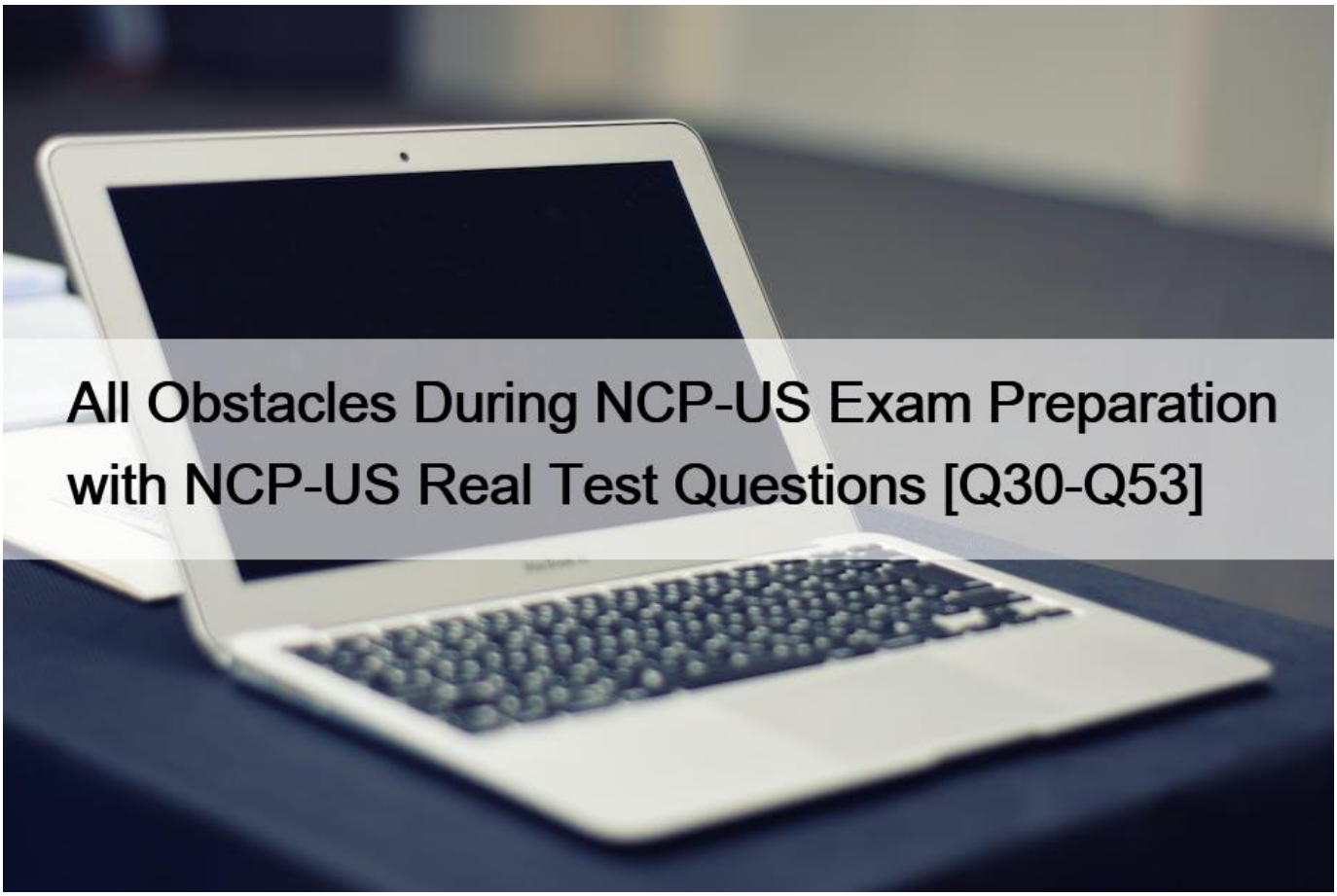
All Obstacles During NCP-US Exam Preparation with NCP-US Real Test Questions [Q30-Q53



All Obstacles During NCP-US Exam Preparation with NCP-US Real Test Questions Fully Updated Free Actual Nutanix NCP-US Exam Questions NO.30 During a recent audit, the auditors discovered several shares that were unencrypted. To remediate the audit item, the administrator enabled Encrypt SMB3 Messages on the accounting, finance, and facilities shares. After encryption was enabled, several users have reported that they are no longer able to access the shares.

