PassQueen
a.k.a dumpsqueen.com

Nutanix Certified Professional – Unified Storage (NCP-US) v6 exam

Nutanix NCP-US

Version Demo

Total Demo Questions: 18

Total Premium Questions: 185

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Storage Concepts and Architecture	22
Topic 2, Nutanix Files	62
Topic 3, Nutanix Objects	32
Topic 4, Nutanix Volumes	17
Topic 5, Data Protection and Disaster Recovery	9
Topic 6, Mix Questions	43
Total	185

QUESTION NO: 1

An administrator configured WORM on an existing Objects bucket at 4 p.m. on Monday. During the configuration, the administrator did not select Enable Version. At 8 a.m. the next morning, a ticket was submitted to update the bucket to include versioning.

What are the correct steps to make the requested change?

A. Create a bucket with Enable Version selected and migrate all data since versioning cannot be changed immediately after WORM is enabled.

B. Create a new' bucket with Enable Version selected and migrate all data since versioning cannot be changed after 12 hours once WORM is enabled.

C. Disable WORM and reconfigure with Enable Version and Enable WORM checked as it has been less than 24 hours since WORM was enabled.

D. update the WORM settings to Enable Version as that setting can be turned on at any point after WORM is enabled.

ANSWER: C

Explanation:

Disable WORM and reconfigure with Enable Version and Enable WORM checked as it has been less than 24 hours since WORM was enabled. is correct because the request arrives only 16 hours after WORM was enabled. Nutanix Objects provides a 24-hour window after WORM activation during which the WORM configuration can be disabled. This grace period allows the administrator to correct an initial WORM configuration before it becomes permanent. After disabling WORM, the administrator can edit the bucket configuration, select *Enable Version*, and then enable WORM again. Enabling versioning as part of the renewed WORM configuration ensures that object versions are retained and can be governed by the bucket's immutability policy. The elapsed time is important: the change must be completed while the bucket remains within the permitted 24-hour WORM-disable period. Nutanix describes the relationship between object versioning and data immutability, including the configuration considerations for WORM-protected buckets, in its Data Immutability and Versioning solution documentation. Additional Nutanix Objects product documentation is available through the Nutanix Support Portal.

QUESTION NO: 2

Which two network requirements must an administrator take into consideration for a new scale-out Files cluster when configuring and defining separate client and storage networks? (Choose two.)

A. The client and storage networks must have differentsubnet.

B. Ensure there is one IP address available for the storagenetwork.

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

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

ANSWER: A C

Explanation:

For a Nutanix Files scale-out deployment using separate client and storage networks, the client and storage networks must have differentsubnet. Separate subnets provide the required Layer 3 separation between client-facing file-service traffic and the internal storage communication used by the Files Storage VMs. This design lets each FSVM use the appropriate network path and IP configuration for its client and storage roles without overlapping address spaces or ambiguous routing.

Ensure the client and storage networks use a tagged VLAN is also required when these logically separate networks are carried over the same physical infrastructure. VLAN tagging identifies traffic belonging to each network, preserving network isolation while allowing the interfaces and uplinks to transport both client and storage traffic. The switch ports, AHV networking configuration, and VLAN IDs must be configured consistently so that FSVM traffic reaches the intended client or storage network.

These requirements should be planned before file-server creation, together with suitable IP pools and connectivity to supporting services such as DNS and Active Directory. Nutanix documents Files networking prerequisites and network-separation considerations in its Files network requirements documentation. Additional product architecture information is available on the Nutanix Files product page.

QUESTION NO: 3

The operations team have been tasked with increasing overall datacenter efficiency with a target minimum of 80% CPU, memory, and storage capacity utilization. They are requesting usage data from all application owners be sent on a monthly basis to be ingested into their capacity management software.

An administrator has an implementation of four Nutanix clusters under the management of a single Prism Central Instance.

How should the administrator best provide the data needed to the operations team to ensure adherence to the datacenter utilization directive?

