퍼펙트한NCP-US-6.5시험대비공부최신덤프모음집

BONUS!!! Itcertkr NCP-US-6.5 시험 문제집 전체 버전을 무료로 다운로드하세요: https://drive.google.com/open?id=1mO-IDdHdhWonMBjdSNio2TWyljDWt8sM

목표를 이루는 방법은 여러가지가 있는데 어느 방법을 선택하면 가장 빨리 목표를 이룰수 있을가요? Nutanix인증 NCP-US-6.5시험을 패스하는 길에는Itcertkr의Nutanix인증 NCP-US-6.5덤프를 공부하는 것이 가장 좋은 방법이라는 것을 굳게 약속드립니다. Itcertkr의Nutanix인증 NCP-US-6.5덤프는 시험문제에 초점을 두어 제작된 공부자료이기에 Nutanix인증 NCP-US-6.5패스를 가장 빠른 시일내에 한방에 할수 있도록 도와드립니다.

Nutanix NCP-US-6.5 시험요강:

주제	소개
주제 1	• Analyze and Monitor Nutanix Unified Storage • Describe the use of Data Lens for data security
주제 2	• Configure Nutanix Objects • Describe how to monitor performance and usage
주제 3	• Configure Nutanix Files with advanced features • Determine the appropriate method to ensure data availability • recoverability
주제 4	• Utilize File Analytics for data security • Troubleshoot Nutanix Unified Storage • Configure Nutanix Volumes
주제 5	• Troubleshoot issues related to Nutanix Objects • Troubleshoot issues related to Nutanix Volumes
주제 6	• Troubleshoot issues related to Nutanix Files • Explain Data Management processes for Files and Objects
주제 7	• Identify the steps to deploy Nutanix Files • Given a scenario, determine product and sizing parameters
주제 8	• Given a scenario, configure shares, buckets, and • or Volume Groups • Troubleshoot a failed upgrade for Files • Objects

NCP-US-6.5인증시험 인기 덤프문제 - NCP-US-6.5시험기출문제

Nutanix 인증 NCP-US-6.5시험대비덤프를 찾고 계시다면Itcertkr가 제일 좋은 선택입니다.저희Itcertkr에서는 여라가지 IT자격증시험에 대비하여 모든 과목의 시험대비 자료를 발췌하였습니다. Itcertkr에서 시험대비덤프자료를 구입하시면 시험불합격시 덤프비용환불신청이 가능하고 덤프 1년 무료 업데이트서비스도 가능합니다. Itcertkr를 선택하시면 후회하지 않을것입니다.

최신 Nutanix Certified Professional (NCP) NCP-US-6.5 무료샘플문제 (Q41-Q46):

질문 # 41
An administrator has been requested to set up a Files instance in a Nutanix environment. After testing data in the environment, it was determined an estimated 4,000 connections on average will be needed per node. What is the proper memory sizing that the administrator should use to configure this environment?

- A. 40 GiB RAM per node
- B. 128 GiB RAM per node
- C. 32 GiB RAM per node
- D. 96 GiB RAM per node

