Nutanix.NCP-US-6.5.v2023-11-23.q32

Exam Code:	NCP-US-6.5
Exam Name:	Nutanix Certified Professional - Unified Storage (NCP-US) v6.5
Certification Provider:	Nutanix
Free Question Number:	32
Version:	v2023-11-23
# of views:	547
# of Questions views:	320
https://www.freepdfdumps.com/Nutanix.NCP-US-6.5.v2023-11-23.q32.html	

NEW QUESTION: 1
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
Answer: (SHOW ANSWER)
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. Reference: Nutanix Data Lens Administration Guide3

NEW QUESTION: 2
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.
Answer: C (LEAVE A REPLY)

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. Reference: Nutanix Volumes Administration Guide1

NEW QUESTION: 3
An administrator is looking for a tool that includes these features:
* Permission Denials
* Top 5 Active Users
* Top 5 Accessed Files
* File Distribution by Type
Nutanix tool should the administrator choose?
A. File Server Manager
B. Prism Central
C. File Analytics
D. Files Console
Answer: (SHOW ANSWER)
The tool that includes these features is File Analytics. 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 display various reports and dashboards that include these features:
Permission Denials: This report shows the number of permission denied events for file operations, such as read, write, delete, etc., along with the user, file, share, and server details.
Top 5 Active Users: This dashboard shows the top five users who performed the most file operations in a given time period, along with the number and type of operations.
Top 5 Accessed Files: This dashboard shows the top five files that were accessed the most in a given time period, along with the number of accesses and the file details.
File Distribution by Type: This dashboard shows the distribution of files by their type or extension, such as PDF, DOCX, JPG, etc., along with the number and size of files for each type. Reference: Nutanix Files Administration Guide, page 93; Nutanix File Analytics User Guide

NEW QUESTION: 4
What is a prerequisite for deploying Smart DR?
A. Requires one-to-many shares.
B. The Files Manager must have at least three file servers.
C. The primary and recovery file servers must have the same domain name.
D. Open TCP port 7515 on all client network IPs (uni-directionally on the source and recovery file servers).
Answer: D (LEAVE A REPLY)

Smart DR is a feature that allows share-level replication between active file server instances for disaster recovery. To configure Smart DR, one of the prerequisites is to open TCP port 7515 on all client network IPs (uni-directionally on the source and recovery file servers). This port is used for communication between the FSVMs and the replication engine. Reference: Nutanix Files Administration Guide, page 79; Nutanix Files Solution Guide, page 9

NEW QUESTION: 5
An administrator is attempting to create a share that will provide user access via SMB and NFS. However, the Enable multiprosotocol accounts for NFS clients settings is not available.
What would cause this issue?
A. The connection to Active Directory has not been configured.
B. The file server instance was only configured with SMB.
C. The incorrect Files license has been applied.
D. NFS configured to use unmanaged authentication.
Answer: A (LEAVE A REPLY)
The cause of this issue is that the connection to Active Directory has not been configured. Active Directory is a service that provides centralized authentication and authorization for Windows-based clients and servers. To create a share that will provide user access via SMB and NFS, the administrator must first configure the connection to Active Directory in the Files Console. This will allow the administrator to enable multiprotocol accounts for NFS clients, which are accounts that map NFS users to SMB users and groups for consistent access control across both protocols. Reference: Nutanix Files Administration Guide, page 32; Nutanix Files Solution Guide, page 6

NEW QUESTION: 6
An administrator is required to place all iSCSI traffic on an isolated network.
How can the administrator meet this requirement?
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 (LEAVE A REPLY)
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

NEW QUESTION: 7

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?
A. Ensure that vCenter in PE cluster is registered using FQDN and that vCenter details in Objects UI are using FQDN.
B. Replace the expired self-signed SSL certificate for the Object Store with a non-expired ' signed by a valid Certificate Authority.
C. Replace the expired self-signed SSL certificate for the Object Store with a non-expired self signed SSL certificate.
D. Ensure that vCenter in PE cluster is registered using FQDN and that vCenter details in Objects UI are using IP address.
Answer: A (LEAVE A REPLY)
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

NEW QUESTION: 8
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
Answer: B (LEAVE A REPLY)
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

NEW QUESTION: 9
An administrator is planning to upgrade all ESXi hypervisors in a cluster hosting Files.
When performing one-click hypervisor upgrades, what prerequisite must be performed?
A. Enable the anti-affinity rules on all FSVMs.