A. Export the CPU Memory end Storage Usage metrics under Virtual Infrastructure/VMs in Prism Central and FTP the file to the operations team's FTP server.

B. Schedule a monthly email report with CPU, Memory, and Storage Usage data across all clusters under the Reporting facility in Prism Central.

C. Create a Metric Chart in Prism Central with CPU, Memory, and Storage usage across all clusters and export the data to be sent to the operations team,

D. Review the VM Efficiencies widget in Prism Central and export the data to a comma delimited file to be sent to the operations team.

ANSWER: B

Explanation:

Schedule a monthly email report with CPU, Memory, and Storage Usage data across all clusters under the Reporting facility in Prism Central. is the best approach because Prism Central provides centralized reporting for the clusters it manages. A report can be configured with the needed virtual-machine resource-consumption metrics and scoped across the managed environment, avoiding the need to collect usage independently from each of the four clusters. The reporting workflow also supports scheduled delivery, allowing the operations team to receive a consistent monthly dataset that can be imported into its capacity-management tooling. This directly supports ongoing measurement of CPU, memory, and storage utilization against the stated utilization target while making the process repeatable and operationally sustainable. Scheduled reporting also ensures that the information is generated from Prism Central's consolidated inventory and metrics history, giving the operations team a standard, recurring view of resource usage for the application estate. Nutanix documents the use of Prism Central reporting to create, schedule, and distribute customized reports in Nutanix Knowledge Base article 9168. Additional Prism Central documentation is available through the Nutanix Documentation Portal.

QUESTION NO: 4

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:

Public Network and **Private Network with VPN** are the valid Network Type choices available when creating a Frame account. Public Network is intended for environments in which users reach Frame workloads through the public internet. It provides the standard internet-accessible connectivity model for a Frame deployment and is appropriate when private enterprise-network connectivity is not required.

Private Network with VPN is designed for organizations that need Frame workloads to communicate securely with resources on an internal or otherwise private network. This model uses a VPN connection to extend network access between the Frame environment and the customer-controlled private network, supporting access to private applications, services, and data that should not be exposed through the public internet.

Selecting the network type during account creation establishes the intended connectivity architecture and is therefore an important early design decision. Nutanix Frame documentation describes these account-creation network choices and the associated connectivity approach. See the Nutanix Frame account creation documentation and the Nutanix Frame documentation portal for current deployment guidance.

QUESTION NO: 5

What are two types Of Frame environment delivery models? (Choose two.)

A. Frame on HP running Hyper-V.

B. Frame on Cisco LICS running VMware ESXi

C. BYO public cloud

D. Nutanix private cloud model running AHV

ANSWER: C D

Explanation:

Frame supports two principal environment delivery models: **BYO public cloud** and the **Nutanix private cloud model running AHV**. With BYO public cloud, an organization connects its own supported public-cloud subscription or account to Frame. Frame then orchestrates the capacity used for end-user desktops and applications in that customer-managed cloud environment, while providing its cloud-native control plane and consumption experience. This model is intended for organizations that want to use their existing public-cloud presence, accounts, and regional infrastructure choices.

The Nutanix private cloud model enables Frame workloads to run on Nutanix infrastructure using the AHV hypervisor. It allows organizations to deliver virtual applications and desktops from their own datacenter or private-cloud environment, while using Frame for streamlined provisioning, management, and access. Together, these models provide deployment flexibility for customers that require either public-cloud infrastructure under their own account or an on-premises/private-cloud implementation based on Nutanix AHV. Nutanix describes Frame as supporting deployments across public clouds and on Nutanix infrastructure. See the Nutanix Frame product page and the Nutanix Frame documentation portal.

QUESTION NO: 6

A RHEL administrator has requested a new NFS v4 export share to be deployed.

The task has been completed with the following settings:

• Authentication - System

• Default Access - Read-Write

Which mount—t nfs -o secoption should the RHEL administrator issue in order to properly mount the new share?

