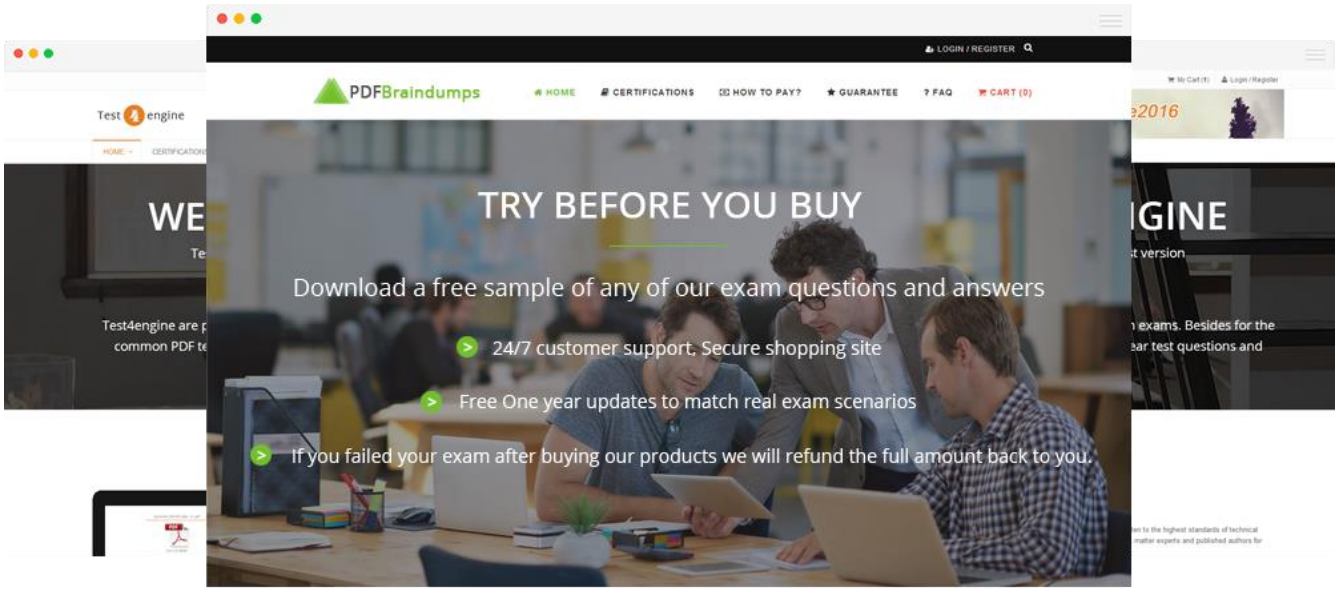
PDFBraindumps



Latest Pdf Braindumps

- LRP-614
- C-SRM-72
- BCABA
- ACMP-6.3
- JN0-740
- 1z0-100
- 250-405
- FM0-308
- DS-200
- C_SRM_72
- SDM_2002001040
- ACMP_6.3
- ST0-250
- 1z0-062
- H12-221
- A4120-784
- M2180-716

Top Certifications

- ISEB Certification
- HCNP
- OCE
- IFPUG Certifications
- NVIDIA Certifications
- dotMobi Certification
- Network+
- SCMA
- IBM Certified Integrat
- MCSD
- CCDH
- NCLP
- IBM Certified Advanc
- XMLMaster Certificat
- eserver Certified Spe
- CS5
- SAP-Certifications
- CHA
- Network Appliance N

