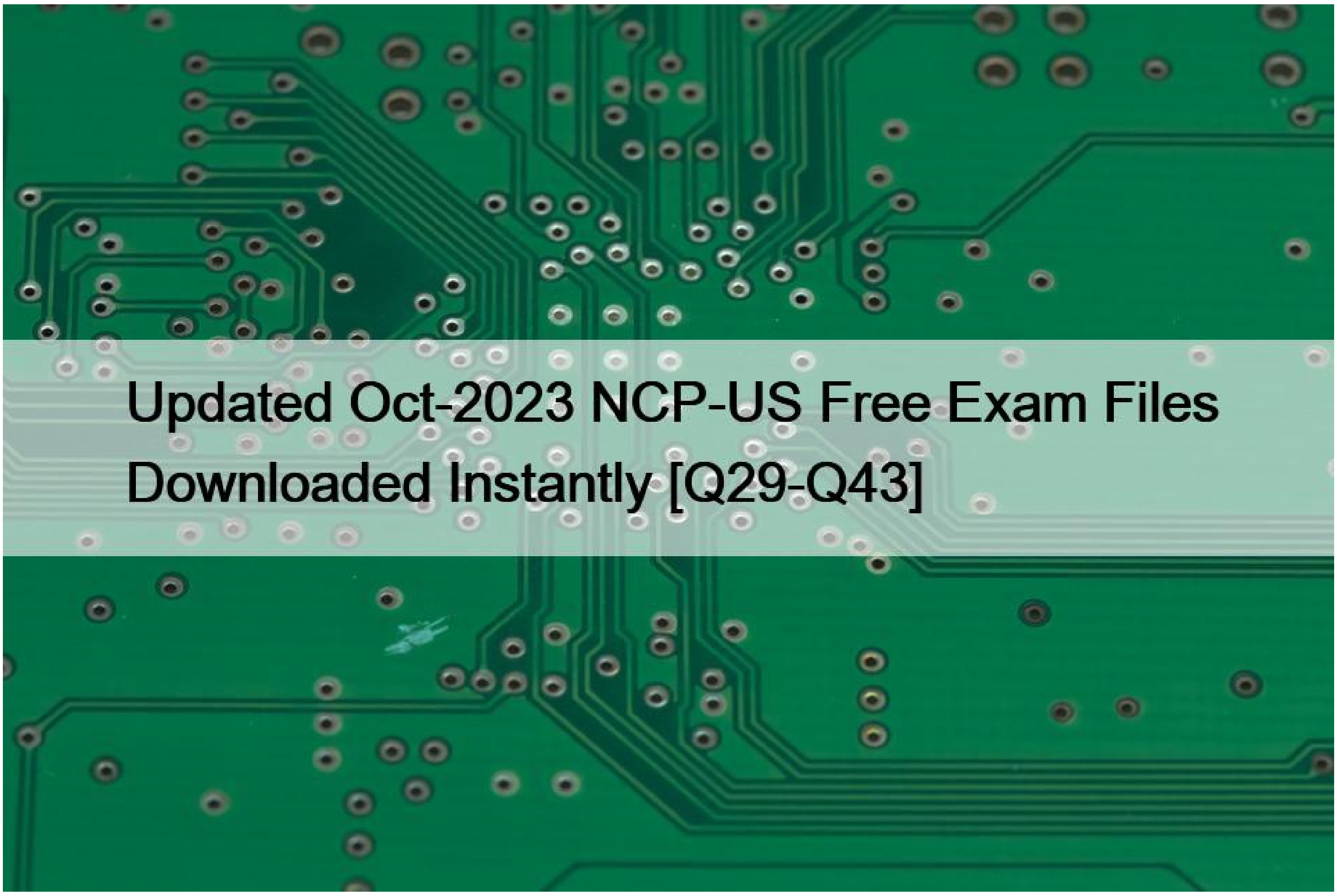
Updated Oct-2023 NCP-US Free Exam Files Downloaded Instantly [Q29-Q43



Updated Oct-2023 NCP-US Free Exam Files Downloaded Instantly
Practice Exams and Training Solutions for Certifications

Q29. An administrator needs to deploy a new Linux log collector package which creates a directory for each monitored item. The logs would be analyzed by a Windows application.

Which action should the administrator take, that will provide the best performance and simplicity?
* Create an Objects bucket with versioning enabled.
* Assign e Volume vDisk to the Linux collector VM,
* Create a Files distributed share with multi-protocol access.
* Configure Files Analytics to analyze the collected logs.

Creating a Files distributed share with multi-protocol access would allow for easy and efficient transfer of log files between the Linux collector package and the Windows application. This would provide simplicity in terms of configuration and management, and would also ensure that the log files are stored in a distributed and highly available manner, making it easier to access them as and when required.