A. Krb5p

B. None

C. Sys

D. Krb5i

ANSWER: C

Explanation:

Sys is the appropriate security flavor because the Files NFS export was configured with System authentication. In Nutanix Files, System authentication uses the standard UNIX AUTH_SYS mechanism, also commonly written as the `sys` NFS security flavor. This mechanism supplies the client user's numeric UID and GID information to the NFS server, allowing access decisions to be made through normal UNIX-style identity and permission handling. The export's Read-Write default access setting governs the access level granted after the client has mounted successfully; it does not change the required NFS authentication flavor.

On the RHEL client, the administrator should therefore include `sec=sys` in the mount options, for example: `mount -t nfs -o vers=4,sec=sys fileserver:/share /mnt/share`. Explicitly specifying the security flavor is useful when ensuring that the client mount behavior matches the security setting selected for the Nutanix Files export. Red Hat documents `sys` as the default NFS security flavor and identifies the Kerberos flavors separately. See the Red Hat NFS mounting documentation and the Linux NFS mount options reference.

QUESTION NO: 7

Which two statements are true about object counts in an object store? (Choose two.)

A. Upload counts are included in the object counts at the bucket level.

B. each upload of a multipart upload is counted as a separate object.

C. Each upload of a multipart upload is counted as a separate object until the object is finalized.

D. upload counts are not included in the object counts at the bucket level,

ANSWER: A C

Explanation:

“Upload counts are included in the object counts at the bucket level.” is correct because bucket-level object accounting includes data associated with uploads that are currently in progress, not solely objects whose upload lifecycle has completed. This makes the reported count useful for observing the actual resources and object entries being handled by the bucket during active ingest activity.

“Each upload of a multipart upload is counted as a separate object until the object is finalized.” is also correct. Multipart upload workflows divide a single intended object into independently uploaded parts. While the multipart operation remains open, those uploaded parts are represented separately for object-count purposes. When the client completes the multipart upload, the service assembles the parts into the final object, and the temporary part-level representation no longer remains as separate finalized objects. This behavior is important when interpreting bucket counts during large-object uploads: counts can temporarily increase beyond the number of final business objects expected in the bucket.

For Nutanix Objects product information and documentation resources, see Nutanix Objects and Nutanix Documentation Portal.

QUESTION NO: 8

An administrator is configuring Object Lock for a Nutanix Objects bucket that contains regulatory records.

Which two retention modes can be used with Object Lock? (Choose two.)

A. Governance mode

B. Compliance mode

C. Archive mode

D. Replication mode

ANSWER: A B

Explanation:

Governance mode and **Compliance mode** are correct. Object Lock retention controls are used to help protect objects from deletion or modification for a defined retention period. Governance mode provides retention protection while allowing appropriately authorized users to bypass retention when necessary. Compliance mode provides stronger retention enforcement and prevents protected objects from being removed before the retention period expires.

Versioning and lifecycle policies can complement an Object Lock design, but they are not Object Lock retention modes. The administrator should select the mode that aligns with the organization's regulatory, legal, and operational requirements.

See the Nutanix Objects documentation portal for Object Lock and bucket data-protection guidance.

QUESTION NO: 9

An administrator is migrating a legacy iSCSI solution to Volumes and needs to reconfigure the iSCSI initiator in the Windows client devices.

What should the administrator understand about the client-side iSCSI configuration?

A. The Enable mufti-path option should be unchecked.

B. IP addresses of all CVMs should be entered.

C. The Nutanix MPIO drivers should be installed.

D. IP addresses of all FSVMs should be entered.

ANSWER: B

Explanation:

IP addresses of all CVMs should be entered. Nutanix Volumes presents block storage to guest operating systems through iSCSI, with the iSCSI target service provided by the Controller VMs in the Nutanix cluster. For resilient client connectivity, the Windows iSCSI Initiator should have a discovery portal configured for each CVM IP address in the cluster. This allows the initiator to discover the available target paths and supports continued access when an individual path or CVM is unavailable. In a Windows deployment, the native Microsoft Multipath I/O feature should also be enabled and configured for iSCSI so that the operating system can manage the multiple paths to the volume group appropriately. Entering every CVM address is therefore a core part of configuring redundant connectivity to Nutanix Volumes; these addresses are the storage-controller endpoints used by the iSCSI client, rather than file-server endpoints. Nutanix's guidance for Volumes emphasizes configuring the initiator with all CVM addresses and using multipathing for availability and path management. See the Nutanix Volumes overview at Nutanix Block Storage and the Nutanix documentation portal at Nutanix Support Portal.