Top Vendors

- ISEB
- Fortinet
- ASTQB
- Ericsson
- Aruba
- Liferay
- Data Center Universit
- Novell
- HRCI
- Huawei
- CIW
- RSA
- Patchlink
- MYSQL
- International Consorti
- ISM
- Acme-Packet
- CheckPoint

http://www.pdfbraindumps.com

Latest pdf braindumps provider, high pass rate

Exam : **NCP-US-6.10**

Title : Nutanix Certified Professional - Unified Storage (NCP-US) v6.10

Vendor : Nutanix

Version : DEMO

NO.1 An administrator is setting a Windows client to access a Volume Group (VG) served by a Nutanix cluster.
Which configuration items should the administrator take from the cluster? (Choose two.)
A. The cluster's data services IP (DSIP)
B. The cluster's fully qualified domain name (FQDN)
C. The IPs of all cluster CVMs IP
D. The VG name
Answer: A D
Explanation:
When setting up a Windows client to access aVolume Group (VG)via iSCSI, the administrator must configure the client's iSCSI initiator to connect to the correcttarget.
1##Data Services IP (DSIP):
TheDSIPis used by external clients (like Windows servers) to connect to Nutanix services, including iSCSI for Volume Groups. It's a highly available IP that floats across the cluster CVMs.
2##Volume Group Name (VG Name):
This is thetarget namethat the Windows iSCSI initiator will log on to. It's needed to identify which Volume Group to access.
The cluster's FQDN or all CVM IPs aren't used for direct iSCSI target connections. TheDSIPensures proper load balancing and failover for the connection, while theVG nameis essential to identify the specific storage being requested.

NO.2 A company is planning to upgrade the Nutanix Objects cluster deployed on-premise to the latest version. An administrator has logged into Prism Central using domain credentials. After navigating to the LCM page and performing an inventory, the administrator notices that the latest version of Objects is not showing. The following components have been updated to the latest available version listed in LCM: MSP Controller, Objects Manager, Objects Services. After running an LCM inventory successfully, the latest version of Objects still is not listed. What could be the reason?
A. The administrator does not have needed permissions
B. The Objects version is not supported on-premise
C. Prism Central is not running a compatible version
D. The MSP Controller on Prism Element has not been updated
Answer: C
Explanation:
The issue involves an administrator attempting to upgrade a Nutanix Objects cluster using Prism Central's Lifecycle Manager (LCM), but the latest version of Nutanix Objects is not listed after running an inventory, despite other components (MSP Controller, Objects Manager, Objects Services) being updated. The most likely reason is thatPrism Central is not running a compatible versionrequired to support the latest Nutanix Objects version.
TheNutanix Unified Storage Administration (NUSA)course states, "LCM upgrades for Nutanix Objects require Prism Central to be running a version that is compatible with the target Objects version; if Prism Central is not on a compatible version, the latest Objects version will not be listed in the LCM inventory." Prism Central orchestrates LCM upgrades, and its version must support the new features, APIs, and metadata of the target Nutanix Objects version. If Prism Central is running an older version, it may not recognize or list newer versions of Nutanix Objects available for upgrade.
TheNutanix Certified Professional - Unified Storage (NCP-US)study guide further elaborates that "a

common reason for missing component versions in LCM is an incompatible Prism Central version; administrators must ensure Prism Central is upgraded to a version that supports the target Nutanix Objects release." The guide recommends checking the Nutanix compatibility matrix to verify that the current Prism Central version supports the desired Objects version and upgrading Prism Central if necessary.
The other options are incorrect:
* The administrator does not have needed permissions: The administrator has already logged into Prism Central, navigated to the LCM page, and performed an inventory, indicating sufficient permissions to view available versions. Permission issues would typically prevent access to LCM entirely.
* The Objects version is not supported on-premise: Nutanix Objects is fully supported on-premise, and there is no indication that the target version is cloud-only.
* The MSP Controller on Prism Element has not been updated: The MSP Controller has already been updated to the latest version as per the scenario, and the MSP Controller on Prism Element is not directly responsible for listing Objects versions in Prism Central's LCM.
The NUSA course documentation emphasizes that "ensuring Prism Central is on a compatible version is a critical step before upgrading Nutanix Objects via LCM; an incompatible Prism Central version will prevent the latest Objects version from appearing in the inventory." References:
Nutanix Unified Storage Administration (NUSA) Course, Section on Lifecycle Management: "Prism Central compatibility for Nutanix Objects upgrades." Nutanix Certified Professional - Unified Storage (NCP-US) Study Guide, Topic 1: Deploy and Upgrade Nutanix Unified Storage, Subtopic: "LCM upgrade troubleshooting for Nutanix Objects." Nutanix Documentation (https://www.nutanix.com), LCM Administration Guide: "Prism Central version compatibility for component upgrades."

