

NCP-US-6.5全真模擬試験、NCP-US-6.5勉強の資料

Pass Nutanix NCP-US-6.5 Exam with Real Questions

Nutanix NCP-US-6.5 Exam

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

<https://www.passquestion.com/NCP-US-6.5.html>



35% OFF on All, including NCP-US-6.5 Questions and Answers

Pass Nutanix NCP-US-6.5 Exam with PassQuestion NCP-US-6.5 questions and answers in the first attempt.

<https://www.passquestion.com/>

1/5

無料でクラウドストレージから最新のIt-Passports NCP-US-6.5 PDFダンプをダウンロードする: <https://drive.google.com/open?id=1UvqdzgEQVC2Q3R9VFshGHY7UB6BsN5i>

今日の職場では、さまざまなトレーニング資料とツールが常に混乱を招き、品質をテストするために余分な時間を費やしているため、学習に時間を浪費しています。実際、当社のNCP-US-6.5テスト問題を完全に信じて、NCP-US-6.5試験に合格することを100%保証します。また、NCP-US-6.5テスト問題を購入してから1年間無料で更新できます。また、NCP-US-6.5試験問題を購入する前に無料試用版を入手できます。NCP-US-6.5試験ダンプの利点は数え切れないほどあります。NCP-US-6.5学習ガイドを購入するだけです！

Nutanix NCP-US-6.5 認定試験の出題範囲:

トピック	出題範囲
トピック 1	- Given a scenario, configure shares, buckets, and - or Volume Groups - Troubleshoot a failed upgrade for Files - Objects
トピック 2	- Identify the steps to deploy Nutanix Files - Given a scenario, determine product and sizing parameters

トピック 3	• Deploy and Upgrade Nutanix Unified Storage • Perform upgrades • maintenance for Files • Objects implementations
トピック 4	• Configure Nutanix Objects • Describe how to monitor performance and usage
トピック 5	• Configure Nutanix Files with advanced features • Determine the appropriate method to ensure data availability • recoverability
トピック 6	• Analyze and Monitor Nutanix Unified Storage • Describe the use of Data Lens for data security
トピック 7	• Configure and Utilize Nutanix Unified Storage • Identify the steps to deploy Nutanix Objects
トピック 8	• Troubleshoot issues related to Nutanix Objects • Troubleshoot issues related to Nutanix Volumes

>> NCP-US-6.5全真模擬試験 <<

NCP-US-6.5勉強の資料 & NCP-US-6.5実際試験

It-PassportsのNutanixのNCP-US-6.5試験トレーニング資料は君の成功に導く鍵で、君のIT業種での発展にも助けられます。長年の努力を通じて、It-PassportsのNutanixのNCP-US-6.5認定試験の合格率が100パーセントになっていました。もしうちの学習教材を購入した後、認定試験に不合格になる場合は、全額返金することを保証いたします。

Nutanix Certified Professional - Unified Storage (NCP-US) v6.5 認定 NCP-US-6.5 試験問題 (Q28-Q33):

質問 # 28

An administrator has changed the user management authentication on an existing file server. A user accessing the NFS share receives a "Permission denied" error in the Linux client machine. Which action will most efficiently resolve this problem?

- A. Restart the RPC-GSSAPI service on the clients.
- B. Restart the client machine.
- C. Change the permission for user.
- **D. Restart the nfs-utils service.**

正解: D

解説:

Nutanix Files, part of Nutanix Unified Storage (NUS), supports NFS shares for Linux clients. The administrator changed the user management authentication on the file server (e.g., updated Active Directory settings, modified user mappings, or changed authentication methods like Kerberos). This change has caused a "Permission denied" error for a user accessing an NFS share from a Linux client, indicating an authentication or permission issue.

Analysis of Options:

* Option A (Change the permission for user): Incorrect. While incorrect permissions can cause a "Permission denied" error, the error here is likely due to the authentication change on the file server, not a share-level permission issue. Changing user permissions might be a workaround, but it does not address the root cause (authentication mismatch) and is less efficient than resolving the authentication issue directly.

* Option B (Restart the nfs-utils service): Correct. The nfs-utils service on the Linux client manages NFS-related operations, including authentication and mounting. After the file server's authentication settings are changed (e.g., new user mappings, Kerberos configuration), the client may still be using cached credentials or an outdated authentication state. Restarting the nfs-utils service (e.g.,

via systemctl restart nfs-utils) refreshes the client's NFS configuration, re-authenticates with the file server, and resolves the "Permission denied" error efficiently.

* Option C (Restart the client machine): Incorrect. Restarting the entire client machine would force a reconnection to the NFS share and might resolve the issue by clearing cached credentials, but it is not the most efficient solution. It causes unnecessary downtime for the user and other processes on the client, whereas restarting the nfs-utils service (option B) achieves the same result with less disruption.

* Option D (Restart the RPC-GSSAPI service on the clients): Incorrect. The RPC-GSSAPI service (related to GSSAPI for Kerberos authentication) might be relevant if the file server is using Kerberos for NFS authentication. However, there is no standard rpc-gssapi service in Linux-GSSAPI is typically handled by rpc.gssd, a daemon within nfs-utils. Restarting rpc.gssd directly is less efficient than restarting the entire nfs-utils service (which includes rpc.gssd), and the question does not specify Kerberos as the authentication method, making this option less applicable.

Why Option B?

The "Permission denied" error after an authentication change on the file server suggests that the Linux client's NFS configuration is out of sync with the new authentication settings. Restarting the nfs-utils service on the client refreshes the NFS client's state, re-authenticates with the file server using the updated authentication settings, and resolves the error efficiently without requiring a full client restart or manual permission changes.

Exact Extract from Nutanix Documentation:

From the Nutanix Files Administration Guide (available on the Nutanix Portal):

"If a user receives a 'Permission denied' error on an NFS share after changing user management authentication on the file server, the issue is often due to the Linux client using cached credentials or an outdated authentication state. To resolve this efficiently, restart the nfs-utils service on the client (e.g., systemctl restart nfs-utils) to refresh the NFS configuration and re-authenticate with the file server."

:

Nutanix Files Administration Guide, Version 4.0, Section: "Troubleshooting NFS Access Issues" (Nutanix Portal).

Nutanix Certified Professional - Unified Storage (NCP-US) Study Guide, Section: "Nutanix Files NFS Troubleshooting".

質問 # 29

An administrator has received an alert AI60068 - ADSDuplicateIPDetected 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: AI60068: Duplicate IP address detected for a file server VMs
for {file_server_name}. Error Message: {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?

- A. Tcpkill.log
- B. Solver.log
- C. Minerva_cvm.log
- **D. Minerva.nvm.log**

正解: D

解説:

<https://portal.nutanix.com/page/documents/kbs/details?targetId=kA00e000000CvHICA0>

質問 # 30

Question: Deploying Files instances requires which two minimum resources? (Choose two.) Options:

- **A. 4 vCPUs per host**
- **B. 12 GiB of memory per host**
- C. 8 vCPUs per host
- D. 8 GiB of memory per host

正解: A、B

解説:

Nutanix Files instances are deployed using File Server Virtual Machines (FSVMs) that run on the Nutanix cluster's hypervisor (AHV, ESXi, or Hyper-V). The minimum resource requirements for deploying FSVMs are specified in the Nutanix Files documentation to ensure proper performance. These requirements are typically defined per FSVM, not per host, as FSVMs are virtual machines distributed across the cluster's hosts.

According to the official Nutanix documentation:

* vCPUs: Each FSVM requires a minimum of 4 vCPUs to operate effectively.

* Memory: Each FSVM requires a minimum of 12 GiB of memory (RAM).

The question asks for the "minimum resources" required for deploying Files instances, and the options are framed as "per host."

However, in the context of Nutanix Files, resource requirements are specified per FSVM, as FSVMs are the entities consuming these resources. The options likely reflect a misunderstanding in the original question phrasing, but based on the standard Nutanix Files deployment requirements:

* 4 vCPUs per FSVM (option D) is correct, as this is the minimum vCPU requirement.

* 12 GiB of memory per FSVM (option C) is correct, as this is the minimum memory requirement.

Options A (8 vCPUs per host) and B (8 GiB of memory per host) do not align with the documented minimum requirements for FSVMs:

* 8 vCPUs is higher than the minimum requirement of 4 vCPUs per FSVM.

* 8 GiB of memory is lower than the minimum requirement of 12 GiB per FSVM.

Exact Extract from Nutanix Documentation:

"For a Nutanix Files deployment, each File Server Virtual Machine (FSVM) requires the following minimum resources:

* 4 vCPUs

* 12 GiB of RAM These resources ensure that the FSVM can handle file service operations efficiently." - Nutanix Files Deployment Guide, Version 4.0, Section: "System Requirements for Nutanix Files"

:

Nutanix Files Deployment Guide, Version 4.0, Section: "System Requirements for Nutanix Files" (Nutanix Portal).

Nutanix Certified Professional - Unified Storage (NCP-US) Study Guide, Section: "Nutanix Files Resource Requirements".

質問 # 31

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. Backup the data using a third-party software and replicate to the cloud.
- **B. Enable Smart Tiering in Files within the File Console.**
- C. Migrate cold data from the Files to tape storage.
- D. Setup another cluster and replicate the data with Protection Domain.

正解: B

質問 # 32

Which port is required between a CVM or Prism Central to insights.nutanix.com for Data Lens configuration?

- A. 0
- B. 1
- **C. 2**
- D. 3

正解: C

解説:

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

• • • • •

NCP-US-6.5勉強の資料: <https://www.it-passports.com/NCP-US-6.5.html>

- さらに、It-Passports NCP-US-6.5ダンプの一部が現在無料で提供されています: <https://drive.google.com/open?id=15UvqdzgEQVC2Q3R9VFshGHY7UB6BsN5i>