QUESTION NO: 10

An administrator is upgrading Objects when the following error message is shown:

```
type[UPGRADE]:code: 500, message: error in processing pod: application post failed: image update
failed: unable to pull docker image 464585393164.dkr.ecr.us-west-2.amazonaws.com/nutanix-
msp/poseidon-zookeeper:buckets-1.0: err Max retries done: exit status 1 status_code: 500
```

type [UPGRADE] : code: 500, message: error in processing pod: application post failed: image update failed: unable to pull docker image 464585393164. dkr. com/nutanix— msp/poseidon-zookeeper:buckets—l.o: err Max retries done: exit status 1 status code: 500

How should the administrator resolve this error?

A. Manually upload the docker image to the bucket and rerun the upgrade.

B. Perform Inventory then upgrade MSP and Objects Manager vie LCM.

C. Manually upgrade Objects Manager to the latest version.

D. Upgrade and Objects service via LCM

ANSWER: D

Explanation:

Upgrade and Objects service via LCM is the appropriate resolution because Nutanix Lifecycle Manager is the supported workflow for obtaining, sequencing, and applying the compatible software payloads required by Nutanix Objects. The error identifies a container-image pull failure while an Objects pod is being updated. Running the Objects service upgrade through LCM ensures that the upgrade uses the correct Objects release bundle and coordinates the required Objects components and their container images as part of the managed lifecycle process. Before initiating the upgrade, the administrator should run an LCM inventory so that available compatible updates are discovered, then select the Objects service entity for upgrade and allow LCM to complete its prechecks and deployment workflow. The cluster must also retain the required network connectivity and name-resolution access for Nutanix-hosted update content during this process. This approach keeps the environment on a supported upgrade path and avoids bypassing LCM's dependency validation and update orchestration. Nutanix documents its Objects administration and lifecycle procedures through the product documentation available in the Nutanix Objects documentation portal; LCM documentation is available from the Nutanix Lifecycle Manager documentation portal.

QUESTION NO: 11

An administrator needs to deploy a Files cluster, create shares and make sure that users cannot upload any infected files to the shares.

Which configuration will fulfill this requirement?

A. NFS share with ICAP server integration.

B. SMB share with ICAP server integration

C. NFS share with File Analytics deployed.

D. SMB share with File Analytics deployed.

ANSWER: B

Explanation:

SMB share with ICAP server integration fulfills the requirement because Nutanix Files uses the Internet Content Adaptation Protocol (ICAP) to connect an SMB file share to a third-party antivirus scanning service. When a client writes a file to an ICAP-enabled SMB share, Files can submit the content to the configured ICAP server for inspection before allowing the write to complete. This provides an enforcement point that prevents files identified as infected from being stored in the share, rather than merely reporting on data after it has been written.

The administrator must configure a reachable, supported ICAP antivirus service and associate the ICAP configuration with the applicable SMB share. The antivirus engine and its signatures are maintained on the external ICAP server, while Nutanix Files provides the SMB file-serving and scan-request integration. This design allows malware scanning policy to be centrally managed in the security tool while protecting user uploads to the Files share. Nutanix Files documentation describes ICAP as its antivirus integration mechanism and identifies its use with SMB shares. See the Nutanix Files documentation and the Nutanix Files product overview.

QUESTION NO: 12

An organization plans to use Nutanix Files as the storage location for user home directories.

Which two controls can an administrator use to limit the amount of capacity consumed by users? (Choose two.)