What is causing this issue?
* The users are accessing the shares from Windows 8 desktops.
* Advanced Encryption Standard 128 & 256 are disabled in Windows 7.
* Advanced Encryption Standard 128 & 256 are disabled in Linux or Mac OS.
* The users are accessing the shares from Linux desktops.

According to Encryption-Files | Nutanix Community1, SMB3 message encryption is a feature that encrypts messages on the file server side and decrypts them on the client side. However, clients that do not support encryption (Linux, Mac, windows 7) cannot access a share with encryption enabled.

According to Nutanix Support & Insights2, Nutanix Files supports SMB3 encryption for SMB3 client-server traffic. This means that only clients that support SMB3 protocol can access encrypted shares.

Therefore, if the users are accessing the shares from Linux desktops, they will not be able to access them because Linux does not support SMB3 encryption.

https://portal.nutanix.com/page/documents/solutions/details?targetId=NVD-2151-Unified-Storage:client-server-traffic-encryption.html

NO.31 While preparing for migrating data from a legacy storage environment to a new Files scale-out file server, the administrator make the following notes:

Requirements:

Number of home directories: 4000

Number of Departmental shares: 1

Everyone is permitted to accessing it

All users use the same Departmental share

The administrator deploys Files using the following configuration:

Number of FSVMs: 3

VCPU & RAM/FSVM: 4VCPU,12GB

One Distributed share with SSR & ABE enabled for the Home Directories

One Standard share for the Departmental share

Does this configuration satisfy the project’s requirements?
* No, the project needs two distributed Share 4 FSVMs. 6 vCPU & 326B RAM
* Yes, the listed configuration elements satisfy the requirements.
* No, the project needs two distributed 4 FSVMs, 24 vcpu & 128GB RAM
* No, the project needs 4 FSVMs 4 vCPU & 12GB RAM.

According to the scenario, the administrator is preparing to migrate data from a legacy storage environment to a new Files scale-out file server in a way that meets the following requirements:

Number of home directories: 4000

Number of Departmental shares: 1

Everyone is permitted to access it

All users use the same Departmental share

The administrator deploys Files using the following configuration:

Number of FSVMs: 3

VCPU & RAM/FSVM: 4VCPU, 12GB

One Distributed share with SSR & ABE enabled for the Home Directories

One Standard share for the Departmental share

Based on this configuration, it appears that the project’s requirements are satisfied. The configuration provides a Distributed share for the home directories, which is recommended when there is a large number of files or directories, and this will distribute the load across multiple FSVMs. Note that everyone is permitted to access it.

In addition, the configuration provides a Standard share for the Departmental share, and since all users use the same Departmental share, this will not create any performance issues. Therefore, the correct answer is B, ‘Yes, the listed configuration elements satisfy the requirements’.

NO.32 An administrator needs to upgrade all the File Analytics deployments in the air-gapped environments.

During the preparation stage, the administrator downloads the lcm_file_analytics_3.2.0.tar.gz bundle and transfers it to the dark site web server.

upon performing the LCM inventory and trying to upgrade File Analytics, the administrator does not see the new version in the software tab.

Which additional file should the administrator transfer to the web server in order for the inventory to work?
* Nutanix_compatibility_bundle.tar.gz
* Nutanix_file_server_4.1.0.3.tar.gz
* Lcm_fsm_x.x.x.x. tar.gz
* lcm_file_manager_x.x.x.tar.gz

This is because this bundle contains LCM file manager component that is required for LCM inventory to work in dark site mode.

Download lcm_file_analytics_x.x.x.tar.gz bundle from Nutanix portal which contains File Analytics software binaries.

Download lcm_file_manager_x.x.x.tar.gz bundle from Nutanix portal which contains LCM file manager component that handles file operations such as upload, download and delete.

Transfer both bundles to a dark site web server that is accessible by LCM.

Configure LCM settings in Prism Element to use dark site mode and specify the URL of the dark site web server.

Perform LCM inventory which scans for available software bundles on the dark site web server.

Upgrade File Analytics using LCM which downloads and installs File Analytics software binaries from lcm_file_analytics_x.x.x.tar.gz bundle.

https://portal.nutanix.com/page/documents/details?targetId=File-Analytics-v3_2:File-Analytics-v3_2

NO.33 An administrator is implementing a storage solution with these requirements:

Is easily searchable

Natively supports disaster recovery

Access to each item needs to be fast

Can scale to petabytes of data

users are granted access after authentication

user data is isolated, but could be shared

How should the administrator satisfy these requirements?
* Deploy Objects with AD integration.
* use Files distributed share with ABE.
* Implement Volumes with CHAP.
* Configure Calm with an application per user.

This is because Objects can provide fast access to each item using S3-compatible API which can be easily searched using metadata tags or third-party tools3. Objects also natively supports disaster recovery using replication policies1. Objects can scale to petabytes of data using erasure coding which reduces storage overhead1. Users can be granted access after authentication using AD integration which simplifies identity management1. User data can be isolated but could be shared using buckets which are logical containers for objects that can have different policies applied1.

NO.34 An administrator would like to convert an existing Volume Group with an attached external Windows client to use Volumes.

The administrator has taken these actions:

* Disconnect any existing iSCSI targets

* Remove targets from the Favorite Targets tab

* Remove targets from the Discovery tab

Which action must the administrator take next to complete this task?
* Connect with MPIO to the iSCSI Data Services IP.
* Connect with MPIO to the Cluster Virtual IP.
* Connect without MPIO to the iSCSI Data Services IP.
* Connect without MPIO to the Cluster Virtual IP.

Connect with MPIO to the iSCSI Data Services IP. The iSCSI Data Services IP (DSIP) is a virtual IP address that provides load balancing and failover for iSCSI traffic across all CVMs in a cluster. The MPIO (Multi-Path I/O) option enables multiple paths for iSCSI traffic between Windows clients and Nutanix Volumes. The Cluster Virtual IP (CVIP) is used for management and communication between CVMs and should not be used for iSCSI traffic.

https://portal.nutanix.com/page/documents/solutions/details?targetId=BP-2049-Nutanix-Volumes:BP-2049-Nutanix-Volumes

NO.35 When completing the Linux Client iSCSI discovery process of the Nutanix cluster Volumes target, which action should an administrator complete first?
* Ensure the iSCSI is started.
* Restart iSCSI service on CVM.
* Discover the Volumes target.
* Establish connection to the Volumes target.

To use Nutanix Volumes with Linux clients, you must install and configure an iSCSI initiator on each client.” Therefore, the administrator should ensure that the iSCSI service is started on the Linux client before discovering or connecting to the Volumes target.

https://next.nutanix.com/installation-configuration-23/data-services-ip-iscsi-33804

NO.36 An administrator is implementing a VDI solution in a Nutanix cluster running AHV. The implementation includes home shares for user files. The shares have to be highly available, only accessible by the named user, and replicated to a DR site.

What solution would best fulfill these requirements?
* Files with Access Based Enumeration enabled.
* Volumes with ISCSI Initiators disabled.
* Objects with WORM enabled.
* Nutanix container with Whitelisting configured.

NO.37 Which action will improve the performance of a database server storage using Volumes that is experiencing persistent slow queries?
* Enable Flash Mode on the Volume Group.
* Disable deduplication on storage pool.
* Create dedicated container for database
* Upgrade CPUs on FSVMs running databases.
According to Nutanix Support & Insights1, Nutanix Volumes is a feature that provides block storage for both VMs and physical hosts using iSCSI protocol. A volume group (VG) is a collection of one or more disks in a Nutanix storage container.

According to Scale-Out Cloud Block Storage Built For AOS | Nutanix2, Flash Mode is an option that allows you to pin a VG to SSD tier for optimal performance. This can help improve the performance of a database server storage that is experiencing persistent slow queries.

https://portal.nutanix.com/page/documents/solutions/details?targetId=BP-2049-Nutanix-Volumes:BP-2049-Nutanix-Volumes

NO.38 An administrator has been asked to create a new user account for an auditor during an audit event. The auditor will write data to a Files share, for confidentiality reasons, the auditors tasks should be not analyzed by the system.

How should the administrator configure File Analytics to accomplish this task?
* Define a blacklisting rule in File Analytics
* Restrict Files access for the auditor.
* Create a dedicated share for the auditor in Files.
* Grant anonymous access to the share used by the auditor.
According to File Auditing and Analytics for your Nutanix Files Enterprise Cloud1, File Analytics is a feature that captures real-time user audit data and file metadata for Nutanix Files environments. It allows you to monitor file activities, analyze usage patterns, and generate reports.

According to Nutanix Files 3.8 and File Analytics 3.02, File Analytics supports blacklisting rules that allow you to exclude certain users or groups from being analyzed by the system. This can help protect the confidentiality of the auditor’s tasks.

https://next.nutanix.com/community-blog-154/nutanix-files-3-8-and-file-analytics-3-0-39309

NO.39 Which two statements are true about object counts in an object store? (Choose two.)
* Upload counts are included in the object counts at the bucket level.
* each upload of a multipart upload is counted as a separate object.
* Each upload of a multipart upload is counted as a separate object until the object is finalized.
* upload counts are not included in the object counts at the bucket level,
Upload counts are a metric that shows how many objects have been uploaded to a bucket in a given time period. Multipart uploads

are a way of uploading large objects by splitting them into smaller parts and uploading them separately. Each part is counted as an object until they are combined into a single object when the upload is finalized.

https://www.nutanix.com/products/objects

NO.40 A CIO has been reviewing the corporate BCDR plan. In this review, the CIO has noticed that they are replicating their Files deployments using the built in Files DR capabilities that are configured out of the box.

Upon further investigation, the CIO has identified that there are no granular share replications between their Files deployments and has requested the administrator to take an initiative and implement a granular Files Share recovery model.

Which Files capability should the administrator configure in order to be able to failover only certain shares?
* Data Lens
* Smart DR
* Smart Tiering
* NC2 on AWS

Smart DR enables granular recovery of individual file shares in Nutanix Files by replicating data at the share level. This allows for more fine-grained control over the failover process and ensures that only critical data is recovered in the event of a disaster or outage.

Files Smart DR is a feature that allows you to replicate between Files instances, either on-premises or running on Nutanix Cloud Clusters on AWS1. With Files Smart DR, you can configure granular share replication, which means you can select which shares to replicate and which ones to exclude1. Therefore, the correct answer to your question is B. Smart DR.

Files Smart DR also supports replicating snapshots between the source share and its target, which can help with data recovery and compliance2. Additionally, Files Smart DR is the mechanism by which Files will support disaster recovery in the Nutanix Xi cloud3.

NO.41 An administrator needs to configure a service to collect data from a forensic software package that audits client access to a specific location. Data need to be immutable, Which option meets these requirements?
* Configure WORM options to an Objects bucket.
* Configure an Objects bucket with versioning.
* Configure an Objects bucket with the Expire current objects lifecycle policy enabled
* Configure standard Objects bucket with the read-on)’ attribute enabled.

WORM stands for write once, read many, and it is a feature that prevents deletion or modification of object data1. Nutanix Objects supports WORM with industry-recognized security standards1.

NO.42 An administrator is determining the most recent operation a user performed on the share cifs1 within the last 24 hours.

How should the administrator complete this task in File Analytics?
* In the Anomalis section. select Users exceed an operation count threshold an input the 24 hour range for share cifs1.
* In the Audit Trails section, search for the user and view their last operations.
* In the Audit Trails section, search for the cifs1 share and view the actions on the share over the past 24-hour range.
* In the Anomalies section view the anomaly rule created for the user with an interval of 24 hours.

File Analytics is a tool used for monitoring and auditing file activity within an organization’s file servers. The administrator needs to determine the most recent operation a user performed on the share cifs1 within the last 24 hours. To accomplish this task in File Analytics, the administrator should go to the Audit Trails section, where they can search for the cifs1 share and view the actions on the share over the past 24-hour range. This will allow the administrator to see all the activity that has occurred on the share, including the most recent operation performed by the user.

