NCP-US$^{\text{Q\&As}}$

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

Pass Nutanix NCP-US Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/ncp-us.html

100% Passing Guarantee
100% Money Back Assurance

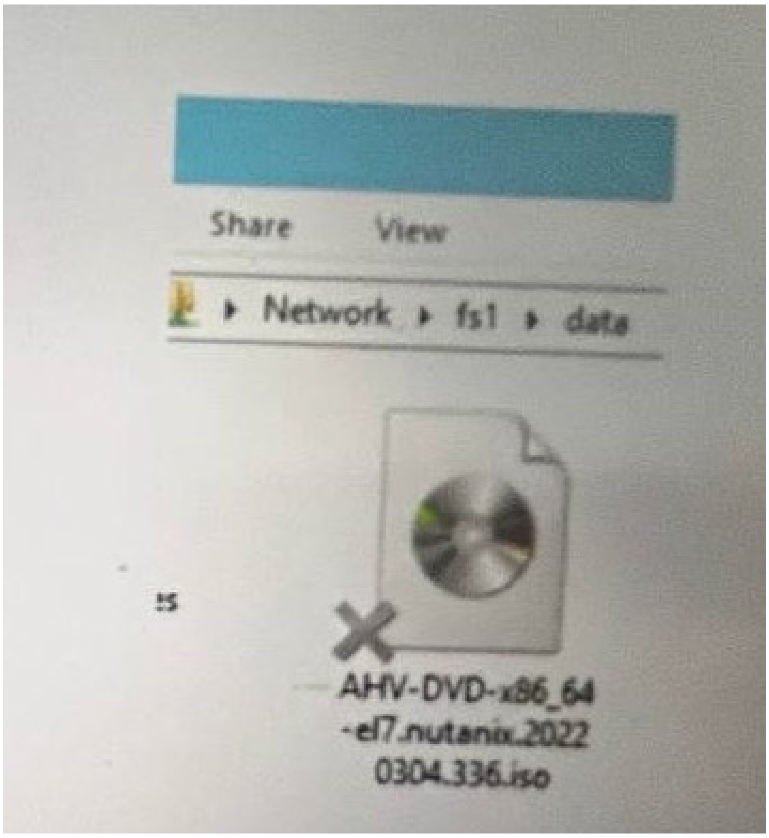
Following Questions and Answers are all new published by Nutanix Official Exam Center

- Instant Download After Purchase
- 100% Money Back Guarantee
- 365 Days Free Update
- 800,000+ Satisfied Customers

SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

Refer to the exhibit.



What does the `\\'X\\'\\' represent on the icon?

A. Share Disconnected File

B. Corrupt ISO

C. Distributed shared file

D. Tiered File

Correct Answer: C

The "X" on the icon represents a distributed shared file, which is a file that belongs to a distributed share or export. A distributed share or export is a type of SMB share or NFS export that distributes the hosting of top-level directories across multiple FSVMs. The "X" indicates that the file is not hosted by the current FSVM, but by another FSVM in the cluster. The "X" also helps to identify which files are eligible for migration when using the Nutanix Files Migration Tool. References: Nutanix Files Administration Guide, page 34; Nutanix Files Migration Tool User Guide, page 10

QUESTION 2

Which ransomware prevention solution for Files is best when the list of malicious file signatures to block is greater than 300?

A. Third-party solution

B. Flow Security Central

C. Data Lens

D. File Analytics

Correct Answer: A

Explanation: Nutanix Files provides a built-in ransomware prevention feature that allows administrators to block malicious file signatures from being written to the file system. However, this feature has a limit of 300 signatures per share or export. If the list of malicious file signatures to block is greater than 300, a third-party solution is recommended2. References: Nutanix Files Administration Guide2

QUESTION 3

An administrator is upgrading Files from version 3.7 to 4.1 in the highly secured environment the pre-upgrade check fail with below error:

FileServer preupgrade check failed with cause (s) Sub task poll timed out

What initial troubleshooting step should the administrator take?

A. Examine the failed tasks on the FSVMs

B. Check the there is enough disk space on FSVMs.

C. Verify connectivity between the FSVMs.

D. Increase upgrades timeout from ecli

Correct Answer: C

Explanation: One of the possible causes of a failed pre-upgrade check for Files is network connectivity issues between the FSVMs. The administrator should verify that there are no firewall rules or network policies that block the communication between the FSVMs on ports 22 (SSH), 9440 (HTTPS), and 2009 (RPC). The administrator can use tools such as ping, traceroute, and telnet to test the connectivity between the FSVMs. References: Nutanix Support Portal Troubleshooting Nutanix Files Upgrade Issues

QUESTION 4

Which Nutanix Unified Storage capability allows for monitoring usage for all Files deployment globally?

A. File Analytics

B. Nutanix Cloud Manager

C. Files Manager

D. Data Lens

Correct Answer: D

Explanation: Data Lens is a feature that provides insights into the data stored in Files across multiple sites, including different geographical locations. Data Lens allows administrators to monitor usage, performance, capacity, and growth trends for all Files deployments globally. Data Lens also provides reports on file types, sizes, owners, permissions, and access patterns3. References: Nutanix Data Lens Administration Guide3

QUESTION 5

Which protocols are supported by Files?

A. SMBv2 SMBv3, NFSv2, NFSv3

B. SMBv1. SMBv2, NFSv2, NFSv3

C. SMBv1. SMBv2, NFSv3, NFSv4

D. SMBv2 SMBv3, NFSv3, NFSv4

Correct Answer: D

Explanation: The protocols that are supported by Files are SMBv2, SMBv3, NFSv3, and NFSv4. SMB (Server Message Block) is a protocol that allows clients to access files, printers, and other resources on a network. NFS (Network File System) is a protocol that allows clients to access files on a remote server as if they were local. Files supports both SMB and NFS protocols for creating shares and exports that can be accessed by different types of clients. References: Nutanix Files Administration Guide, page 31; Nutanix Files Solution Guide, page 6

QUESTION 6

An administrator ha having difficulty enabling Data Lens for a file server.

What is the most likely cause of this issue?

A. The file server has blacklisted file types.

B. SSR is enabled on the file server.

C. The file server has been cloned.

D. The file server is in a Protection Domain.

Correct Answer: C

Explanation: The most likely cause of this issue is that the file server has been cloned. Cloning a file server is not a supported operation and can cause various problems, such as Data Lens not being able to enable or disable for the cloned file server. To avoid this issue, the administrator should use the scale-out feature to add more FSVMs to an existing file server, or create a new file server from scratch. References: Nutanix Files Administration Guide, page 28; Nutanix Files Troubleshooting Guide, page 11

QUESTION 7

An administrator has deployed a new Files cluster within a Windows Environment.

After some days, he Files environment is not able to synchronize users with the Active Directory server anymore. The administrator observes a large time difference between the Files environment and the Active Directory Server that is responsible for the behavior.

How should the administrator prevent the Files environment and the AD Server from having such a time difference in future?

A. Use the same NTP Servers for the File environment and the AD Server.

B. Use 0.pool.ntp.org as the NTP Server for the AD Server.

C. Use 0.pool.ntp.org as the NTP Server for the Files environment.

D. Connect to every FSVM and edit the time manually.

Correct Answer: A

Explanation: The administrator should prevent the Files environment and the AD Server from having such a time difference in future by using the same NTP Servers for the File environment and the AD Server. NTP (Network Time Protocol) is a protocol that synchronizes the clocks of devices on a network with a reliable time source. NTP Servers are devices that provide accurate time information to other devices on a network. By using the same NTP Servers for the File environment and the AD Server, the administrator can ensure that they have consistent and accurate time settings and avoid any synchronization issues or errors. References: Nutanix Files Administration Guide, page 32; Nutanix Files Troubleshooting Guide

QUESTION 8

An administrator has created a volume and needs to attach it to a windows host a via iSCSI. The data Services IP has been configured in the MS iSCSI Initiator, but no target are visible.

What is most likely the cause this issue?

A. The host\\' s IP address is not authorized to access the volume.

B. The CHAP password configured on the client is incorrect.

C. The CHAP Authentication has not been configured on the client.

D. The host\\'s IQN is not authorized to access to the volume.

Correct Answer: D

Explanation: Nutanix Volumes uses IQN-based authorization to control access to volumes. The administrator must specify the IQN of the host that needs to access the volume when creating or editing the volume. If the host\\'s IQN is not authorized, it will not be able to see the target in the MS iSCSI Initiator3. References: Nutanix Volumes Administration Guide3

QUESTION 9

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. Add File Services VM admin credentials to a MyNutanix account.

D. Configure the Data Services IP in Prism Central.

Correct Answer: AD

Explanation: The two steps that are required for enabling Data Lens are: In Prism, enable Pulse health monitoring: Pulse is a feature that collects diagnostic and usage information from Nutanix clusters and services and sends it to Nutanix for analysis and support purposes. Pulse health monitoring is a feature that monitors the health status of Nutanix clusters and services and sends alerts to Nutanix if any issues are detected. To enable Data Lens, Pulse health monitoring must be enabled in Prism Element or Prism Central. Configure the Data Services IP in Prism Central: Data Services IP is an IP address that is used for communication between Prism Central and Data Lens. Data Services IP must be configured in Prism Central before enabling Data Lens for any file server. Data Services IP must be routable from both Prism Central and Data Lens. References: Nutanix Files Administration Guide, page 93; Nutanix Data Lens Deployment Guide

QUESTION 10

A team of developers are working on a new processing application and requires a solution where they can upload the ... code for testing API calls. Older iterations should be retained as newer code is developer and tested.