B. Manually migrate the FSVMs.
C. Shutdown the FSVMs.
D. Disable the anti-affinity rules on all FSVMs.
Answer: D (LEAVE A REPLY)
The prerequisite that must be performed before performing one-click hypervisor upgrades is to disable the anti-affinity rules on all FSVMs. Anti-affinity rules are rules that prevent two or more VMs from running on the same host at the same time. Anti-affinity rules can improve the availability and performance of FSVMs by distributing them across different hosts in a cluster. However, anti-affinity rules can interfere with one-click hypervisor upgrades, which require all VMs on a host to be migrated to another host before upgrading the host. Therefore, the administrator must disable the anti-affinity rules on all FSVMs before performing one-click hypervisor upgrades, and re-enable them after the upgrades are completed. Reference: Nutanix Files Administration Guide, page 22; Nutanix Files Upgrade Guide

NEW QUESTION: 10
What tool can be used to report on a specific user's activity within a Files environment?
A. Prism Element Alerts menu
B. Prism Central Activity menu
C. Data Lens Audit Trails
D. Files Console Usage
Answer: C (LEAVE A REPLY)
The tool that can be used to report on a specific user's activity within a Files environment is Data Lens Audit Trails. Data Lens Audit Trails is a feature that provides detailed logs of all file operations performed by users on Files shares and exports, such as create, read, write, delete, rename, move, copy, etc. Data Lens Audit Trails can help administrators track and audit user actions and identify any unauthorized or malicious activities. The administrator can use Data Lens Audit Trails to filter and search for a specific user's activity based on various criteria, such as file name, file type, file size, file path, file share, file server, operation type, operation time, operation status, and so on. Reference: Nutanix Files Administration Guide, page 98; Nutanix Data Lens User Guide

NEW QUESTION: 11
Which two prerequisites are needed when deploying Objects to a Nutanix cluster? (Choose two.)
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 (LEAVE A REPLY)
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

NEW QUESTION: 12
A healthcare administrator configure a Nutanix cluster with the following requirements:
* Enable for long-term data retention of large files
* Data should be kept for two years
* Deletion or overwrite of the data must not be allowed
Which Nutanix-enabled technology should the administrator employ to satisfy these requirements?
A. Files - Connected share
B. Files - Read-only share
C. Objects - WORM with versioning
D. Objects - Life Cycle Policy
Answer: C (LEAVE A REPLY)
The Nutanix-enabled technology that meets these requirements is Objects - WORM with versioning. WORM (Write-Once Read-Many) is a feature that prevents anyone from modifying or deleting data in a bucket while the policy is active. WORM policies help comply with strict data retention regulations that mandate how long specific data must be stored. Versioning is a feature that keeps multiple versions of an object in a bucket whenever it is overwritten or deleted. Versioning policies help preserve previous versions of an object for backup or recovery purposes. By enabling WORM and versioning for an Objects bucket, the administrator can ensure that data is kept for two years without being deleted or overwritten. Reference: Nutanix Objects User Guide, page 17; Nutanix Objects Solution Guide, page 9

NEW QUESTION: 13
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
Answer: (SHOW ANSWER)
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. Reference: Nutanix Files Administration Guide, page 27; Nutanix Files Solution Guide, page 6

NEW QUESTION: 14
An organization currently has a Files cluster for their office data including all department shares. Most of the data is considered cold Data and they are looking to migrate to free up space for future growth or newer data.
The organization has recently added an additional node with more storage. In addition, the organization is using the Public Cloud for .. storage needs.
What will be the best way to achieve this requirement?
A. Enable Smart Tiering in Files within the File Console.
B. Setup another cluster and replicate the data with Protection Domain.
C. Backup the data using a third-party software and replicate to the cloud.
D. Migrate cold data from the Files to tape storage.
Answer: (SHOW ANSWER)

NEW QUESTION: 15
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.
Answer: (SHOW ANSWER)
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. Reference: Nutanix Objects User Guide, page 9; Nutanix Objects Deployment Guide