According to the Nutanix Unified Storage v6 documents at nutanix.com1, File Analytics captures all file activity for registered file

server instances and provides an audit trail for administrators2. In the Audit Trails section, you can search for the user or the share name and view their operations over a specified time range2. This would allow you to determine the most recent operation a user performed on the share cifs1 within the last 24 hours.

NO.43 An administrator is upgrading Files. When running the preupgrade check, the following message is generated:

Fileserver in HA state

Which two steps should the administrator take to resolve this error message? (Choose two.)
* Verify FSVM is booted and not stuck.
* Check if Zookeeper services are running.
* Check for alerts for NVM being down.
* Check if Stargate services are running,

These steps are based on a guide from Nutanix on how to troubleshoot pre-upgrade checks failure for Nutanix Files1. The guide states that one possible cause of this error message is that Nutanix files node (fsvms) might not be up or accessible1. The guide also suggests checking if Zookeeper services are running on all FSVMs as part of the troubleshooting process1.

NO.44 An administrator has Files deployed globally and would like to run a report to understand cold, warm, and hot data.

Which Nutanix service would allow the administrator to view the data from a single management console?
* Data Lens
* Files Analytics
* Files Manager
* NCM Pro

According to Nutanix Cloud Platform to Deliver Strengthened Data Services for Unstructured and Structured Data1, “Nutanix Data Lens is a new unstructured data governance service that provides visibility into data usage and storage capacity across Nutanix Files deployments globally.” Therefore, the administrator can use Data Lens to run a report to understand cold, warm, and hot data across Files deployments.

https://www.nutanix.com/solutions/databases

NO.45 What is the reason for the alert: File Server In Heterogeneous State?
* The FSVMs are distributed properly on the hosts in the cluster.
* Performance of the File Server is optimal, and the alert can be ignored.
* The FSVMs do not match in their CPU or memory
* The hosts where the FSVMs run do not match in their CPU or memory configuration

According to the Nutanix Files Solution Guide1, all the FSVMs have the same basic configuration: four vCPU and 12 GB of RAM1. However, you can add more vCPU, RAM, and FSVMs to the cluster1.

Based on this information, the alert: File Server In Heterogeneous State indicates that the FSVMs do not match in their CPU or memory configuration1. This could affect the performance and availability of the file server

NO.46 Due to a new IP addressing plan for the vDesktops network, an administrator needs to change the Files client-side network.

Which action should the administrator perform first?
* Stop the Files service,
* Power off the FSVMs.
* Create a new’ managed virtual network.
* Remove existing DNS entries.

According to the Nutanix Unified Storage v6 documents at nutanix.com1, Files uses two types of networks: client-side and

server-side2. The client-side network is used for SMB and NFS access to Files shares, while the server-side network is used for internal communication between FSVMs3. To change the client-side network, you need to create a new managed virtual network on Prism Element and assign it to your FSVMs4. This will allow you to change the IP addresses of your FSVMs without affecting their connectivity to each other.

NO.47 A company’s IT security policy requires that all network traffic must be secure, and no web browser certificate error warnings should be accepted by end users.

An administrator is tasked with configuring Objects so that it uses a certificate from an internal Certificate Authority (CA), How should the administrator configure Objects to meet the security policy?
* Import the Private key and certificate files from the internal CA.
* Import the Private key with Subject Alternate Name of the company donmain.
* Regenerate the self-signed certificate with RSA 2048 as the bit type
* Regenerate the CSR and download certificates from the internal CA

According to Nutanix Support & Insights1, “To set the SSL certificate, do the following: … Under SSL Certificates, click Replace SSL Certificate. Click Regenerate CSR. Copy and save the generated CSR text. Use this text to request a certificate from your CA.” Therefore, the administrator should regenerate the CSR and download certificates from the internal CA to replace the self-signed certificate that Objects uses by default.

https://next.nutanix.com/installation-configuration-23/objects-user-guide-38847

NO.48 Which Nutanix interface is used to deploy a new Files instance?
* Prism Element
* Prism Central
* Files Manager
* Life Cycle Manager

According to Nutanix Support & Insights1, Nutanix Files is a scale-out file storage solution that provides SMB and NFS file services to clients. Nutanix Files instances are composed of a set of VMs (called FSVMs) that run on Nutanix clusters.

