Question 1

An administrator created a bucket for an upcoming project where internal users as well as an outside consultant .... Object Browser. The administrator needs to provide both internal and consultant access to the same bucket.

The organization would like to prevent internal access to the consultant, based on their security policy.

Which two items are requires to fulfill this requirement (Choose two.)

Options:

A- Configure Directory Services under the Access Keys section

B- Generate access keys based on directory and email-based users.

C- Install third-party software for bucket access to all users.

D- Generate access keys using third-party software.

Answer:

A, B

Explanation:

Nutanix Objects supports directory services integration, which allows administrators to configure access keys based on directory and email-based users. This enables granular access control and security for buckets and objects.The administrator can configure directory services under the Access Keys section in Prism Central, and then generate access keys for internal users from the directory service and for the consultant from an email address2. Reference: Nutanix Objects Administration Guide2

Question 2

Question Type: MultipleChoice

Which two prerequisites are needed when deploying Objects to a Nutanix cluster? (Choose two.)

Options:

A- Microsegmentation is enabled.

B- Data Services IP is configured on the PI

C- DNS is configured on the PE.

D- AHV IPAM is disabled on the VLAN used for Objects.

Answer:

B

Explanation:

Nutanix Objects requires a Data Services IP to be configured on the Prism Infrastructure (PI) cluster, which is used to expose the S3 API endpoint for accessing buckets and objects.Nutanix Objects also requires AHV IP Address Management (IPAM) to be disabled on the VLAN used for Objects, as Objects uses its own DHCP service to assign IP addresses to the Objects VMs1. Reference: Nutanix Objects Administration Guide1

Question 3

How many configure snapshots are supported for SSR in a file server?

Options:

A- 25

B- 50

C- 100

D- 200

Answer:

D

Explanation:

The number of configurable snapshots that are supported for SSR in a file server is 200. SSR (Snapshot-based Replication) is a feature that allows administrators to replicate snapshots of shares or exports from one file server to another file server on a different cluster or site for disaster recovery purposes. SSR can be configured with various parameters, such as replication frequency, replication status, replication mode, etc. SSR supports up to 200 configurable snapshots per share or export in a file server.Reference:Nutanix Files Administration Guide, page 81; Nutanix Files Solution Guide, page 9

Question 4

Question Type: MultipleChoice

An administrator has deployed a new Files cluster within a Windows Environment.

After some days, he Files environment is not able to synchronize users with the Active Directory server anymore. The administrator observes a large time difference between the Files environment and the Active Directory Server that is responsible for the behavior.

How should the administrator prevent the Files environment and the AD Server from having such a time difference in future?

Options:

A- Use the same NTP Servers for the File environment and the AD Server.

B- Use 0.pool.ntp.org as the NTP Server for the AD Server.

C- Use 0.pool.ntp.org as the NTP Server for the Files environment.

D- Connect to every FSVM and edit the time manually.

Answer:

A

Explanation:

The administrator should prevent the Files environment and the AD Server from having such a time difference in future by using the same NTP Servers for the File environment and the AD Server. 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. By using the same NTP Servers for the File environment and the AD Server, the administrator can ensure that they have consistent and accurate time settings and avoid any synchronization issues or errors.Reference:Nutanix Files Administration Guide,

Question 5

Question Type: MultipleChoice

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

Options:

A- Enable the File Server.

B- Disable the File Server.

C- Update the data retention period.

D- Configure the audit trail target.

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

Question 6

Question Type: MultipleChoice

Which metric is utilized when sizing a Files deployment based on performance requirements?

Options:

A- Quantity of SMB shares

B- SMB concurrent connections

C- NFS concurrent connections

D- Quantity of NFS exports

Answer:

B

Explanation:

This metric indicates the number of active clients that are accessing the Files cluster via SMB protocol, which affects the performance of the Files cluster. NFS concurrent connections is also a relevant metric, but it is not the best answer, as it only applies to NFS protocol, not SMB. The quantity of SMB shares or NFS exports does not directly affect the performance of the Files cluster, as they are logical entities that do not consume resources. Reference: Nutanix Files Sizing Guide

Question 7

Question Type: MultipleChoice

An administrator is required to place all iSCSI traffic on an isolated network.