정답：D

설명：
Nutanix Files, part of Nutanix Unified Storage (NUS), uses File Server Virtual Machines (FSVMs) to manage file services (e.g., SMB, NFS). Each FSVM runs on a node in the Nutanix cluster, and the number of connections per node impacts the resource requirements, particularly memory (RAM), for the FSVMs. The administrator needs to size the memory for a Files instance where each node will handle an average of 4,000 connections.
Sizing Guidelines:
Nutanix provides sizing guidelines for Files deployments based on the number of connections per FSVM (and thus per node, assuming one FSVM per node, which is the default configuration). The memory requirements scale with the number of connections to ensure performance and stability:
* The minimum memory per FSVM is 12 GiB (as noted in Question 2), which supports up to 1,000 connections.
* For higher connection counts, Nutanix recommends increasing the memory proportionally.
According to Nutanix documentation:
* Up to 1,000 connections: 12 GiB RAM per FSVM.
* 1,000 to 2,000 connections: 24 GiB RAM per FSVM.
* 2,000 to 4,000 connections: 48 GiB RAM per FSVM.
* 4,000 to 8,000 connections: 96 GiB RAM per FSVM.
Since the question specifies 4,000 connections per node, and assuming one FSVM per node (standard deployment), the FSVM on each node needs to handle 4,000 connections. Based on the sizing guidelines:
* 4,000 connections fall into the 4,000 to 8,000 range, requiring 96 GiB RAM per FSVM.
* Since each node hosts one FSVM, this translates to 96 GiB RAM per node dedicated to the FSVM.
Analysis of Options:
* Option A (32 GiB RAM per node): Incorrect. 32 GiB RAM per node is sufficient for up to 2,000 connections (24 GiB for the FSVM, plus some overhead), but it is insufficient for 4,000 connections, which require 96 GiB.
* Option B (40 GiB RAM per node): Incorrect. 40 GiB RAM per node is still too low for 4,000 connections, as it falls short of the 96 GiB recommended for this connection range.
* Option C (96 GiB RAM per node): Correct. 96 GiB RAM per node aligns with Nutanix's sizing guidelines for an FSVM handling 4,000 to 8,000 connections, ensuring the Files instance can manage the expected load efficiently.
* Option D (128 GiB RAM per node): Incorrect. While 128 GiB RAM per node would work, it exceeds the recommended sizing for 4,000 connections. Nutanix recommends 96 GiB for up to 8,000 connections, and 128 GiB is typically reserved for even higher connection counts (e.g., >8,000) or additional workloads on the node. The question asks for the "proper" sizing, which is the minimum recommended for the given load, making 96 GiB the correct choice.
Why Option C?
For 4,000 connections per node, Nutanix recommends 96 GiB RAM per FSVM (one FSVM per node), which translates to 96 GiB RAM per node dedicated to the FSVM. This ensures the Files instance can handle the connection load without performance degradation, aligning with Nutanix's sizing guidelines.

Exact Extract from Nutanix Documentation:
From the Nutanix Files Sizing Guide (available on the Nutanix Portal):
"For Nutanix Files deployments, memory sizing depends on the number of connections per FSVM. For 4,000 to 8,000 connections, allocate 96 GiB of RAM per FSVM. Assuming one FSVM per node, this translates to
96 GiB RAM per node dedicated to the FSVM to ensure optimal performance." Additional Notes:
* The question assumes one FSVM per node, which is the default configuration for Nutanix Files unless otherwise specified. If multiple FSVMs were on a single node, the total RAM would need to be adjusted, but the question's phrasing ("per node") aligns with the standard one-FSVM-per-node deployment.
* The 96 GiB RAM is for the FSVM itself; the node may require additional RAM for other workloads (e.
g., CVM, VMs), but the question focuses on the Files instance's memory sizing, making 96 GiB the correct answer.
:
Nutanix Files Sizing Guide, Version 4.0, Section: "Memory Sizing for Nutanix Files" (Nutanix Portal).
Nutanix Certified Professional - Unified Storage (NCP-US) Study Guide, Section: "Nutanix Files Sizing and Performance".

질문 # 42
What is the minimum and maximum file size limitations for Smart Tiering?

- A. 64 KiB minimum and 5 TiB maximum
- B. 128 KiB minimum and 13 TiB maximum
- C. 128 IOB minimum and 5 TiB maximum
- D. 64 KiB minimum and 15 TiB maximum

정답： A

설명:
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

질문 # 43
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?

- A. Files Console Share View
- B. Files Console Monitoring View
- C. Files Console Data Management View
- D. Files Console Dashboard View

정답： D

설명:
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. References: Nutanix Files Administration Guide2

질문 # 44
With the settings shown on the exhibit, if there were 1000 files in the repository, how many files would have to be... anomaly alert to the administrator?