, Files is a software-defined scale-out file storage solution that provides a single namespace for unstructured data2. Files supports both SMB and NFS protocols, which means you can access the same share from both Linux and Windows machines3. This would provide the best performance and simplicity for your log collector package and analysis application.

Q30. 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.

Q31. 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?
* The Enable mufti-path option should be unchecked.
* IP addresses of all CVMs should be entered.
* The Nutanix MPIO drivers should be installed.
* IP addresses of all FSVMs should be entered.
IP addresses of all FSVMs should be entered. FSVMs are File Server Virtual Machines that provide iSCSI services for Nutanix Volumes. The iSCSI initiator in Windows client devices should be configured with the IP addresses of all FSVMs in a cluster to enable load balancing and failover. The Enable multi-path option should be checked to use multiple paths for iSCSI traffic. The Nutanix MPIO drivers are not required for Windows clients as they can use native MPIO drivers.

https://next.nutanix.com/how-it-works-22/nutanix-volumes-recommendations-and-best-practices-38585

Q32. 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&#8217;s tasks.

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

Q33. An administrator of an existing Nutanix cluster running Kubernetes with multiple PODs notices that NCC checks report that some volume groups experience the following error:

Node x .x.x.x:

FAIL: Volume Group pvc -XXXXXX-XXXX-XXXX-XXXX-XXXXXXXXX space usage (908) The administrator checks the volume group usage from the Kubernetes pod and get different usage results. The current stats are 55% used disk space.

The results of the NCC check do not match what manually-executed checks report.

What is the cause of this behavior?
- The garbage collection process has yet to run.
- Kubernetes is not correctly reporting its storage usage
- The NCC checks need to be updated to the latest version.
- Volumes has not received the needed uNMAP commands.

The garbage collection process is performed by Curator, a service that runs on Nutanix clusters and is responsible for cleaning up unused data and reclaiming space12. Curator scans run periodically in the background and can be monitored from Prism2.

https://next.nutanix.com/how-it-works-22/ncc-health-check-garbage-egroups-39097

Q34. The Compliance department would like the administrator to have the ability to revert documents to previous versions.

How should the administrator facilitate this request?
- Configure Protection snapshots on the File Server.
- Enable Self-Service Restore on the Share/Export.
- Configure Protection snapshots on the Share/Export.
- Enable Self-Service Restore on the File Server

Protection snapshots are external snapshots that can be used to recover the file server cluster or individual files and folders1. They can be created through a protection domain schedule or via a user-initiated one-time snapshot of the protection domain1. By configuring protection snapshots on the share/export, the administrator can enable self-service restore for users to revert documents to previous versions2.

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

Q35. 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

Q36. 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&#8217;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.

Q37. 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)&#8217; 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.

Q38. An administrator has deployed a new backup software suite and needs to meet the following requirements:
* use S3-compatible storage.
* provide one-year retention.
* protect from deletions or overwrites for one year.
* meet regulatory requirements.
The administrator should use Nutanix Objects as the backup software suite.

Nutanix Objects is a S3-compatible storage solution that provides one-year retention and protection from deletions or overwrites for one year using WORM (Write Once Read Many) policies.

WORM policies can help meet regulatory requirements such as SEC 17a-4(f), FINRA 4511, CFTC 1.31-(d), and Rule 204-2 of Investment Advisers Act of 1940.

https://www.nutanix.com/sg/support-services/training-certification/certifications/certification-details-nutanix-certified-professional-unified-storage-v6 https://next.nutanix.com/education-blog-153/nutanix-unified-storage-v6-5-training-now-available-a-special-cert-offer-41673

Q39. 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

Q40. Which setting should the administrator apply to a newly-created Objects bucket to ensure the requirements are met?
* Configure a Lifecycle Policy to overwrite one-year old data in the bucket.
* Apply an Object versioning policy with one-year retention.
* Configure the bucket WORM policy with a one-year retention,
* Apply a bucket Lifecycle Policy with a one-year expiration.

Q41. 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.&#8221; 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

Q42. The Files administrator has received reports from users in the accounting department that they can see folders that they don&#8217;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 the accounting share can only see folders they have permission to access?
* Remove read-only access to shares users should not access.
* Enable Access-Based Enumeration on the accounting share.
* Enable Access-Based Enumeration on the File Sewer.
* Remove File Blocking on the accounting shares.

According to Nutanix Support & Insights1, Access-based enumeration (ABE) is a Windows feature that filters the list of available files and folders on the file server to include only those the requesting user can access. ABE can be enabled on a per-share basis for SMB shares.

Therefore, if the Files administrator wants to ensure that users in the accounting share can only see folders they have permission to access, they can enable ABE on the accounting share.

https://www.nutanix.com/support-services/training-certification/certifications/certification-details-nutanix-certified-professional-unified-storage-v6

Q43. 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.

Q&As with Explanations Verified & Correct Answers: https://www.dumpsmaterials.com/NCP-US-real-torrent.html]