NEW QUESTION: 16
An administrator needs to allow individual users to restore files and folders hosted in Files.
How can the administrator meet this requirement?
A. Configure a Protection Domain for the shares/exports.
B. Configure a Protection Domain on the FSVMs.
C. Enable Self-Service Restore on shares/exports.
D. Enable Self-Service Restore on the FSVMs.
Answer: C (LEAVE A REPLY)
Self-Service Restore (SSR) is a feature that allows individual users to restore files and folders hosted in Files without requiring administrator intervention. SSR can be enabled on a per-share or per-export basis, and users can access the snapshots of their data through a web portal or a Windows client application1. Reference: Nutanix Files Administration Guide1

NEW QUESTION: 17
What is the binary image extension of File Analytics?
A. JSON
B. QCOW2
C. ISO
D. VMDK
Answer: B (LEAVE A REPLY)
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

NEW QUESTION: 18
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.
Answer: B (LEAVE A REPLY)
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.

Reference: Nutanix Files Administration Guide, page 75; Nutanix Files Self-Service Restore Guide

NEW QUESTION: 19
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.
Answer: B (LEAVE A REPLY)
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. Reference: Nutanix Volumes Administration Guide, page 25; Nutanix Volumes Security Guide

NEW QUESTION: 20
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
Answer: (SHOW ANSWER)
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

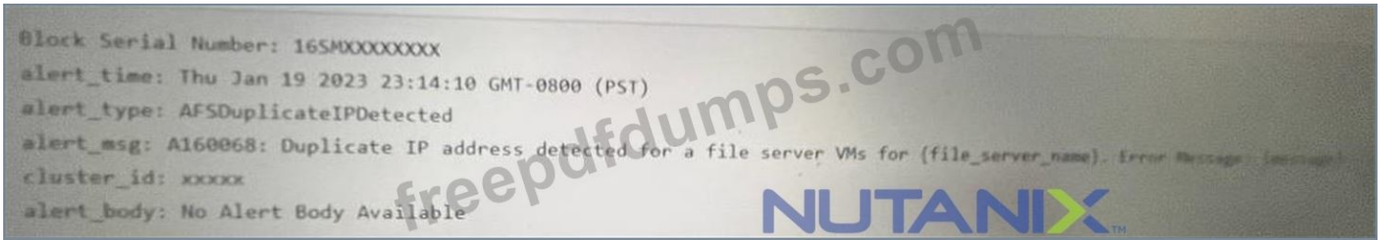
NEW QUESTION: 21
Which protocols are supported by Files?
A. SMBv2 SMBv3, NFSv2, NFSv3
B. SMBv1. SMBv2, NFSv2, NFSv3
C. SMBv1. SMBv2, NFSv3, NFSv4
D. SMBv2 SMBv3, NFSv3, NFSv4
Answer: (SHOW ANSWER)
The protocols that are supported by Files are SMBv2, SMBv3, NFSv3, and NFSv4. SMB (Server Message Block) 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

NEW QUESTION: 22
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.
Answer: C (LEAVE A REPLY)
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

NEW QUESTION: 23
An existing Object bucket was created for backups with these requirements:
* WORM policy of one year
* Versioning policy of one year
* Lifecycle policy of three years
A recent audit has reported a compliance failure. Data that should be retained for three years has been deleted prematurely.
How should the administrator resolve the compliance failure within Objects?

A. Modify the existing bucket versioning policy from one year to three years.
B. Recreate a new bucket with the retention policy of three years.
C. Modify the existing bucket WORM policy from one year to three years.
D. Create a tiering policy to store deleted data on cold storage for three years.
Answer: C (LEAVE A REPLY)
The administrator should resolve the compliance failure within Objects by modifying the existing bucket WORM (Write-Once Read-Many) policy from one year to three years. WORM is a feature that prevents anyone from modifying or deleting data in a bucket while the policy is active. WORM policies help comply with strict data retention regulations that mandate how long specific data must be stored. The administrator can extend the WORM retention period for a bucket at any time, but cannot reduce it or delete it. By extending the WORM policy from one year to three years, the administrator can ensure that data in the bucket is retained for the required duration and not deleted prematurely. Reference: Nutanix Objects User Guide, page 17; Nutanix Objects Solution Guide, page 9

NEW QUESTION: 24
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?
A. Tcpkill.log
B. Minerva_cvm.log
C. Solver.log
D. Minerva.nvm.log
Answer: B (LEAVE A REPLY)
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

