Vendor: Nutanix

Exam Code:NCP-US

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

Version: Demo

QUESTION 1

A Files administrator needs to generate a report listing the files matching those in the exhibit.

What is the most efficient way to complete this task?

A. Use Report Builder in File Analytics.

B. Create a custom report in Prism Central.

C. Use Report Builder in Files Console.

D. Create a custom report in Files Console.

Correct Answer: A

Explanation: The most efficient way to generate a report listing the files matching those in the exhibit is to use Report Builder in File Analytics. Report Builder is a feature that allows administrators to create custom reports based on various filters and criteria, such as file name, file type, file size, file owner, file age, file access time, file modification time, file permission change time, and so on. Report Builder can also export the reports in CSV format for further analysis or sharing. References: Nutanix Files Administration Guide, page 97; Nutanix File Analytics User Guide

---

QUESTION 2

What is the most efficient way of enabling users to restore their files without administrator intervention in multiple Files shares?

A. Click Enable next to the name of the share in Manage Recovery Settings from Data Lens.

B. Click Enable Self Service Restore in the Edit wizard for each share in Shares tab from Files Console.

C. Assign the same Category to all FSVMs and adding that Category to a single Protection Policy in PC.

D. Add all FSVMs to a Consistency Group within a single asynchronous Protection Domain in PE.

Correct Answer: B

Explanation: Nutanix Files allows users to restore their files from the snapshots taken by the 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. A protection policy can be applied to one or more file shares. To enable users to restore their files without administrator intervention, the administrator must enable the Self Service Restore option for each share in the Files Console. This option adds a hidden folder named .snapshot in each share, which contains all the snapshots taken by the protection policy. Users can access this folder and browse the snapshots to find and restore their files. The administrator can also configure the permissions and quota for the .snapshot folder. References: Nutanix Files Administration Guide, page 75; Nutanix Files Self-Service Restore Guide

---

QUESTION 3

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?

A. Verify sharing policies at the bucket level.

B. Reset the Active Directory user password.

C. Replace SSL Certificates at the Object store level.

D. Verify Access Keys for the user.

Correct Answer: D

Explanation: 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. References: Nutanix Objects User Guide, page 13; Nutanix Objects Solution Guide, page 8

QUESTION 4

What best describes the data protection illustrated in the exhibit?

A. Smart DR

B. Metro Availability

C. Availability Zones

D. NearSync

Correct Answer: A

Explanation: 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. References: Nutanix Files Administration Guide, page 79; Nutanix Files Solution Guide, page 9

QUESTION 5

An administrator is tasked with creating an Objects store with the following settings:

Medium Performance (around 10,000 requests per second) 10 TiB capacity Versioning disabled Hosted on an AHV cluster

immediately after creation, the administrator is asked to change the name of Objects store

Who will the administrator achieve this request?

A. Enable versioning and then rename the Object store, disable versioning

B. The Objects store can only be renamed if hosted on ESXI.

C. Delete and recreate a new Objects store with the updated name

Correct Answer: C

Explanation: The administrator can achieve this request by deleting and recreating a new Objects store with the updated name. Objects is a feature that allows users to create and manage object storage clusters on a Nutanix cluster. Objects clusters can provide S3- compatible access to buckets and objects for various applications and users. Objects clusters can be created and configured in Prism Central. However, once an Objects cluster is created, its name cannot be changed or edited. Therefore, the only way to change the name of an Objects cluster is to delete the existing cluster and create a new cluster with the updated name. References: Nutanix Objects User Guide, page 9; Nutanix Objects Solution Guide, page 8

QUESTION 6

Which action is required to allow the deletion of file server audit data in Data Lens?

A. Enable the File Server.

B. Disable the File Server.

C. Update the data retention period.

D. Configure the audit trail target.

Correct Answer: C

Explanation: 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. References: Nutanix Files Administration Guide, page 98; Nutanix Data Lens User Guide

---

QUESTION 7

An administrator has been directed to configure Volumes to Nutanix\\'s best practices for security.

What should the administrate! do to be compliant?

A. Enable at-rest encryption on Volume Groups.

B. Configure Volume Groups to use CHAP.

C. Use data services IP for external host connectivity.

D. Segment iSCSI traffic to a physically separate network.

Correct Answer: B

Explanation: Nutanix 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 secure volume groups from unauthorized access, Nutanix recommends configuring CHAP (Challenge-Handshake Authentication Protocol) for each volume group in Prism Element. CHAP is a security feature that authenticates iSCSI initiators and targets before allowing access to a volume group. CHAP requires both the initiator and the target to have a shared secret (a password) that is used to generate a challenge and a response during the authentication process. CHAP can prevent unauthorized access to volume groups and protect data from malicious attacks. References: Nutanix Volumes Administration Guide, page 25; Nutanix Volumes Security Guide

---

QUESTION 8

Which port is required between a CVM or Prism Central to insights,nutanix.com for Data Lens configuration?

A. 80

B. 443

C. 8443

D. 9440

Correct Answer: B

Explanation: 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. References: Nutanix Files Administration Guide, page 93; Nutanix Data Lens User Guide

---

QUESTION 9

An administrator has performed an upgrade to Files. After upgrading, the file server cannot reach the given domain name with the specified DNS server list.

Which two steps should the administrator perform to resolve the connectivity issues with the domain controller servers? (Choose two.)

A. Verify the DNS settings in Prism Element.

B. DNS entries for the given domain name.

C. Verify the DNS settings in Prism Central.

D. DNS server addresses of the domain controllers.

Correct Answer: AB

Explanation: The two steps that the administrator should perform to resolve the connectivity issues with the domain controller servers are:

Verify the DNS settings in Prism Element: DNS (Domain Name System) is a system that translates domain names into IP addresses. DNS settings are configurations that specify which DNS servers to use for resolving domain names.

Verifying the DNS settings in Prism Element is a step that the administrator should perform, because it can help identify and correct any incorrect or outdated DNS server addresses or domain names that may cause connectivity issues with

the domain controller servers.

Verify the DNS entries for the given domain name: DNS entries are records that map domain names to IP addresses or other information. Verifying the DNS entries for the given domain name is another step that the administrator should

perform, because it can help check and update any incorrect or outdated IP addresses or other information that may cause connectivity issues with the domain controller servers. References: Nutanix Files Administration Guide, page 32;

Nutanix Files Troubleshooting Guide

QUESTION 10

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 11

An administrator needs to scale out an existing Files instance. Based on the Company\\'s requirements, File instance has four FSVMs configured and needs to expand to six. How many additional Client IP addresses and Storage IP addresses does the administrator require to complete this task?

A. 3 Client IPs and 2 Storage IPs

B. 2 Client IPs and 2 Storage IPs

C. 3 Client IPs and 3 Storage IPs

D. 2 Client IPs and 3 Storage IPs

Correct Answer: B

Explanation: To scale out an existing Files instance, the administrator needs to add one Client IP and one Storage IP for each additional FSVM. Since the Files instance needs to expand from four FSVMs to six FSVMs, the administrator needs to add two Client IPs and two Storage IPs in total. The Client IPs are used for communication between the FSVMs and the clients, while the Storage IPs are used for communication between the FSVMs and the CVMs. References: Nutanix Files Administration Guide, page 28; Nutanix Files Solution Guide, page 7

QUESTION 12

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