According to Your Complete Guide to Nutanix Files Training Resources2, Prism Central is the interface used to deploy a new Files instance. Prism Central is a centralized management console that provides visibility and control across multiple Nutanix clusters and services.

NO.49 What is the reason for the alert: File Server In Heterogeneous State?
* The FSVMs are distributed properly on the hosts in the cluster.
* The FSVMs do not match in their CPU or memory
* Performance of the File Server is optimal, and the alert can be ignored.
* The hosts where the FSVMs run do not match in their CPU or memory configuration

According to the Nutanix Files Solution Guide1, all the FSVMs have the same basic configuration: four vCPU and 12 GB of RAM1. However, you can add more vCPU, RAM, and FSVMs to the cluster1.

Based on this information, the alert: File Server In Heterogeneous State indicates that the FSVMs do not match in their CPU or memory configuration1. This could affect the performance and availability of the file server

NO.50 Which feature ensures that a host failure’s impact on a Files cluster will be minimal?
* VM-VM anti-affinity rules
* VM-VM affinity rules
* VM-Host anti-affinity rules
* VM-Host affinity rules

These rules ensure that VMs are distributed across different hosts in a cluster, so that if one host fails, the impact on the VMs and

their data will be minimal1. Nutanix Files also supports DFS-N (Distributed File System – Namespaces), which allows multiple file servers hosting the same data to support a common folder and provide site affinity for users2.

NO.51 What happens to an FSVM during a node failure in a 3-node cluster?
* Due to host affinity rules, the FSVM will not restart
* The FSVM will automatically restart on one of the remaining nodes.
* A new FSVM must be deployed to the cluster.
* The FSVM must be manually restarted on one of the remaining nodes.

According to the Nutanix Unified Storage (NCP-US) v6 documentation, when a node fails in a 3-node cluster, the FSVM (File Server Virtual Machine) will automatically restart on one of the remaining nodes. The remaining nodes will handle the storage traffic without requiring any user intervention.

https://portal.nutanix.com/page/documents/solutions/details?targetId=NVD-2151-Unified-Storage:high-availability-at-the-nutanix-files-level.html

NO.52 An administrator needs to configure a Files share with these requirements:

Supports 100 virtual desktop users

Share would host user data

Share is limited to 1 TB, evenly distributed across users

Optimized for best I/0 performance within the current environment

Which two configuration actions should the administrator take to meet these requirements? (Choose two.)
* Configure a standard share.
* Create a distributed share.
* Add a quote policy to the share.
* Enable ABE on the share.

According to Nutanix Files SMB Share Default Permission1, a standard share is created with default permissions for three built-in groups: Administrators, Users, and Backup Operators. This may not be suitable for hosting user data that needs to be evenly distributed across users.

According to Nutanix Support & Insights2, a distributed share is a type of SMB share that allows you to distribute files across multiple file servers for better performance and scalability. This can help optimize the I/O performance within the current environment.

According to Nutanix File and NFS Mount Examples3, a quota policy is a way to limit the amount of space that a user or group can consume on a share. This can help enforce the 1 TB limit on the share and ensure that each user gets an equal amount of space.

https://portal.nutanix.com/page/documents/solutions/details?targetId=TN-2041-Nutanix-Files%3ATN-2041-Nutanix-Files

NO.53 An administrator is scheduling to upgrade Files from version 3.8.1.3 to 4.1.0.2 for all the dark sites.

After transferring the dark site bundle to the internal web server, the administrator performs an LCM inventory but cannot check off the Files upgrade to be performed.

Which component needs to be upgraded along side of the core Files components?
* Files Sender

* File Server Module
* Files Manager
* File Analytics

When upgrading Files from version 3.8.1.3 to 4.1.0.2 for all dark sites, the File Server Module component needs to be upgraded alongside the core Files components. This is because the File Server Module is a core component of Files and is responsible for file-level data services, including access control, auditing, and file sharing.

If the File Server Module is not upgraded alongside the core Files components, it can result in compatibility issues and potentially cause the upgrade to fail.

Therefore, it is recommended to upgrade the File Server Module together with the core Files components when upgrading Files.