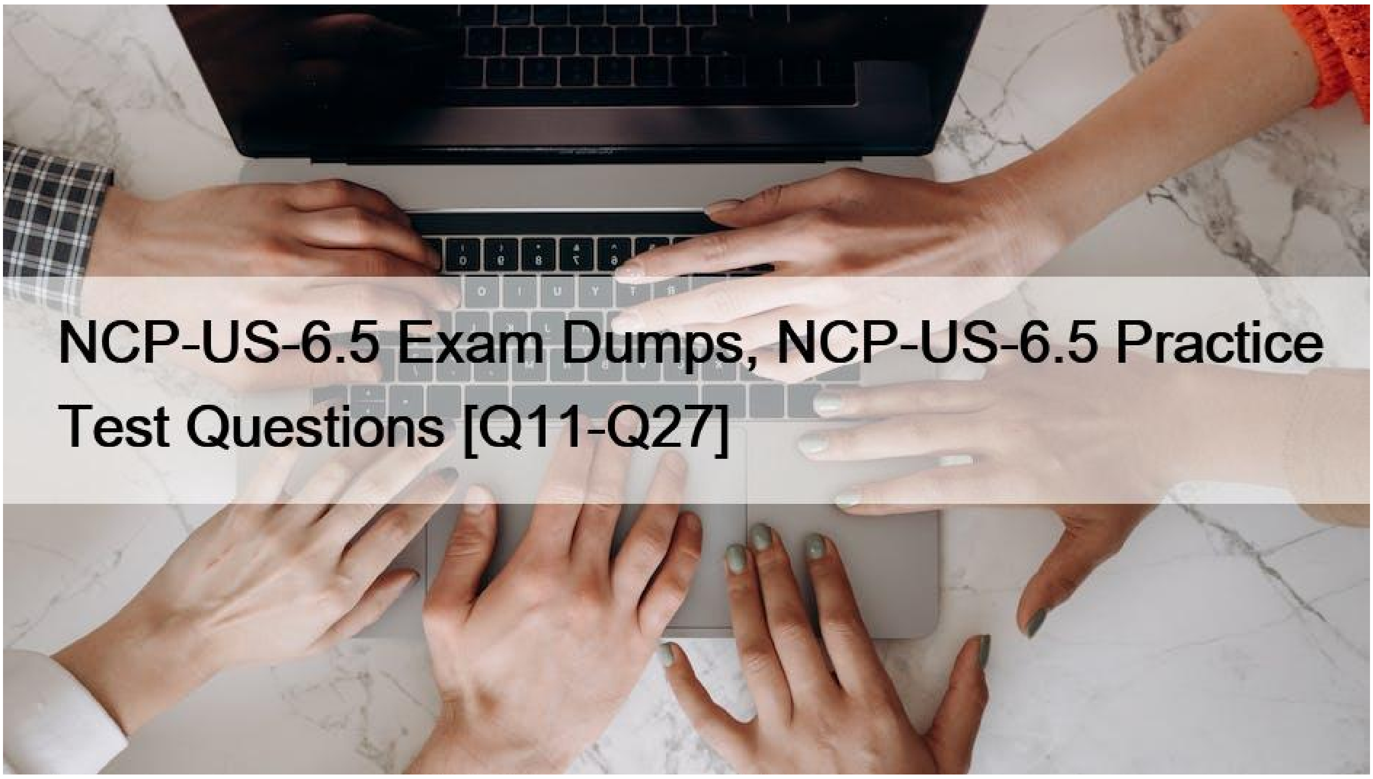
NCP-US-6.5 Exam Dumps, NCP-US-6.5 Practice Test Questions [Q11-Q27



NCP-US-6.5 Exam Dumps, NCP-US-6.5 Practice Test Questions
PDF (New 2024) Actual Nutanix NCP-US-6.5 Exam Questions

Nutanix NCP-US-6.5 Exam Syllabus Topics:

TopicDetailsTopic 1- Given a scenario, configure shares, buckets, and- or Volume Groups- Troubleshoot a failed upgrade for Files- ObjectsTopic 2- Configure Nutanix Objects- Describe how to monitor performance and usageTopic 3- Utilize File Analytics for data security- Troubleshoot Nutanix Unified Storage- Configure Nutanix VolumesTopic 4- Troubleshoot issues related to Nutanix Objects- Troubleshoot issues related to Nutanix VolumesTopic 5- Deploy and Upgrade Nutanix Unified Storage- Perform upgrades- maintenance for Files- Objects implementationsTopic 6- Troubleshoot issues related to Nutanix Files- Explain Data Management processes for Files and ObjectsTopic 7- Configure and Utilize Nutanix Unified Storage- Identify the steps to deploy Nutanix Objects