How can the administrator meet this requirement?

Options:

A- Create a new network interface on the CVMs via ncli.

B- Create a Volumes network in Prism Central.

C- Configure network segmentation for Volumes.

D- Configure the Data Services IP on an isolated network.

Answer:

C

Explanation:

The administrator can meet this requirement by configuring network segmentation for Volumes. Network segmentation is a feature that allows administrators to isolate network traffic for different types of services, such as Volumes, Files, or Objects, on a Nutanix cluster. Network segmentation can improve the security, performance, and manageability of network traffic. By configuring network segmentation for Volumes, the administrator can place all iSCSI traffic on an isolated network and prevent it from interfering with other services or applications.Reference:Nutanix Volumes Administration Guide, page 15; Nutanix Volumes Solution Guide, page 7

Question 8

Question Type: **MultipleChoice**

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?

Options:

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

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

Question 9

An administrator has received an alert AI60068 -- ADSDuplicationIPDetected details of alert as follows:

```
Block Serial Number: 16SMXXXXXXXXX
alert_time: Thu Jan 19 2023 23:14:10 GMT-0800 (PST)
alert_type: AFSDuplicateIPDetected
alert_msg: A160068: Duplicate IP address detected for a file server VMs for (file_server_name). Error Message: [...]
cluster_id: xxxxx
alert_body: No Alert Body Available
```

Which error log should the administrator review to determine the related Duplicate IP address involved?

Options:

A- Tcpkill.log

B- Minerva_cvm.log

C- Solver.log

D- Minerva.nvm.log

Answer:

B

Explanation:

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

Question 10

Question Type: MultipleChoice

What is the binary image extension of File Analytics?

Options:

A- JSON

B- QCOW2

C- ISO

D- VMDK

Answer:

B

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 is deployed as a VM on an AHV cluster using a QCOW2 binary image file that contains the File Analytics software and configuration3. Reference: Nutanix File Analytics Administration Guide3

Question 11

Question Type: **MultipleChoice**

The Administrator needs to review the following graphs, as displayed in the exhibit.

* Storage Used

* Open Connections

* Number of Files

* Top Shares by Current Capacity

* Top Shares by current Connections

Where should the administrator complete this action?

Options:

A- Files Console Share View

B- Files Console Data Management View

C- Files Console Monitoring View

D- Files Console Dashboard View

Answer:

D

Explanation:

The Files Console Dashboard View provides an overview of the Files cluster performance and usage, including the following graphs:

Storage Used: Shows the total storage used by the Files cluster, including data, metadata, and snapshots.

Open Connections: Shows the number of active SMB and NFS connections to the Files cluster.

Number of Files: Shows the number of files stored in the Files cluster, excluding snapshots.

Top Shares by Current Capacity: Shows the top five shares by current capacity usage in the Files cluster.

Top Shares by Current Connections: Shows the top five shares by current connection count in the Files cluster2. Reference: Nutanix Files Administration Guide2

Question 12

Question Type: **MultipleChoice**

An administrator is tasked with deploying a Microsoft Server Failover Cluster for a critical application that uses shared storage.

The failover cluster instance will consist of VMs running on an AHV-hosted cluster and bare metal servers for maximum resiliency.

What should the administrator do to satisfy this requirement?

Options:

A- Create a Bucket with Objects.

B- Provision a Volume Group with Volume.

C- Create an SMB Share with Files.

D- Provision a new Storage Container.

Answer:

B

Explanation:

Nutanix Volumes allows administrators to provision a volume group with one or more volumes that can be attached to multiple VMs or physical servers via iSCSI. This enables the creation of a Microsoft Server Failover Cluster that uses shared storage for a critical application.The volume group can be attached to VMs running on an AHV-hosted cluster and bare metal servers for maximum resiliency1. Reference: Nutanix Volumes Administration Guide1