Buy Latest Jan 19, 2024 NCP-US-6.5 Exam Q&A PDF - One Year Free Update [Q39-Q56
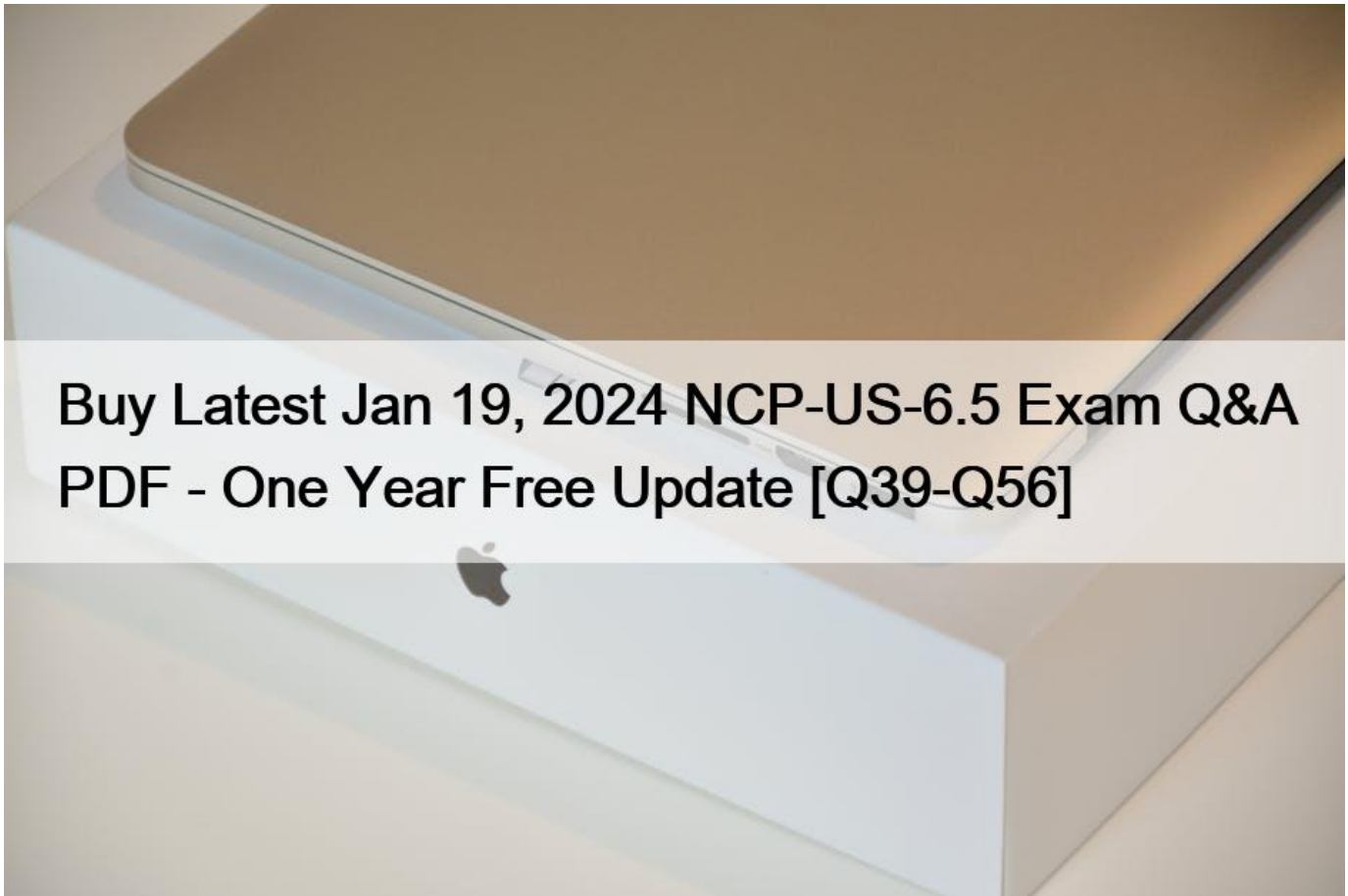
Buy Latest Jan 19, 2024 NCP-US-6.5 Exam Q&A PDF - One Year Free Update

Download the Latest NCP-US-6.5 Dump - 2024 NCP-US-6.5 Exam Questions

Nutanix NCP-US-6.5 Exam Syllabus Topics:

TopicDetailsTopic 1- Deploy and Upgrade Nutanix Unified Storage- Perform upgrades- maintenance for Files- Objects implementationsTopic 2- Utilize File Analytics for data security- Troubleshoot Nutanix Unified Storage- Configure Nutanix VolumesTopic 3- Given a scenario, configure shares, buckets, and- or Volume Groups- Troubleshoot a failed upgrade for Files- ObjectsTopic 4- Configure Nutanix Objects- Describe how to monitor performance and usageTopic 5- Analyze and Monitor Nutanix Unified Storage- Describe the use of Data Lens for data security

NO.39 Which protocols are supported by Files?
* SMBv2 SMBv3, NFSv2, NFSv3
* SMBv1. SMBv2, NFSv2, NFSv3
* SMBv1. SMBv2, NFSv3, NFSv4
* SMBv2 SMBv3, NFSv3, NFSv4

The protocols that are supported by Files are SMBv2, SMBv3, NFSv3, and NFSv4. SMB (Server Message Block) is a protocol that allows clients to access files, printers, and other resources on a network. NFS (Network File System) is a protocol that allows clients to access files on a remote server as if they were local. Files supports both SMB and NFS protocols for creating shares and exports that can be accessed by different types of clients. Reference: Nutanix Files Administration Guide, page 31; Nutanix Files Solution Guide, page 6

NO.40 Immediately after creation, the administrator is asked to change the name of Objects store.

How will the administrator achieve this request?
* Enable versioning and then rename the Objects store, disable versioning
* The Objects store can only be renamed if hosted on ESXi.
* Delete and recreate a new Objects store with the updated name.
* Update the name of the Objects stores by using a CORS XML file

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. Reference: Nutanix Objects User Guide, page 9; Nutanix Objects Solution Guide, page 8

NO.41 What is the network requirement for a File Analytics deployment?
* Must use the CVM not work
* Must use the Backplane network
* Must use the Storage-side network
* Must use the Client-side network

Nutanix File Analytics is a feature that provides insights into the usage and activity of file data stored on Nutanix 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. The FAVM collects metadata and statistics from the FSVMs and displays them in a graphical user interface (GUI). The FAVM must be deployed on the same network as the FSVMs, which is the Client-side network. This network is used for communication between File Analytics and FSVMs, as well as for accessing the File Analytics UI from a web browser. The Client-side network must have DHCP enabled and must be routable from the external hosts that access the file shares and File Analytics UI. Reference: Nutanix Files Administration Guide, page 93; Nutanix File Analytics Deployment Guide

NO.42 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 ‘ 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

NO.43 Life Cycle manager must the compatible versions of which two components before installing or upgrading Files? (Choose two.)

* Active Directory Services
* Nutanix Cluster Check
* File Server Mobile
* Acropolis Operating System

Before installing or upgrading Files, Life Cycle Manager (LCM) must check the compatibility versions of Nutanix Cluster Check (NCC) and Acropolis Operating System (AOS). NCC is a framework of scripts that helps diagnose cluster health, and AOS is the core operating system that runs on each node in a Nutanix cluster. LCM will not proceed with the installation or upgrade if NCC or AOS versions are incompatible with Files. Reference: Nutanix Files Administration Guide, Nutanix Cluster Check Guide

NO.44 An administrator has created a volume and needs to attach it to a windows host a via iSCSI. The data Services IP has been configured in the MS iSCSI Initiator, but no target are visible.

What is most likely the cause this issue?
* The host’ s IP address is not authorized to access the volume.
* The CHAP password configured on the client is incorrect.
* The CHAP Authentication has not been configured on the client.
* The host’s IQN is not authorized to access to the volume.

Nutanix Volumes uses IQN-based authorization to control access to volumes. The administrator must specify the IQN of the host that needs to access the volume when creating or editing the volume. If the host’s IQN is not authorized, it will not be able to see the target in the MS iSCSI Initiator3. Reference: Nutanix Volumes Administration Guide3

NO.45 What are two ways to manage Objects? (Choose two.)
* PC
* CLI
* API
* SSH

There are two ways to manage Objects: PC (Prism Central) and API (Application Programming Interface). PC is a web-based user interface that allows administrators to create, configure, monitor, and manage Objects clusters, buckets, users, and policies. API is a set of S3-compatible REST APIs that allows applications and users to interact with Objects programmatically. API can be used to perform operations such as creating buckets, uploading objects, listing objects, downloading objects, deleting objects, and so on. Reference: Nutanix Objects User Guide; Nutanix Objects API Reference Guide