A. User quotas

B. Directory quotas

C. Replication factor

D. Shadow Clones

E. Protection domain

ANSWER: A B

Explanation:

User quotas and **directory quotas** are appropriate controls for limiting capacity usage in Nutanix Files. A user quota restricts the amount of space consumed by an individual user. A directory quota applies a limit to a specified directory, which can be useful for departmental folders, project locations, or other shared data sets.

Replication factor is an AOS resiliency setting and does not enforce a logical consumption limit for a user or directory. Shadow Clones optimize shared read behavior for virtual-machine workloads and are unrelated to Files capacity quotas. A protection domain provides data-protection management for supported workloads rather than Files user-space limits. Nutanix Files administration guidance is available in the Nutanix Files documentation portal.

QUESTION NO: 13

What are two primary purposes of a Frame utility Server? (Choose two.)

A. Backend for a client-server application

B. shared file server

C. Test and develop virtual desktops.

D. A server that monitors virtual desktop usage

ANSWER: A B

Explanation:

A Frame utility server is a standalone, general-purpose Windows Server instance deployed alongside a Frame account. It is intended to provide supporting services that should remain available independently of individual user desktops and their session lifecycle. Using it as a **Backend for a client-server application** is a primary use case because line-of-business applications often require a persistent server-side component, such as an application service or database-adjacent service, while users access the client portion from Frame workloads.

Operating a **shared file server** is also a core utility-server use case. A utility server can host shared data that must be accessible to multiple Frame users or virtual desktops, giving the environment a centralized location for common files rather than coupling shared storage to a particular user session. This design helps keep supporting infrastructure separate from desktop images and user workloads. Nutanix documents utility servers as versatile Windows servers for services including client-server application back ends and file sharing. See the Nutanix Frame Utility Servers documentation and the Nutanix Frame documentation portal for deployment and administration guidance.

QUESTION NO: 14

The Files administrator has received reports from users in the accounting department that they can see folders that they don't have permission to access. The accounting department manager has requested that employees should only be able to see folders that they have permission to access.

How would a Files administrator ensure that users in theaccountingshare can only see folders they have permission to access?

A. Remove read-only access to shares users should not access.

B. Enable Access-Based Enumeration on the accounting share.

C. Enable Access-Based Enumeration on the File Sewer.

D. Remove File Blocking on the accounting shares.

ANSWER: B

Explanation:

Enable Access-Based Enumeration on the accounting share. Access-Based Enumeration (ABE) is designed for precisely this SMB-share visibility requirement: it evaluates the requesting user's effective permissions and hides files and folders that the user cannot access from directory listings. Users retain visibility only of the folders for which their assigned NTFS/ACL permissions grant access. This reduces confusion for accounting users, avoids exposing the names of restricted folders, and lets the administrator maintain access control through the existing permissions model rather than altering permissions merely to change what appears in a browse list.

In Nutanix Files, ABE is configured at the SMB share level, which permits the administrator to apply the requirement specifically to the accounting share without changing folder visibility behavior for unrelated shares. The underlying folder permissions must still be configured correctly; ABE uses those permissions when deciding which objects to enumerate for each user. This is consistent with Microsoft's description of ABE as filtering displayed files and folders according to the user's access rights. See Microsoft's Access-Based Enumeration documentation and the Nutanix Files documentation for Access-Based Enumeration.

QUESTION NO: 15

An administrator needs to deploy a Files cluster, create shares and make sure that users cannot upload any infected files to the shares.

Which configuration will fulfill this requirement?

A. NFS share with ICAP server integration.

B. SMB share with ICAP server integration.

C. NFS share with File Analytics deployed.

D. SMB share with File Analytics deployed.

ANSWER: B

Explanation:

SMB share with ICAP server integration fulfills the requirement because Nutanix Files uses the Internet Content Adaptation Protocol (ICAP) to integrate an external antivirus or malware-scanning service with SMB file shares. When a user attempts to write a file to an SMB share protected by an ICAP policy, Files submits the content to the configured ICAP server for inspection. The scan result is used to enforce the configured malware-protection behavior, allowing the environment to prevent infected content from being written to the share. This provides the required protection at the file-service layer while retaining the central antivirus engine and signature management of the organization's chosen ICAP-compatible security product. The Files antivirus integration is specifically designed around SMB share protection, so the share must be created as an SMB share and associated with the ICAP configuration. Nutanix describes Files as its scale-out file-storage service and documents antivirus protection as an ICAP-based Files capability. See the Nutanix Files product page and the Nutanix Files antivirus documentation.

QUESTION NO: 16

An administrator is configuring a Nutanix Files share for Linux application servers.

Which two protocols can Nutanix Files provide for client access? (Choose two.)

A. SMB

B. NFS

C. iSCSI

D. S3

E. Fibre Channel

ANSWER: A B

Explanation:

SMB and **NFS** are supported Nutanix Files client-access protocols. SMB is commonly used by Windows clients and applications, while NFS is commonly used by Linux and UNIX clients. Files can therefore provide centrally managed file services for environments with mixed operating systems.

iSCSI is a block-storage protocol associated with Nutanix Volumes rather than Files share access. S3 is the object-storage protocol provided by Nutanix Objects. Fibre Channel is not a Nutanix Files client-access protocol. Nutanix Files protocol support is described in the Nutanix Files product overview.

QUESTION NO: 17

A company is planning to implement Citrix Virtual Apps and Desktops on Nutanix clusters running AHV.

The initial implementation will be sized for 1000 virtual desktops with Windows 1 1, Microsoft Office 2021 and Adobe Creative Cloud All Apps installed.

What is the correct prerequisite to implement a successful installation of the Nutanix AHV MCS Plug-in?

A. Nutanix cluster virtual IP address is reachable.

B. Nutanix data services IP address is reachable.

C. The user running Nutanix AHV MCS installer must have administrator privileges on the Citrix Broker.

D. The user running Nutanix AHV MCS installer must have administrator privileges on the Citrix Storefront.

ANSWER: C

Explanation:

The user running Nutanix AHV MCS installer must have administrator privileges on the Citrix Broker. The Nutanix AHV MCS Plug-in is installed on Citrix Delivery Controllers, historically called Brokers, because it extends Citrix Machine Creation Services with the capability to communicate with Prism and provision or manage virtual desktops hosted on AHV. Installation modifies components and configuration on the Delivery Controller, so the installing account requires local administrative rights there. This permission is required to run the installer successfully and to register the plug-in components used by the Citrix site when creating a Nutanix hosting connection and catalog resources. In a production deployment, administrators should also ensure that the Delivery Controller can communicate with the relevant Prism management endpoint and that the account used later for the hosting connection has the required Nutanix RBAC permissions. Those are important environment and operational requirements, but local administrator privileges on the Citrix Broker are the stated prerequisite for executing the plug-in installation. Citrix identifies Delivery Controllers as the components that manage desktop and application resources and communicate with hosting infrastructure. See Citrix Delivery Controller installation documentation and the Nutanix and Citrix solution information.

QUESTION NO: 18

An administrator is provisioning Nutanix Volumes for two application servers. The administrator must ensure that only the approved servers can connect to the iSCSI block storage.

Which two configuration items are required? (Choose two.)

A. An iSCSI initiator group

B. The approved server initiator IQNs

C. An SMB share permission

D. An S3 access key

E. A Prism Central project

ANSWER: A B

Explanation:

An iSCSI initiator group and **the approved server initiator IQNs** are required to control which servers can connect to a Nutanix volume group. The initiator group contains the iSCSI initiator identities of authorized clients. Associating that group with the volume group restricts block-storage access to the listed initiators.

An SMB share permission controls access to Files shares and does not authorize iSCSI clients. An S3 access key is used for object-storage requests. A Prism Central project can provide administrative organization and governance, but it does not replace iSCSI initiator authorization. Nutanix documents initiator-group and volume-group configuration in the Nutanix Volumes documentation portal.