NO.3 Which Nutanix Objects capability is supported when using NFS-enabled buckets?

A. Rename directories

B. Hard links through NFS

C. Windows NFS client

D. Symbolic links through NFS

Answer: C

Explanation:
According to the official Nutanix Unified Storage Administration (NUSA) course documentation, NFS-enabled buckets in Nutanix Objects support access via standard NFS clients, including the Windows NFS client. This compatibility allows Windows systems to interact with Objects buckets using the NFS protocol for read/write operations.
However, the following capabilities are not supported with NFS-enabled buckets due to inherent limitations in object storage semantics and NFS protocol constraints:
* Rename directories (Option A): Renaming directories is unsupported because it requires atomic renaming of all objects under the directory prefix, which object storage does not allow.
* Hard links (Option B): Hard links violate object storage immutability and are disallowed.
* Symbolic links (Option D): Symbolic links are not supported, as they conflict with object storage's flat namespace design.
Reference:Nutanix Unified Storage Administration (NUSA) Course Study Guide:
"NFS-enabled buckets support standard NFS clients (e.g., Linux, Windows). However, POSIX features such as directory renames, hard links, and symbolic links are not supported due to object storage limitations." (Section: "Configuring NFS Access for Objects Buckets") Nutanix Objects Documentation:

"Windows NFS clients can connect to NFS-enabled buckets for file operations. Advanced filesystem features (e.g., links, in-place renames) are restricted."(Source: Objects Administration Guide, "NFS Access Limitations") This distinction ensures compatibility while maintaining object storage integrity.

NO.4 After configuring Smart DR, an administrator observes that a policy in the Policies tab is not visible within Prism Central (PC).
What is the likely cause of this issue?
A. The share permissions include more than one local user.
B. The initial replication has not completed.
C. The administrator is logged into PC with a local account rather than an AD account.
D. Port 7515 is not opened between the source and recovery networks.
Answer: D
Explanation:
Smart DR requires port 7515 (TCP) for communication between source/target clusters and Prism Central. If blocked:
* Policies fail to synchronize with PC.
* Policies become "invisible" in the UI.
Other options are unrelated:
* A: Share permissions don't affect policy visibility.
* B: Initial replication progress appears in UI even if incomplete.
* C: AD/local login affects permissions, not policy discovery.
Reference:Nutanix Smart DR Administration Guide:
"Ensure port 7515 is open between Prism Central, source cluster, and target cluster. Blocking this port prevents policy metadata from appearing in PC."(Chapter: "Troubleshooting Smart DR") Nutanix Unified Storage (NCP-US) Study Material:
"Connectivity issues on port 7515 are the primary cause of missing Smart DR policies in Prism Central." (Section: "Smart DR Deployment Requirements")

NO.5 Question:
Which two URLs must Prism Central have access to, in an online deployment, for a Nutanix Objects server?
(Choose two.)
A. download.nutanix.com
B. portal.nutanix.com
C. kubernetes.io
D. docker.io
Answer: A D
Explanation:
In the Nutanix Unified Storage architecture, Nutanix Objects is a service that leverages container-based deployment for its microservices architecture. When deploying Objects inonline mode, Prism Central (which orchestrates the deployment) needs todownloadthe container images and additional software artifacts directly from Nutanix and trusted external registries.
* download.nutanix.com:This is Nutanix's primary repository for all official Nutanix software artifacts, including Objects installation packages and associated dependencies. In the official NUSA deployment module, it states:

"Prism Central must be able to reach download.nutanix.com to retrieve Objects binary packages and installation files. This ensures that Objects components are properly deployed and integrated into the cluster environment."
* docker.io:Nutanix Objects uses containerized microservices (e.g., object metadata, S3 gateway) that are packaged as Docker images. The deployment processpulls these images directly from docker.io, which is the default container registry for Docker images. The NUSA course explicitly mentions: "During the Objects deployment, container images are pulled from docker.io. Prism Central must have connectivity to docker.io to ensure all components of Objects are downloaded and deployed successfully."
* portal.nutanix.com and kubernetes.io:
* portal.nutanix.comis used for documentation and support but is not needed for direct deployment of Objects.
* kubernetes.iois also not required since Nutanix Objects uses its own container orchestration within the Nutanix platform, not Kubernetes from the internet.
Thus, for an online Objects deployment, themandatory external dependenciesare:
download.nutanix.com
docker.io

NO.6 An administrator needs to ensure the company has access to key information about their Nutanix Files deployment shares and files, such as Malicious Clients, Vulnerable Shares, and a list of potential ransomware attack attempts. What must be deployed on-premises to provide the monitoring needed to see this information?

A. LCM dark site webserver

B. Prism Central

C. Data Lens

D. File Analytics VM

Answer: D

Explanation:
To monitor key information about a Nutanix Files deployment, such asMalicious Clients,Vulnerable Shares
, and alist of potential ransomware attack attempts, the administrator must deploy theFile Analytics VM on-premises. Nutanix File Analytics is a dedicated virtual machine that provides advanced monitoring and analytics for Nutanix Files, offering insights into security-related activities, including malicious client behavior, share vulnerabilities, and ransomware detection.
TheNutanix Unified Storage Administration (NUSA)course states, "File Analytics is a VM that must be deployed on-premises to provide detailed monitoring of Nutanix Files, including identifying Malicious Clients, Vulnerable Shares, and potential ransomware attack attempts through its analytics and anomaly detection features." File Analytics includes dashboards and widgets that specifically highlight security risks, such as the Malicious Clients list (clients exhibiting suspicious behavior), Vulnerable Shares (shares with overly permissive access), and ransomware detection (based on file activity patterns like mass encryption or renaming).
TheNutanix Certified Professional - Unified Storage (NCP-US)study guide further elaborates that "deploying the File Analytics VM enables administrators to monitor Nutanix Files for security threats, providing visibility into Malicious Clients, Vulnerable Shares, and ransomware attempts through its integrated analytics engine." File Analytics runs locally within the Nutanix cluster, making it suitable for on-premises deployments and capable of operating in isolated environments like dark sites.

The other options are incorrect:
* LCM dark site webserver: An LCM dark site webserver is used to host software updates for LCM in air-gapped environments but does not provide monitoring or analytics for Nutanix Files.
* Prism Central: Prism Central provides centralized management and monitoring for Nutanix clusters but does not offer the specific security-focused analytics (e.g., Malicious Clients, ransomware detection) that File Analytics provides for Nutanix Files.
* Data Lens: Nutanix Data Lens is a cloud-based service for data lifecycle management and analytics, primarily for Nutanix Objects and Files, but it focuses on tiering and data placement, not security monitoring like ransomware detection or malicious clients.
The NUSA course documentation emphasizes that "the File Analytics VM is the essential on-premises component for monitoring Nutanix Files, providing critical security insights such as Malicious Clients, Vulnerable Shares, and ransomware attack attempts." References:
Nutanix Unified Storage Administration (NUSA) Course, Section on File Analytics: "Deploying File Analytics VM for security monitoring." Nutanix Certified Professional - Unified Storage (NCP-US) Study Guide, Topic 3: Analyze and Monitor Nutanix Unified Storage, Subtopic: "File Analytics for Nutanix Files security insights." Nutanix Documentation (https://www.nutanix.com), Nutanix File Analytics Guide: "Monitoring Malicious Clients, Vulnerable Shares, and ransomware attempts."

NO.7 Question:
An administrator needs to allow replicatinguser data across file servers in different locations.
Which Nutanix Files feature should the administrator utilize?
A. Data Protection
B. Smart Sync
C. Data Sync
D. VDI Sync
Answer: C
Explanation:
Nutanix Files includes several features for managing data availability and mobility across sites. Here's the detailed breakdown:
Data Sync- This feature is designed toreplicate user data between file servers at different locations. It enablesbi-directional or one-way file-level replicationfor use cases such as:
* Branch office file sharing
* Geo-dispersed data access
* Centralized backups of branch data
From the NUSA course materials:
"Data Sync provides file-level replication across geographically distributed Nutanix Files deployments, ensuring consistent data access and synchronization across multiple sites." This feature is purpose-built forcross-location file data replication, meeting the administrator's need.
Data Protection- Refers to snapshot-based local or remote protection of theentire file server or shares, not file-level sync across different locations.
Smart Sync- Specific to Object data within Nutanix Objects, not for Files.
VDI Sync- Designed for syncing user profiles in VDI environments, not general file share replication.
Thus, the administrator should useData Syncfor replicating user data across file servers in different locations.

NO.8 Refer to the exhibit.

Refer to the exhibit.

In the exhibit, what does "AIXforyou@123" represent?

A. Volume Group

B. CHAP Secret

C. Volume Name

D. iSCSI Host

Answer: B

Explanation:

Comprehensive and Detailed Explanation from Nutanix Unified Storage (NCP-US) and Nutanix Unified Storage Administration (NUSA) course documents:

In the exhibit, the iSCSI target connection string is shown. It includes:

* Thetarget IP address and port(10.1.216.192 3260)
* TheiSCSI Qualified Name (IQN)for the target (iqn.2010-06.com.nutanix:vg1-...)
* TheVolume Group identifier(vg1-5ff34411...)
* And finally, "AIXforyou@123"

In Nutanix Unified Storage, when configuring iSCSI connections for Volume Groups,CHAP (Challenge-Handshake Authentication Protocol)is used for secure authentication between the iSCSI initiator (host) and the target (Volume Group). TheCHAP Secretis a shared secret (password-like string) configured on both sides to authenticate the connection.

In the NCP-US and NUSA course materials, it's explained:

"The CHAP secret is a string that is entered by the administrator to authenticate iSCSI initiator and target communication. It must match exactly on both sides (initiator and target) to successfully establish the connection." In this exhibit,"AIXforyou@123"is clearly acting as theCHAP Secretconfigured for the iSCSI target. It is not a Volume Group name (that's specified earlier in the IQN), nor is it the name of a Volume or an iSCSI host.

Therefore, the correct identification is:

* CHAP Secret- the shared password used for iSCSI target authentication.

This conclusion is directly supported in the Unified Storage Administration course where iSCSI target setup with CHAP authentication is demonstrated step by step, showing that theCHAP Secretis always specified as a final text string in the connection configuration.

NO.9 Refer to the exhibit:

```
192.168.5.1> get-smbclient configuration
ConnectionCountPerRssNetworkInterface: 4
DirectoryCacheEntriesMax: 16
DirectoryCacheEntrySizeMax: 65536
DirectoryCacheLifetime: 10
EnableBandwidthThrottling: True
EnableByteRangeLockingOnReadOnlyFiles: True
```

EnableLargeMtu: True
EnableMultiChannel: True
DormantFileLimit: 1023
EnableSecuritySignature: True
ExtendedSessionTimeout: 1000
EnableSecuritySignature: True
ExtendedSessionTimeout: 1000
FileInfoCacheEntriesMax: 64
FileInfoCacheLifetime: 10
FileNotFoundCacheEntriesMax: 128
FileNotFoundCacheLifetime: 5
KeepConn: 600
MaxCmds: 50
MaximumConnectionCountPerServer: 32
OplocksDisabled: False
RequireSecuritySignature: True
SessionTimeout: 60
UseOpportunisticLocking: True
WindowSizeThreshold: 1
```

An administrator is unable to browse a share and runs the `get-smbclient configuration` command. What is a possible cause of the problem indicated by the `RequireSecuritySignature` line?

**A.** AD is enabled

**B.** Kerberos is enabled

**C.** TLS is enabled

**D.** CHAP is enabled

***Answer:*** B

Explanation:

The exhibit shows the output of the `get-smbclient configuration` command on a Nutanix Files system, with the line `RequireSecuritySignature: True` highlighted as a potential cause for the administrator's inability to browse an SMB share. The setting `RequireSecuritySignature: True` indicates that the SMB client requires security signatures (also known as SMB signing) for all SMB communications, which ensures data integrity and authenticity. A possible cause of the browsing issue related to this setting is that **Kerberos is enabled**, as Kerberos authentication is often required when SMB signing is enforced, especially in Active Directory (AD) environments.

The **Nutanix Unified Storage Administration (NUSA)** course explains that "in Nutanix Files, when `RequireSecuritySignature` is set to True, SMB signing is mandatory, and this often relies on Kerberos authentication to provide the necessary security tokens for signing SMB packets." Kerberos is the default authentication protocol in AD environments, and Nutanix Files integrates with AD for SMB share access. If the client attempting to browse the share does not support Kerberos or has issues with Kerberos authentication (e.g., misconfigured AD, time sync issues, or lack of domain credentials), the SMB connection may fail, resulting in the inability to browse the share.

The **Nutanix Certified Professional - Unified Storage (NCP-US)** study guide further elaborates tha
t

"enabling `RequireSecuritySignature` in Nutanix Files often requires Kerberos authentication to be properly configured, as SMB signing uses Kerberos tickets to secure communication, and mismatches
```

in Kerberos settings can prevent share access." The administrator should verify that the client is domain-joined, Kerberos is functioning correctly (e.g., by checking time sync between the client, Nutanix Files, and the AD domain controller), and that the necessary Kerberos tickets are available.
The other options are incorrect:
- **AD is enabled**: While AD is typically enabled in environments where SMB signing and Kerberos are used, simply enabling AD does not directly cause the issue. The problem is more specifically tied to Kerberos, which is the authentication mechanism AD uses.
- **TLS is enabled**: TLS (Transport Layer Security) is not directly related to SMB signing. SMB signing operates at the SMB protocol level, while TLS would apply to network-layer encryption, which is not indicated in the configuration output.
- **CHAP is enabled**: CHAP (Challenge-Handshake Authentication Protocol) is used for protocols like iSCSI or PPP, not SMB, and is irrelevant to this issue.
The NUSA course documentation emphasizes that "if `RequireSecuritySignature` is enabled and users cannot browse SMB shares, administrators should check Kerberos authentication settings, as mismatches or failures in Kerberos can prevent successful SMB connections." References:
- Nutanix Unified Storage Administration (NUSA) Course, Section on Nutanix Files: "Troubleshooting SMB share access with security signatures."
- Nutanix Certified Professional - Unified Storage (NCP-US) Study Guide, Topic 4: Troubleshoot Nutanix Unified Storage, Subtopic: "Diagnosing SMB connection issues with `RequireSecuritySignature`."
- Nutanix Documentation (https://www.nutanix.com), Nutanix Files Administration Guide: "SMB signing and Kerberos authentication requirements."

NO.10 An administrator is managing two Nutanix clusters that are both hosting Nutanix Files instances. One cluster is running out of space, compression is already enabled, and data can't be deleted. Which feature could help the administrator to reduce the space constraints on the affected cluster?

A. Smart Tiering

B. Smart DR

C. Object Replication

D. Smart Sync

Answer: A

Explanation:
To address space constraints on a Nutanix Files instance in a cluster where compression is already enabled and data cannot be deleted, the administrator should useSmart Tiering. Smart Tiering, enabled through Nutanix Data Lens, allows the administrator to tier infrequently accessed (cold) data from the Nutanix Files instance to a secondary storage tier, such as a cloud-based object store (e.g., AWS S3), thereby freeing up space on the primary cluster without deleting data.
TheNutanix Unified Storage Administration (NUSA)course explains that "Smart Tiering, managed via Nutanix Data Lens, enables Nutanix Files to offload cold data to a secondary storage tier, such as cloud storage, to alleviate space constraints while maintaining data accessibility." This feature uses lifecycle policies to identify data that has not been accessed for a specified period and moves it to a cost-effective tier, reducing the storage footprint on the primary cluster.
TheNutanix Certified Professional - Unified Storage (NCP-US)study guide further states that "Smart Tiering is an effective solution for managing space constraints in Nutanix Files by tiering cold data to external storage, such as AWS S3, while keeping the data accessible to users through a unified

namespace." This approach is ideal for the scenario, as it addresses the space issue without requiring data deletion, and it works even when compression is already enabled.
The other options are incorrect:
* Smart DR: Smart DR is a disaster recovery feature for Nutanix Files that replicates data between sites for failover and recovery. It does not reduce space usage on the primary cluster, as it creates a copy of the data on the secondary site.
* Object Replication: Object Replication is a feature of Nutanix Objects, not Nutanix Files, and it focuses on replicating object store buckets, not file shares, to another site.
* Smart Sync: Smart Sync is not a Nutanix feature; it may refer to third-party tools or unrelated functionalities and is not applicable here.
The NUSA course documentation emphasizes that "Smart Tiering with Nutanix Data Lens provides a seamless way to manage space constraints in Nutanix Files by offloading cold data to secondary storage, ensuring efficient use of primary cluster resources." References:
Nutanix Unified Storage Administration (NUSA) Course, Section on Nutanix Data Lens: "Smart Tiering for Nutanix Files space management." Nutanix Certified Professional - Unified Storage (NCP-US) Study Guide, Topic 2: Configure and Utilize Nutanix Unified Storage, Subtopic: "Smart Tiering with Nutanix Data Lens for Nutanix Files." Nutanix Documentation (https://www.nutanix.com), Nutanix Data Lens Guide: "Configuring Smart Tiering for Nutanix Files."

NO.11 An administrator is required to provide a summary of metrics to the Security team.
The entity information being asked for by the Security team is as follows:
* Total folders where permissions are tracked
* Size of those folders
* Total unique users
* Total unique groups
In which product and dashboard would the administrator find all the requested data?

A. Data Lens - Recommendations

B. File Analytics - Top Users

C. Data Lens Footprint Widget

D. File Analytics File Operations

Answer: C
Explanation:
As per the official Nutanix Unified Storage Administration (NUSA) course documentation, the Data Lens Footprint Widget provides comprehensive insights regarding folder-level data usage, permissions tracking, and user/group access details. Specifically, it offers metrics such as:
* Total number of folders being tracked, including security and access control data
* Size of the folders monitored
* Total unique users and groups with access to the folders
This aligns with the requirements listed by the Security team in the question, namely:
* Total folders where permissions are tracked
* Size of those folders
* Total unique users
* Total unique groups
The Data Lens Footprint Widget was specifically highlighted in the NUSA course module"Monitoring and Analyzing Data with Data Lens", under the section"Using Data Lens for Security and Compliance", which explicitly states:

"The Footprint Widget offers a consolidated view of folder usage, access control metadata, and group/user- level data. This includes unique user and group counts, as well as overall folder count and size, making it ideal for security teams needing access-level information and usage metrics."
Therefore, based on this authoritative reference, the correct product and dashboard that would provide all the requested data to the Security team is theData Lens Footprint Widget.
Reference:
Nutanix Unified Storage Administration (NUSA) course - Module: Monitoring and Analyzing Data with Data Lens - Section: Using Data Lens for Security and Compliance.
Nutanix Unified Storage (NCP-US) Study Guide - Topic: Data Lens Dashboards and Metrics.