NEW QUESTION: 25
Immediately after creation, the administrator is asked to change the name of Objects store.
How will the administrator achieve this request?
A. Enable versioning and then rename the Objects 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.
D. Update the name of the Objects stores by using a CORS XML file
Answer: C (LEAVE A REPLY)
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

NEW QUESTION: 26
Which ransomware prevention solution for Files is best when the list of malicious file signatures to block is greater than 300?
A. Third-party solution
B. Flow Security Central
C. Data Lens
D. File Analytics
Answer: A (LEAVE A REPLY)
Nutanix Files provides a built-in ransomware prevention feature that allows administrators to block malicious file signatures from being written to the file system. However, this feature has a limit of 300 signatures per share or export. If the list of malicious file signatures to block is greater than 300, a third-party solution is recommended2. Reference: Nutanix Files Administration Guide2

NEW QUESTION: 27
What best describes the data protection illustrated in the exhibit?
A. Smart DR
B. Metro Availability
C. Availability Zones
D. NearSync
Answer: A (LEAVE A REPLY)
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. Reference: Nutanix Files Administration Guide, page 79; Nutanix Files Solution Guide, page 9

NEW QUESTION: 28

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.
Answer: (SHOW ANSWER)
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. Reference: Nutanix Objects User Guide, page 13; Nutanix Objects Solution Guide, page 8

NEW QUESTION: 29
Which two steps are required for enabling Data Lens? (Choose two.)
A. In Prism, enable Pulse health monitoring.
B. Configure a MyNutanix account to access the Data Lens console-
C. Add File Services VM admin credentials to a MyNutanix account.
D. Configure the Data Services IP in Prism Central.
Answer: D (LEAVE A REPLY)
The two steps that are required for enabling Data Lens are:
In Prism, enable Pulse health monitoring: Pulse is a feature that collects diagnostic and usage information from Nutanix clusters and services and sends it to Nutanix for analysis and support purposes. Pulse health monitoring is a feature that monitors the health status of Nutanix clusters and services and sends alerts to Nutanix if any issues are detected. To enable Data Lens, Pulse health monitoring must be enabled in Prism Element or Prism Central.
Configure the Data Services IP in Prism Central: Data Services IP is an IP address that is used for communication between Prism Central and Data Lens. Data Services IP must be configured in Prism Central before enabling Data Lens for any file server. Data Services IP must be routable from both Prism Central and Data Lens. Reference: Nutanix Files Administration Guide, page 93; Nutanix Data Lens Deployment Guide

NEW QUESTION: 30
What is the minimum and maximum file size limitations for Smart Tiering?
A. 64 KiB minimum and 15 TiB maximum
B. 128 IOB minimum and 5 TiB maximum

C. 64 KiB minimum and 5 TiB maximum
D. 128 KiB minimum and 13 TiB maximum
Answer: (SHOW ANSWER)
Smart Tiering is a feature that allows Files to tier data across different storage tiers based on the file size and access frequency. Smart Tiering supports files with a minimum size of 64 KiB and a maximum size of 5 TiB2. Reference: Nutanix Files Administration Guide2

NEW QUESTION: 31
After configuring Smart DR, an administrator is unable see the policy in the Policies tab. The administrator has confirmed that all FSVMs are able to connect to Prism Central via port 9440 bidirectional.
What is the possible reason for this issue?
A. The primary and recovery file servers do not have the same protocols.
B. Port 7575 should be open for all External/Client IPS of FSVMs on the Source and Target cluster.
C. The primary and recovery file servers do not have the same version.
D. Port 7575 should be open for all Internal/Storage IPs of FSVMs on the Source and Target.
Answer: B (LEAVE A REPLY)
Smart DR is a feature that allows share-level replication between active file server instances for disaster recovery. To configure Smart DR, one of the prerequisites is to open TCP port 7575 for all External/Client IPs of FSVMs on the Source and Target cluster. This port is used for communication between the FSVMs and Prism Central. If this port is not open, Smart DR policies will not be visible in the Policies tab in Prism Central. Reference: Nutanix Files Administration Guide, page 79; Nutanix Files Solution Guide, page 9

NEW QUESTION: 32
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?
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 (LEAVE A REPLY)
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