desktops Delivery Controllers. The plugin supplies the integration layer that lets the Citrix control plane use Nutanix AHV as a hosting resource for MCS provisioning operations, including creating and managing the virtual machines used by catalog workloads. During configuration, the administrator adds the Nutanix hosting connection in Citrix Studio and provides the appropriate Nutanix cluster and Prism Element connection details. Installing the plugin on the Delivery Controller ensures that the Citrix services responsible for catalog provisioning can access the Nutanix-specific provider functionality. Nutanix documents this requirement for Citrix Virtual Apps and Desktops on AHV, and Citrix documents Nutanix AHV as a supported hosting platform for machine provisioning. See the [Nutanix Citrix Virtual Apps and Desktops on AHV technical note](#) and [Citrix provisioning documentation](#).

QUESTION NO: 5

An administrator has created a Nutanix Files share for a finance department. The finance manager must be able to grant access to project folders without receiving full administrative access to the Files cluster.

Which capability should the administrator configure?

- A. Self-service restore and share management delegation
- B. Prism Element cluster administrator access
- C. Object bucket owner access
- D. iSCSI initiator access

ANSWER: A

Explanation:

Self-service restore and share management delegation is correct because Nutanix Files supports delegated administration for appropriate file-service tasks. Delegation allows designated administrators to manage authorized share-level functions without granting them full control of the Nutanix cluster or the complete Files deployment.

This approach follows least-privilege practices by separating file-share administration from infrastructure administration. The finance manager can be assigned the necessary authorization for the relevant share scope, while cluster configuration, upgrades, and broader storage administration remain under the responsibility of the Nutanix administrator. See the [Nutanix Files documentation](#) for share and access-management guidance.

QUESTION NO: 6

An administrator is planning a Nutanix Files deployment for Citrix user profiles.

Which two characteristics make a Files distributed share appropriate for this workload? (Choose two.)

- A. Scale-out SMB capacity
- B. Load distribution across file server resources
- C. VM-level CPU scheduling
- D. Automatic conversion of profiles to VMDK files

ANSWER: A B

Explanation:

Scale-out SMB capacity and **load distribution across file server resources** are correct. A distributed share is designed to use the scale-out architecture of a Nutanix Files deployment. It can distribute client connections and file operations across the available file server resources, which is useful for a Citrix profile workload with many concurrent user logons.

Citrix profile stores commonly generate simultaneous SMB operations during logon and logoff periods. A distributed share helps the administrator provide a scalable location for those profile data operations while avoiding dependence on a single file-server resource. Storage containers and Prism Central reports do not provide SMB client load distribution. See the [Nutanix Files overview](#) for Files scale-out file service capabilities.

QUESTION NO: 7

A compliance team needs visibility into file activity, including which users accessed sensitive files and which files contain personally identifiable information.

Which Nutanix capability should the administrator use?

- A. File Analytics
- B. Prism Central Capacity Runway
- C. Volume Group snapshots
- D. Shadow Clones

ANSWER: A

Explanation:

File Analytics is correct because it provides visibility into file data, user activity, access patterns, and data classification within a Nutanix Files environment. The administrator can use File Analytics to investigate file activity and identify sensitive information according to configured classification policies.

This capability helps organizations understand where sensitive data resides and how it is being used, supporting governance and compliance workflows. A Files share provides client data access, but it does not provide the same analytics and classification functionality. See the [Nutanix Files overview](#) and the [Nutanix Files documentation](#).

QUESTION NO: 8

An administrator is preparing Nutanix Files for use with an existing Microsoft Active Directory environment.

Which two items should be available before joining the Files deployment to the domain? (Choose two.)

- A. Active Directory domain credentials with permission to join computers
- B. DNS resolution for the Active Directory domain controllers
- C. A vCenter Server registration
- D. An S3 access key and secret key

ANSWER: A B

Explanation:

Active Directory domain credentials with permission to join computers and **DNS resolution for the Active Directory domain controllers** are correct. Nutanix Files must communicate with the Active Directory domain controllers during the domain-join process. The credentials used must have sufficient privileges to create or join the required computer accounts in the domain.

Correct DNS resolution is also essential because the Files deployment uses DNS to locate domain controllers and related Active Directory services. A vCenter Server is not required for a Files deployment on AHV, and an S3 access key is used for object-storage access rather than an Active Directory join. See the [Nutanix Files documentation](#) for directory-service configuration guidance.

QUESTION NO: 9

An administrator is designing a Nutanix Files solution for users in two data centers.

The users must access their local Files deployment, and the same departmental data must remain available at both locations.

Which two design considerations are required? (Choose two.)

- A. Configure a replication relationship for the required shares.
- B. Direct users to the local Files access path at each site.

C. Use one shared IP address for both Files deployments.

D. Create a Volume Group for each user profile.

ANSWER: A B

Explanation:

Configure a replication relationship for the required shares and **direct users to the local Files access path at each site** are correct. A replication relationship keeps the required share data synchronized between the Files deployments. Directing users to the local share path ensures that users access the local Files cluster at the data center where they are working.

Using one shared IP address for both independent Files deployments would not provide site-aware local access. A Volume Group is block storage and is not used to replicate SMB home-directory or profile data between Files deployments. See the [Nutanix Files overview](#).