QUESTION 11

An administrator needs to ensure maximum performance, throughput, and redundancy for the company&#8217;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

QUESTION 12

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

QUESTION 13

An administrator is attempting to create a share that will provide user access via SMB and NFS. However, the Enable multiprosotocol accounts for NFS clients settings is not available.

What would cause this issue?

* The connection to Active Directory has not been configured.
* The file server instance was only configured with SMB.
* The incorrect Files license has been applied.
* NFS configured to use unmanaged authentication.

The cause of this issue is that the connection to Active Directory has not been configured. Active Directory is a service that provides centralized authentication and authorization for Windows-based clients and servers. To create a share that will provide user access via SMB and NFS, the administrator must first configure the connection to Active Directory in the Files Console. This will allow the administrator to enable multiprotocol accounts for NFS clients, which are accounts that map NFS users to SMB users and groups for consistent access control across both protocols. Reference: Nutanix Files Administration Guide, page 32; Nutanix Files Solution Guide, page 6

QUESTION 14

An administrator wants to monitor their Files environment for suspicious activities, such mass deletion or access denials.

How can the administrator be alerted to such activities?

How can the administrator be alerted to such activities?

* Configure Alerts & Events in the Files Console, filtering for Warning severity.
* Deploy the Files Analytics VM. and configure anomaly rules.
* Configure Files to use ICAP servers, with monitors for desired activities.

* Create a data protection policy in the Files view in Prism Central.

The administrator can monitor their Files environment for suspicious activities, such as mass deletion or access denials, by deploying the File Analytics VM and configuring anomaly rules. 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 alert the administrator when there is an unusual or suspicious activity on file data, such as mass deletion, encryption, permission change, or access denial. The administrator can configure anomaly rules to define the threshold, time window, and notification settings for each type of anomaly.
Reference: Nutanix Files Administration Guide, page 93; Nutanix File Analytics User Guide

QUESTION 15

A team of developers are working on a new processing application and requires a solution where they can upload the &#8230; code for testing API calls. Older iterations should be retained as newer code is developer and tested.

* Create an SMB Share with Files and enable Previous Version
* Create a bucket in Objects with Versioning enabled.
* Provision a Volume Group and connect via iSCSI with MPIO.
* Create an NFS Share, mounted on a Linux Server with Files.

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.
Reference: Nutanix Objects Administration Guide

QUESTION 16

A team of developers are working on a new processing application and requires a solution where they can upload the &#8230; code for testing API calls. Older iterations should be retained as newer code is developer and tested.

* Create an SMB Share with Files and enable Previous Version
* Provision a Volume Group and connect via iSCSI with MPIO.
* Create an NFS Share, mounted on a Linux Server with Files.
* Create a bucket in Objects with Versioning enabled.

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.
Reference: Nutanix Objects Administration Guide

QUESTION 17

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

QUESTION 18

What is the binary image extension of File Analytics?

* JSON
* QCOW2
* ISO
* VMDK

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 is deployed as a VM on an AHV cluster using a QCOW2 binary image file that contains the File Analytics software and configuration3. Reference: Nutanix File Analytics Administration Guide3

QUESTION 19

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

QUESTION 20

An administrator is able to review and modify objects in a registered ESXI cluster from a PE instance, but when the administrator attempts to deploy an Objects cluster to the same ESXi cluster, the error that is shown in the exhibit is shown.

What is the appropriate configuration to verify to allow successful Objects cluster deployment to this ESXi cluster?

* Ensure that vCenter in PE cluster is registered using FQDN and that vCenter details in Objects UI are using FQDN.
* Replace the expired self-signed SSL certificate for the Object Store with a non-expired &#8216; signed by a valid Certificate Authority.
* Replace the expired self-signed SSL certificate for the Object Store with a non-expired self signed SSL certificate.
* Ensure that vCenter in PE cluster is registered using FQDN and that vCenter details in Objects UI are using IP address.

The appropriate configuration to verify to allow successful Objects cluster deployment to this ESXi cluster is to ensure that vCenter in PE cluster is registered using FQDN (Fully Qualified Domain Name) and that vCenter details in Objects UI are using FQDN. FQDN is a domain name that specifies the exact location of a host in the domain hierarchy. For example, esxi01.nutanix.com is an FQDN for an ESXi host. Using FQDN instead of IP addresses can avoid certificate validation errors when deploying Objects clusters to ESXi clusters. Reference: Nutanix Objects User Guide, page 9; Nutanix Objects Troubleshooting Guide, page 5

QUESTION 21

An administrator has been tasked with creating a distributed share on a single-node cluster, but has been unable to successfully complete the task.

Why is this task failing?

* File server version should be greater than 3.8.0

* AOS version should be greater than 6.0.
* Number of distributed shares limit reached.
* Distributed shares require multiple nodes.
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 task of creating a distributed share on a single-node cluster will fail. Reference: Nutanix Files Administration Guide, page 33; Nutanix Files Solution Guide, page 8

QUESTION 22

Which port is required between a CVM or Prism Central to insights,nutanix.com for Data Lens configuration?
* 80
* 443
* 8443
* 9440
Data Lens is a SaaS that provides file analytics and reporting, anomaly detection, audit trails, ransomware protection features, and tiering management for Nutanix Files. To configure Data Lens, one of the network requirements is to allow HTTPS (port 443) traffic between a CVM or Prism Central to insights.nutanix.com. This allows Data Lens to collect metadata and statistics from the FSVMs and display them in a graphical user interface. Reference: Nutanix Files Administration Guide, page 93; Nutanix Data Lens User Guide

QUESTION 23

Which action is required to allow the deletion of file server audit data in Data Lens?
* Enable the File Server.
* Disable the File Server.
* Update the data retention period.
* Configure the audit trail target.
The action that is required to allow the deletion of file server audit data in Data Lens is to update the data retention period. Data retention period is a setting that defines how long Data Lens keeps the file server audit data in its database. Data Lens collects and stores various metadata and statistics from file servers, such as file name, file type, file size, file owner, file operation, file access time, etc. Data Lens uses this data to generate reports and dashboards for file analytics and anomaly detection. The administrator can update the data retention period for each file server in Data Lens to control how long the audit data is kept before being deleted. Reference: Nutanix Files Administration Guide, page 98; Nutanix Data Lens User Guide

QUESTION 24

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

QUESTION 25

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

What is the most likely cause of this issue?
* The file server has blacklisted file types.
* SSR is enabled on the file server.
* The file server has been cloned.
* The file server is in a Protection Domain.
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. Reference: Nutanix Files Administration Guide, page 28; Nutanix Files Troubleshooting Guide, page 11

QUESTION 26

Users are complaining about having to reconnecting to share when there are networking issues.

Which files feature should the administrator enable to ensure the sessions will auto-reconnect in such events?
* Durable File Handles
* Multi-Protocol Shares
* Connected Shares
* Workload Optimization
The Files feature that the administrator should enable to ensure the sessions will auto-reconnect in such events is Durable File Handles. Durable File Handles is a feature that allows SMB clients to reconnect to a file server after a temporary network disruption or a client sleep state without losing the handle to the open file. Durable File Handles can improve the user experience and reduce the risk of data loss or corruption. Durable File Handles can be enabled for each share in the Files Console. Reference: Nutanix Files Administration Guide, page 76; Nutanix Files Solution Guide, page 10

QUESTION 27

An administrator has discovered that File server services are down on a cluster.

Which service should the administrator investigation for this issue?
* Minerva-nvm
* Sys_stats_server
* Cassandra
* Insights_collector
The service that the administrator should investigate for this issue is Minerva-nvm. Minerva-nvm is a service that runs on each CVM and provides communication between Prism Central and Files services. Minerva-nvm also monitors the health of Files services and reports any failures or alerts to Prism Central. If Minerva-nvm is down on any CVM, it can affect the availability and functionality of Files services on that cluster. Reference: Nutanix Files Administration Guide, page 23; Nutanix Files Troubleshooting Guide

Updated Aug-2024 Pass NCP-US-6.5 Exam - Real Practice Test Questions: https://www.braindumpsit.com/NCP-US-6.5_real-exam.html]