NCP-US-6.5 Q&As

Nutanix Certified Professional - Unified Storage (NCP-US) v6.5

Pass Nutanix NCP-US-6.5 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/ncp-us-6-5.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Nutanix Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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.

A. Create a Bucket replication rule, set the destination Objects instances.

B. With Object Browser, upload the data at the destination site.

C. Leverage the Objects Baseline Replication Tool from a Linus VM

D. Use a protection Domain to replicate the objects Volume Group.

Correct Answer: A

Explanation: 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. References: Nutanix Objects User Guide, page 19; Nutanix Objects Solution Guide, page 9

QUESTION 2

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?

A. File Analytics

B. Syslog Server

C. Files Console

D. Protection Domain

Correct Answer: A

Explanation: 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. References: Nutanix File Analytics Administration Guide2

QUESTION 3

With the settings shown on the exhibit, if there were 1000 files in the repository, how many files would have to be... anomaly alert to the administrator?

A. 1

B. 10

C. 100

D. 1000

Correct Answer: B

Explanation: With the settings shown on the exhibit, if there were 1000 files in the repository, 10 files would have to be deleted within an hour to trigger an anomaly alert to the administrator. Anomaly alert is a feature that notifies the administrator when there is an unusual or suspicious activity on file data, such as mass deletion or encryption. Anomaly alert can be configured with various parameters, such as threshold percentage, time window, minimum number of files, and so on. In this case, the threshold percentage is set to 1%, which means that if more than 1% of files in a repository are deleted within an hour, an anomaly alert will be triggered. Since there are 1000 files in the repository, 1% of them is 10 files. Therefore, if 10 or more files are deleted within an hour, an anomaly alert will be sent to the administrator. References: Nutanix Files Administration Guide, page 98; Nutanix Data Lens User Guide

QUESTION 4

Which error logs should the administrator be reviewing to determine why the relates service is down?

A. Solver.log

B. Arithmos.ERROR

C. Cerebro.ERROR

D. Tcpkill.log

Correct Answer: C

Explanation: The error log that the administrator should review to determine why the relay service is down is Cerebro.ERROR. Cerebro is a service that runs on each FSVM and provides relay functionality for Data Lens. Relay service is responsible for collecting metadata and statistics from FSVMs and sending them to Data Lens via HTTPS. If Cerebro.ERROR log shows any errors or exceptions related to relay service, it can indicate that relay service is down or not functioning properly. References: Nutanix Files Administration Guide, page 23; Nutanix Data Lens User Guide

QUESTION 5

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 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

Deploying Files instances require which two minimum resources? (Choose two)

A. 12 GiB of memory per host

B. 8 vCPUs per host

C. 8 GiB of memory per host

D. 4 vCPUs per host

Correct Answer: CD

Explanation: The two minimum resources that are required for deploying Files instances are 8 GiB of memory per host and 4 vCPUs per host. Memory and vCPUs are resources that are allocated to VMs (Virtual Machines) to run applications and processes. Files instances are file server instances (FSIs) that run on FSVMs (File Server VMs) on a Nutanix cluster. FSVMs require at least 8 GiB of memory and 4 vCPUs per host to function properly and provide SMB

and NFS access to file shares and exports. The administrator should ensure that there are enough memory and vCPUs available on each host before deploying Files instances. References: Nutanix Files Administration Guide, page 27; Nutanix Files Solution Guide, page 6

QUESTION 8

Which confirmation is required for an Objects deployment?

A. Configure Domain Controllers on both Prism Element and Prism Central.

B. Configure VPC on both Prism Element and Prism Central.

C. Configure a dedicated storage container on Prism Element or Prism Cent

D. Configure NTP servers on both Prism Element and Prism Central.

Correct Answer: D

Explanation: The configuration that is required for an Objects deployment is to configure NTP servers on both Prism Element and Prism Central. 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. Configuring NTP servers on both Prism Element and Prism Central is required for an Objects deployment, because it ensures that the time settings are consistent and accurate across the Nutanix cluster and the Objects cluster, which can prevent any synchronization issues or errors. References: Nutanix Objects User Guide, page 9; Nutanix Objects Deployment Guide

QUESTION 9

What are two network requirements for a four-node FSVM deployment? (Choose two.)

A. Four available IP addresses on the Storage network

B. Five available IP addresses on the Client network

C. Five available IP addresses on the Storage network

D. Four available IP addresses on the Client network

Correct Answer: BC

Explanation: The two network requirements for a four-node FSVM deployment are five available IP addresses on the Client network and five available IP addresses on the Storage network. The Client network is used for communication between the FSVMs and the clients, while the Storage network is used for communication between the FSVMs and the CVMs. For each FSVM, one Client IP and one Storage IP are required. Additionally, one extra Client IP is required for the file server VIP (Virtual IP), which is used as a single point of access for all shares and exports on the file server. References: Nutanix Files Administration Guide, page 28; Nutanix Files Solution Guide, page 7

QUESTION 10

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

A. Create an SMB Share with Files and enable Previous Version

B. Provision a Volume Group and connect via iSCSI with MPIO.

C. Create an NFS Share, mounted on a Linux Server with Files.

D. Create a bucket in Objects with Versioning enabled.

Correct Answer: D

Explanation: 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. References: Nutanix Objects Administration Guide

QUESTION 11

An administrator has been asked to confirm the ability of a physical windows Server 2019 host to boot from storage on a Nutanix AOS cluster.

Which statement is true regarding this confirmation by the administrator?

A. Physical servers may boot from an object bucket from the data services IP and MPIO is required.

B. Physical servers may boot from a volume group from the data services IP and MPIO is not required.

C. Physical servers may boot from a volume group from the data services IP and MPIO is

D. Physical servers may boot from an object bucket from the data services IP address and MPIO is not required.

Correct Answer: C

Explanation: Nutanix Volumes allows physical servers to boot from a volume group that is exposed as an iSCSI target from the data services IP. To ensure high availability and load balancing, multipath I/O (MPIO) is required on the physical server. Object buckets cannot be used for booting physical servers1. References: Nutanix Volumes Administration Guide1

QUESTION 12

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 13

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?

A. Configure Alerts and Events in the Files Console, filtering for Warning severity.

B. Deploy the Files Analytics VM. and configure anomaly rules.

C. Configure Files to use ICAP servers, with monitors for desired activities.

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

Correct Answer: B

Explanation: 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. References: Nutanix Files Administration Guide, page 93; Nutanix File Analytics User Guide

QUESTION 14

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 15

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

How should the administrator meet this requirement?

A. Create a protection domain in the Data Protection view in Prism Element.

B. Configure data protection polices in File Server view in Prism Element

C. Create a protection domain in the Data Protection view in Prism Central.

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

Correct Answer: D

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