NO.46 Before upgrading Files or creating a file server, which component must first be upgraded to a compatible version?
* FSM
* File Analytics
* Prism Central
* FSVM

The component that must first be upgraded to a compatible version before upgrading Files or creating a file server is Prism Central. Prism Central is a web-based user interface that allows administrators to manage multiple Nutanix clusters and services, including Files. Prism Central must be upgraded to a compatible version with Files before upgrading an existing file server or creating a new file server. Otherwise, the upgrade or creation process may fail or cause unexpected errors. Reference: Nutanix Files Administration Guide, page 21; Nutanix Files Upgrade Guide

NO.47 An administrator needs to protect a Files cluster unique policies for different shares.

How should the administrator meet this requirement?
* Create a protection domain in the Data Protection view in Prism Element.
* Configure data protection polices in File Server view in Prism Element
* Create a protection domain in the Data Protection view in Prism Central.
* Configure data protection polices in the Files view in Prism Central.

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

NO.48 An administrator has received an alert AI60068 – ADSDuplicationIPDetected details of alert as follows:

Which error log should the administrator review to determine the related Duplicate IP address involved?
* Tcpkill.log
* Minerva_cvm.log
* Solver.log
* Minerva.nvm.log

The Minerva_cvm.log file contains information about the Minerva service, which is responsible for managing the FSVMs and their communication with Prism Central. The Minerva_cvm.log file can be used to troubleshoot issues related to Nutanix Files, such as duplicate IP address detection. The log file can be found in /home/nutanix/data/logs/minerva on any CVM in the cluster. Reference: Nutanix Support Portal – Troubleshooting Nutanix Files

NO.49 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.
* 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

NO.50 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?
* Examine the failed tasks on the FSVMs
* Check the there is enough disk space on FSVMs.
* Verify connectivity between the FSVMs.
* Increase upgrades timeout from ecli

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. Reference: Nutanix Support Portal – Troubleshooting Nutanix Files Upgrade Issues

NO.51 ionization deployed Files in multiple sites, including different geographical locations across the globe. The organization has the following requirements to improves their data management lifecycle:

* Provide a centralized management solution.

* Automate archiving tier policies for compliance purposes.

* Protect the data against ransomware.

Which solution will satisfy the organization’s requirements?
* Prims Central
* Data Lens
* Files Analytics

Data Lens can provide a centralized management solution for Files deployments in multiple sites, including different geographical locations. Data Lens can also automate archiving tier policies for compliance purposes, by allowing administrators to create policies based on file attributes, such as age, size, type, or owner, and move files to a lower-cost tier or delete them after a specified period. Data Lens can also protect the data against ransomware, by allowing administrators to block malicious file signatures from being written to the file system. Reference: Nutanix Data Lens Administration Guide

NO.52 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

NO.53 Which user is authorized to deploy File Analytics?
* Prism Central administrator
* AD user mapped to a Prism admin role
* Prism Element administrator
* AD user mapped to a Cluster admin role

The user that is authorized to deploy File Analytics is Prism Central administrator. Prism Central is a web-based user interface that allows administrators to manage multiple Nutanix clusters and services, including Files and File Analytics. Prism Central administrator is a user role that has full access and control over all Prism Central features and functions. To deploy File Analytics, the user must log in to Prism Central as a Prism Central administrator and follow the steps in the File Analytics Deployment wizard. Reference: Nutanix Files Administration Guide, page 93; Nutanix File Analytics Deployment Guide

NO.54 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.

* Create a Bucket replication rule, set the destination Objects instances.
* With Object Browser, upload the data at the destination site.
* Leverage the Objects Baseline Replication Tool from a Linus VM
* Use a protection Domain to replicate the objects Volume Group.

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

NO.55 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?
* File Analytics
* Syslog Server
* Files Console
* Protection Domain

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. Reference: Nutanix File Analytics Administration Guide2

NO.56 What are two network requirements for a four-node FSVM deployment? (Choose two.)
* Four available IP addresses on the Storage network
* Five available IP addresses on the Client network
* Five available IP addresses on the Storage network
* Four available IP addresses on the Client network

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. Reference: Nutanix Files Administration Guide, page 28; Nutanix Files Solution Guide, page 7

Verified NCP-US-6.5 Dumps Q&As - 1 Year Free & Quickly Updates: