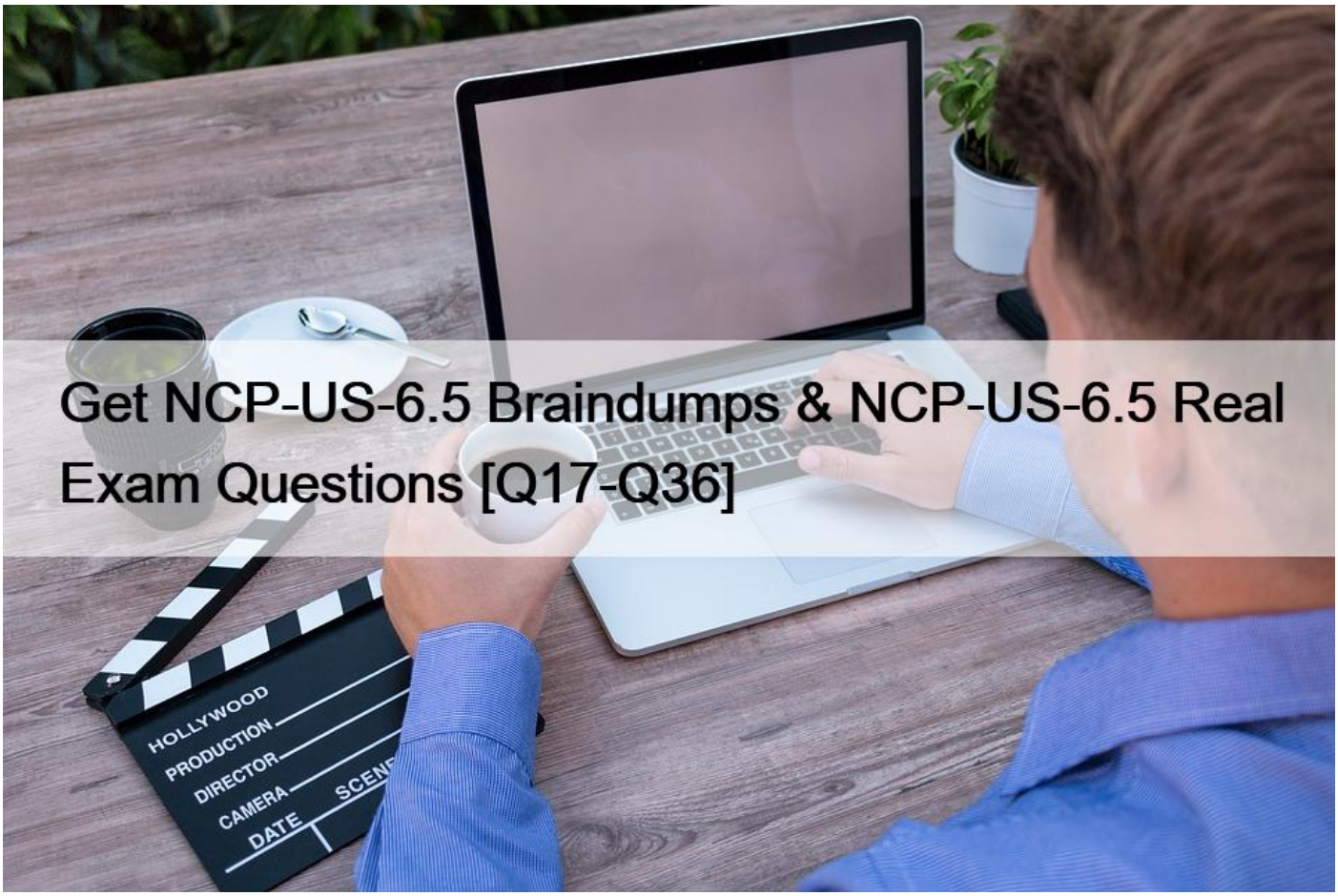
Get NCP-US-6.5 Braindumps & NCP-US-6.5 Real Exam Questions [Q17-Q36



Get NCP-US-6.5 Braindumps & NCP-US-6.5 Real Exam Questions
Nutanix NCP-US-6.5 Actual Questions and Braindumps

NEW QUESTION 17

Which two platform are currently supported for Smart Tiering? (Choose two.)
* Google Cloud Storage
* AWS Standard
* Wasabi
* Azure Blob

The two platforms that are currently supported for Smart Tiering are AWS Standard and Azure Blob. Smart Tiering is a feature that allows administrators to tier data from Files to cloud storage based on file age, file size, and file type. Smart Tiering can help reduce the storage cost and optimize the performance of Files. Smart Tiering currently supports AWS Standard and Azure Blob as the cloud storage platforms, and more platforms will be added in the future. Reference: Nutanix Files Administration Guide, page 99; Nutanix Files Solution Guide, page 11

NEW QUESTION 18

An administrator successfully installed Objects and was able to create a bucket.

When using the reference URL to access this Objects store, the administrator is unable to write data in the bucket when using an Action Directory account.

Which action should the administrator take to resolve this issue?
* Verify sharing policies at the bucket level.
* Reset the Active Directory user password.
* Replace SSL Certificates at the Object store level.
* Verify Access Keys for the user.

The action that the administrator should take to resolve this issue is to verify Access Keys for the user. Access Keys are credentials that allow users to access Objects buckets using S3-compatible APIs or tools. Access Keys consist of an Access Key ID and a Secret Access Key, which are used to authenticate and authorize requests to Objects. If the user is unable to write data in the bucket using an Active Directory account, it may be because the user does not have valid Access Keys or the Access Keys do not have sufficient permissions. The administrator can verify and manage Access Keys for the user in Prism Central. Reference: Nutanix Objects User Guide, page 13; Nutanix Objects Solution Guide, page 8

NEW QUESTION 19

Which scenario is causing the alert and need to be addressed to allow the entities to be protected?
* One or more VMs or Volume Groups belonging to the Consistency Group is part of multiple Recovery Plans configured with a Witness.
* One or more VMs or Volume Groups belonging to the Consistency Group may have been deleted
* The logical timestamp for one or more of the Volume Groups is not consistent between clusters
* One or more VMs or Volume Groups belonging to the Consistency Group contains state metadata

The scenario that is causing the alert and needs to be addressed to allow the entities to be protected is that one or more VMs or Volume Groups belonging to the Consistency Group may have been deleted. A Consistency Group is a logical grouping of VMs or Volume Groups that are protected together by a Protection Policy. A Protection Policy is a set of rules that defines how often snapshots are taken, how long they are retained, and where they are replicated for disaster recovery purposes. If one or more VMs or Volume Groups belonging to the Consistency Group are deleted, the Protection Policy will fail to protect them and generate an alert with the code AI303551 – VolumeGroupProtectionFailed. Reference: Nutanix Volumes Administration Guide, page 29; Nutanix Volumes Troubleshooting Guide

NEW QUESTION 20

What best describes the data protection illustrated in the exhibit?
* Smart DR
* Metro Availability
* Availability Zones
* NearSync

The data protection illustrated in the exhibit is Smart DR. Smart DR is a feature that allows share-level replication between active file server instances for disaster recovery. Smart DR can replicate shares from a primary FSI to one or more recovery FSIs on different clusters or sites. Smart DR can also perform failover and failback operations in case of a disaster or planned maintenance. The exhibit shows a Smart DR configuration with one primary FSI and two recovery FSIs. Reference: Nutanix Files Administration Guide, page 79; Nutanix Files Solution Guide, page 9

NEW QUESTION 21

An administrator has created a distributed share on the File cluster. The administrator connects to the share using Windows Explorer and starts creating folders in the share. The administrator observes that none of the created folder can be renamed as the company

naming convention requires.

How should the administrator resolve this issue?
* Use the Files MMC Snapln and rename the folders.
* Modify the Files shares to use the NFS protocol.
* Modify the read/write permissions on the created folders.
* Use the Microsoft Shared Folder MMC Snapln.

The administrator should resolve this issue by using the Files MMC Snap-in and renaming the folders. The Files MMC Snap-in is a tool that allows administrators to manage Files shares and exports from a Windows machine. The administrator can use the Files MMC Snap-in to connect to a distributed share or export and rename the top-level directories that are hosted by different FSVMs. Renaming the directories from Windows Explorer will not work because Windows Explorer does not recognize the distributed nature of the share or export and will try to rename all directories on the same FSVM, which will fail. Reference: Nutanix Files Administration Guide, page 35; Nutanix Files MMC Snap-in User Guide

NEW QUESTION 22

Which ransomware prevention solution for Files is best when the list of malicious file signatures to block is greater than 300?
* Third-party solution
* Flow Security Central
* Data Lens
* File Analytics

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. Reference: Nutanix Files Administration Guide2

NEW QUESTION 23

An administrator is looking for a tool that includes these features:

* Permission Denials

* Top 5 Active Users

* Top 5 Accessed Files

* File Distribution by Type

Nutanix tool should the administrator choose?
* File Server Manager
* Prism Central
* File Analytics
* Files Console

The tool that includes these features is File Analytics. File Analytics is a feature that provides insights into the usage and activity of file data stored on Files. File Analytics consists of a File Analytics VM (FAVM) that runs on a Nutanix cluster and communicates with the File Server VMs (FSVMs) that host the file shares. File Analytics can display various reports and dashboards that include these features:

Permission Denials: This report shows the number of permission denied events for file operations, such as read, write, delete, etc., along with the user, file, share, and server details.

Top 5 Active Users: This dashboard shows the top five users who performed the most file operations in a given time period, along with the number and type of operations.

Top 5 Accessed Files: This dashboard shows the top five files that were accessed the most in a given time period, along with the number of accesses and the file details.

File Distribution by Type: This dashboard shows the distribution of files by their type or extension, such as PDF, DOCX, JPG, etc., along with the number and size of files for each type. Reference: Nutanix Files Administration Guide, page 93; Nutanix File Analytics User Guide

NEW QUESTION 24

Which Data Lens feature maximizes the available file server space by moving cold data from the file server to an object store?
* Backup
* Versioning
* Smart Tier
* Smart DR

The Data Lens feature that maximizes the available file server space by moving cold data from the file server to an object store is Smart Tier. Smart Tier is a feature that allows administrators to tier data from Files to cloud storage based on file age, file size, and file type. Smart Tier can help reduce the storage cost and optimize the performance of Files. Smart Tier can move cold data, which is data that has not been accessed or modified for a long time, from the file server to an object store, such as AWS Standard or Azure Blob, and free up the file server space for hot data, which is data that is frequently accessed or modified. Reference: Nutanix Files Administration Guide, page 99; Nutanix Files Solution Guide, page 11

NEW QUESTION 25

An organization currently has two Objects instances deployed between two sites. Both instances are managed via manage the same Prism Central to simplify management.

The organization has a critical application with all data in a bucket that needs to be replicated to the secondary site for DR purposes. The replication needs to be asynchronous, including al delete the marker versions.
* Create a Bucket replication rule, set the destination Objects instances.
* With Object Browser, upload the data at the destination site.
* Leverage the Objects Baseline Replication Tool from a Linus VM
* Use a protection Domain to replicate the objects Volume Group.

The administrator can achieve this requirement by creating a bucket replication rule and setting the destination Objects instance. Bucket replication is a feature that allows administrators to replicate data from one bucket to another bucket on a different Objects instance for disaster recovery or data migration purposes. Bucket replication can be configured with various parameters, such as replication mode, replication frequency, replication status, etc. Bucket replication can also replicate all versions of objects, including delete markers, which are special versions that indicate that an object has been deleted. By creating a bucket replication rule and setting the destination Objects instance, the administrator can replicate data from one Objects instance to another asynchronously, including all delete markers and versions. Reference: Nutanix Objects User Guide, page 19; Nutanix Objects Solution Guide, page 9

NEW QUESTION 26

Before upgrading Files or creating a file server, which component must first be upgraded to a compatible version?
* FSM
* File Analytics
* Prism Central
* FSVM

The component that must first be upgraded to a compatible version before upgrading Files or creating a file server is Prism Central. Prism Central is a web-based user interface that allows administrators to manage multiple Nutanix clusters and services, including Files. Prism Central must be upgraded to a compatible version with Files before upgrading an existing file server or creating a new file server. Otherwise, the upgrade or creation process may fail or cause unexpected errors. Reference: Nutanix Files Administration Guide, page 21; Nutanix Files Upgrade Guide

NEW QUESTION 27

An organization currently has a Files cluster for their office data including all department shares. Most of the data is considered cold Data and they are looking to migrate to free up space for future growth or newer data.

The organization has recently added an additional node with more storage. In addition, the organization is using the Public Cloud for .. storage needs.

What will be the best way to achieve this requirement?
* Migrate cold data from the Files to tape storage.
* Backup the data using a third-party software and replicate to the cloud.
* Setup another cluster and replicate the data with Protection Domain.
* Enable Smart Tiering in Files within the File Console.

NEW QUESTION 28

What is a mandatory criterion for configuring Smart Tier?
* VPC name
* Target URL over HTTP
* Certificate
* Access and secret keys

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. Reference: Nutanix Files Administration Guide3

NEW QUESTION 29

An administrator has performed an AOS upgrade, but noticed that the compression on containers is not happening.

What is the delay before compression begins on the Files container?
* 30 minutes
* 60 minutes
* 12 hours
* 24 hours

The delay before compression begins on the Files container is 12 hours. Compression is a feature that reduces the storage space required for data by applying an algorithm that eliminates redundant or unnecessary bits. Compression can improve the storage efficiency and performance of Files. Compression is enabled by default on the Files container and runs in the background as a low-priority task. Compression does not start immediately after an AOS upgrade, but waits for 12 hours to avoid interfering with other high-priority tasks or operations. Reference: Nutanix Files Administration Guide, page 24; Nutanix Files Solution Guide, page 10

NEW QUESTION 30

Which two prerequisites are needed when deploying Objects to a Nutanix cluster? (Choose two.)

* Microsegmentation is enabled.
* Data Services IP is configured on the PI
* DNS is configured on the PE.
* AHV IPAM is disabled on the VLAN used for Objects.

Nutanix Objects requires a Data Services IP to be configured on the Prism Infrastructure (PI) cluster, which is used to expose the S3 API endpoint for accessing buckets and objects. Nutanix Objects also requires AHV IP Address Management (IPAM) to be disabled on the VLAN used for Objects, as Objects uses its own DHCP service to assign IP addresses to the Objects VMs1. Reference: Nutanix Objects Administration Guide1

NEW QUESTION 31

An administrator needs to ensure maximum performance, throughput, and redundancy for the company’s Oracle RAC on Linux implementation, while using the native method for securing workloads.

Which configuration meets these requirements?

* Flies with a distributed share and ABE
* Files with a general purpose share and File Blocking
* Volumes with MPIO and a single vDisk
* Volumes with CHAP and multiple vDisks

Volumes is a feature that allows users to create and manage block storage devices (volume groups) on a Nutanix cluster. Volume groups can be accessed by external hosts using the iSCSI protocol. To ensure maximum performance, throughput, and redundancy for Oracle RAC on Linux implementation, while using the native method for securing workloads, the recommended configuration is to use Volumes with MPIO (Multipath I/O) and a single vDisk (virtual disk). MPIO is a technique that allows multiple paths between an iSCSI initiator and an iSCSI target, which improves performance and availability. A single vDisk is a logical unit number (LUN) that can be assigned to multiple hosts in a volume group, which simplifies management and reduces overhead. Reference: Nutanix Volumes Administration Guide, page 13; Nutanix Volumes Best Practices Guide

NEW QUESTION 32

An administrator wants to provide security against ransomware attacks in Files. The administrator wants to configure the environment to scan files for ransomware in real time and provide notification in the event of a ransomware attack.

Which component should the administrator use to meet this requirement?

* File Analytics
* Syslog Server
* Files Console
* Protection Domain

File Analytics is a feature that provides insights into the data stored in Files, such as file types, sizes, owners, permissions, and access patterns. File Analytics also provides security against ransomware attacks by scanning files for ransomware in real time and providing notification in the event of a ransomware attack. File Analytics can detect ransomware based on file extensions, file signatures, or third-party solutions2. Reference: Nutanix File Analytics Administration Guide2

NEW QUESTION 33

An administrator needs to protect a Files cluster unique policies for different shares.

How should the administrator meet this requirement?

* Create a protection domain in the Data Protection view in Prism Element.
* Configure data protection polices in File Server view in Prism Element
* Create a protection domain in the Data Protection view in Prism Central.

* Configure data protection polices in the Files view in Prism Central.

The administrator can meet this requirement by configuring data protection policies in the Files view in Prism Central. Data protection policies are policies that define how file data is protected by taking snapshots, replicating them to another site, or tiering them to cloud storage. Data protection policies can be configured for each share or export in a file server in the Files view in Prism Central. The administrator can create different data protection policies for different shares or exports based on their protection needs and requirements. Reference: Nutanix Files Administration Guide, page 79; Nutanix Files Solution Guide, page 9

NEW QUESTION 34

An administrator is trying to create a Distributed Share, but the Use Distributed Share/Export type instead of Standard option is not present when creating the share.

What is most likely the cause for this?

* The file server does not have the correct license
* The cluster only has three nodes.
* The file server resides on a single node cluster.
* The cluster is configured with hybrid storage

The most likely cause for this issue is that the file server resides on a single node cluster. A distributed share is a type of SMB share or NFS export that distributes the hosting of top-level directories across multiple FSVMs, which improves load balancing and performance. A distributed share cannot be created on a single node cluster, because there is only one FSVM available. A distributed share requires at least two nodes in the cluster to distribute the directories. Therefore, the option to use distributed share/export type instead of standard is not present when creating a share on a single node cluster. Reference: Nutanix Files Administration Guide, page 33; Nutanix Files Solution Guide, page 8

NEW QUESTION 35

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?

* Use the same NTP Servers for the File environment and the AD Server.
* Use 0.pool.ntp.org as the NTP Server for the AD Server.
* Use 0.pool.ntp.org as the NTP Server for the Files environment.
* Connect to every FSVM and edit the time manually.

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. Reference: Nutanix Files Administration Guide, page 32; Nutanix Files Troubleshooting Guide

NEW QUESTION 36

An administrator has created a distributed share on the File cluster. The administrator connects to the share using Windows Explorer and starts creating folders in the share. The administrator observes that none of the created folder can be renamed as the company naming convention requires.

How should the administrator resolve this issue?

* Use the Files MMC Snapln and rename the folders.
* Use the Microsoft Shared Folder MMC Snapln.
* Modify the read/write permissions on the created folders.
* Modify the Files shares to use the NFS protocol.

The administrator should resolve this issue by using the Files MMC Snap-in and renaming the folders. The Files MMC Snap-in is a tool that allows administrators to manage Files shares and exports from a Windows machine. The administrator can use the Files MMC Snap-in to connect to a distributed share or export and rename the top-level directories that are hosted by different FSVMs. Renaming the directories from Windows Explorer will not work because Windows Explorer does not recognize the distributed nature of the share or export and will try to rename all directories on the same FSVM, which will fail. Reference: Nutanix Files Administration Guide, page 35; Nutanix Files MMC Snap-in User Guide