A. Create an SMB Share with Files and enable Previous Version

B. Provision a Volume Group and connect via iSCSI with MPIO.

C. Create an NFS Share, mounted on a Linux Server with Files.

D. Create a bucket in Objects with Versioning enabled.

Correct Answer: D

Explanation: Nutanix Objects supports versioning, which is a feature that allows multiple versions of an object to be preserved in the same bucket. Versioning can be useful for developers who need to upload their code for testing API calls and retain older iterations as newer code is developed and tested. Versioning can also provide protection against accidental deletion or overwrite of objects. References: Nutanix Objects Administration Guide

QUESTION 11

ionization deployed Files in multiple sites, including different geographical locations across the globe. The organization has the following requirements to improves their data management lifecycle:

Provide a centralized management solution.

Automate archiving tier policies for compliance purposes.

Protect the data against ransomware.

Which solution will satisfy the organization\\'s requirements?

A. Prims Central

B. Data Lens

C. Files Analytics

Correct Answer: B

Explanation: Data Lens can provide a centralized management solution for Files deployments in multiple sites, including different geographical locations. Data Lens can also automate archiving tier policies for compliance purposes, by allowing administrators to create policies based on file attributes, such as age, size, type, or owner, and move files to a lower-cost tier or delete them after a specified period. Data Lens can also protect the data against ransomware, by allowing administrators to block malicious file signatures from being written to the file system. References: Nutanix Data Lens Administration Guide

QUESTION 12

What is the minimum and maximum file size limitations for Smart Tiering?

A. 64 KiB minimum and 15 TiB maximum

B. 128 IOB minimum and 5 TiB maximum

C. 64 KiB minimum and 5 TiB maximum

D. 128 KiB minimum and 13 TiB maximum

Correct Answer: C

Explanation: Smart Tiering is a feature that allows Files to tier data across different storage tiers based on the file size and access frequency. Smart Tiering supports files with a minimum size of 64 KiB and a maximum size of 5 TiB2. References: Nutanix Files Administration Guide2

QUESTION 13

An administrator needs to allow individual users to restore files and folders hosted in Files.

How can the administrator meet this requirement?

A. Configure a Protection Domain for the shares/exports.

B. Configure a Protection Domain on the FSVMs.

C. Enable Self-Service Restore on shares/exports.

D. Enable Self-Service Restore on the FSVMs.

Correct Answer: C

Explanation: Self-Service Restore (SSR) is a feature that allows individual users to restore files and folders hosted in Files without requiring administrator intervention. SSR can be enabled on a per-share or per-export basis, and users can access the snapshots of their data through a web portal or a Windows client application1. References: Nutanix Files Administration Guide1

QUESTION 14

A healthcare administrator configure a Nutanix cluster with the following requirements:

Enable for long-term data retention of large files Data should be kept for two years Deletion or overwrite of the data must not be allowed

Which Nutanix-enabled technology should the administrator employ to satisfy these requirements?

A. Files-Connected share

B. Files-Read-only share

C. Objects-WORM with versioning

D. Objects-Life Cycle Policy

Correct Answer: C

Explanation: The Nutanix-enabled technology that meets these requirements is Objects -WORM with versioning. WORM (Write-Once Read-Many) is a feature that prevents anyone from modifying or deleting data in a bucket while the policy is active. WORM policies help comply with strict data retention regulations that mandate how long specific data must be stored. Versioning is a feature that keeps multiple versions of an object in a bucket whenever it is overwritten or deleted. Versioning policies help preserve previous versions of an object for backup or recovery purposes. By enabling WORM and versioning for an Objects bucket, the administrator can ensure that data is kept for two years without being deleted or overwritten. References: Nutanix Objects User Guide, page 17; Nutanix Objects Solution Guide, page 9

QUESTION 15

What is a mandatory criterion for configuring Smart Tier?

A. VPC name

B. Target URL over HTTP

C. Certificate

D. Access and secret keys

Correct Answer: D

Explanation: Smart Tier requires access and secret keys to authenticate with the target storage tier, which can be Nutanix Objects or any S3-compatible storage service. The access and secret keys are generated by the target storage service and must be provided when configuring Smart Tier3. References: Nutanix Files Administration Guide3

NCP-US VCE Dumps NCP-US Study Guide NCP-US Braindumps