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

정답：C

설명：
With the settings shown on the exhibit, if there were 1000 files in the repository, 10 files would have to be deleted within an hour to trigger an anomaly alert to the administrator. Anomaly alert is a feature that notifies the administrator when there is an unusual or suspicious activity on file data, such as mass deletion or encryption. Anomaly alert can be configured with various parameters, such as threshold percentage, time window, minimum number of files, and so on. In this case, the threshold percentage is set to 1%, which means that if more than 1% of files in a repository are deleted within an hour, an anomaly alert will be triggered.
Since there are 1000 files in the repository, 1% of them is 10 files. Therefore, if 10 or more files are deleted within an hour, an anomaly alert will be sent to the administrator. References: Nutanix Files Administration Guide, page 98; Nutanix Data Lens User Guide

질문 # 45
An administrator needs to add a signature to the ransomware block list. How should the administrator complete this task?

- A. Search the Block List for the file signature to be added, click Add to Block List when the signature is not found in File Analytics.
- B. Open a support ticket to have the new signature added. Nutanix support will provide an updated Block List file.
- C. Add the file signature to the Blocked Files Type in the Files Console.
- D. Download the Block List CSV file, add the new signature, then upload the CSV.

정답：B

설명：
Nutanix Files, part of Nutanix Unified Storage (NUS), can protect against ransomware using integrated tools like File Analytics and Data Lens, or through integration with third-party solutions. In Question 56, we established that a third-party solution is best for signature-based ransomware prevention with a large list of malicious file signatures (300+). The administrator now needs to add a new signature to the ransomware block list, which refers to the list of malicious file signatures used for blocking.
Analysis of Options:
* Option A (Open a support ticket to have the new signature added. Nutanix support will provide an updated Block List file): Correct. Nutanix Files does not natively manage a signature-based ransomware block list within its own tools (e.g., File Analytics, Data Lens), as these focus on behavioral detection (as noted in Question 56). For signature-based blocking, Nutanix integrates with third-party solutions, and the block list (signature database) is typically managed by Nutanix or the third-party provider. To add a new signature, the administrator must open a support ticket with Nutanix, who will coordinate with the third-party provider (if applicable) to update the Block List file and provide it to the customer.
* Option B (Add the file signature to the Blocked Files Type in the Files Console): Incorrect. The "Blocked Files Type" in the Files Console allows administrators to blacklist specific file extensions (e.
g., .exe, .bat) to prevent them from being stored on shares. This is not a ransomware block list based on signatures-it's a simple extension-based blacklist, and file signatures (e.g., hashes or patterns used for ransomware detection) cannot be added this way.
* Option C (Search the Block List for the file signature to be added, click Add to Block List when the signature is not found in File Analytics): Incorrect. File Analytics provides ransomware detection through behavioral analysis (e.g., anomaly detection, as in Question 7), not signature-based blocking.
There is no "Block List" in File Analytics for managing ransomware signatures, and it does not have an "Add to Block List" option for signatures.
* Option D (Download the Block List CSV file, add the new signature, then upload the CSV): Incorrect. Nutanix Files does not provide a user-editable Block List CSV file for ransomware signatures. The block list for signature-based blocking is managed by Nutanix or a third-party integration, and updates are handled through support (option A), not by manually editing a CSV file.
Why Option A?
Signature-based ransomware prevention in Nutanix Files relies on third-party integrations, as established in Question 56. The block list of malicious file signatures is not user-editable within Nutanix tools like the Files Console or File Analytics. To add a new signature, the administrator must open a support ticket with Nutanix, who will provide an updated Block List file, ensuring the new signature is properly integrated with the third- party solution.
Exact Extract from Nutanix Documentation:
From the Nutanix Files Administration Guide (available on the Nutanix Portal):

"For signature-based ransomware prevention, Nutanix Files integrates with third-party solutions that maintain a block list of malicious file signatures. To add a new signature to the block list, open a support ticket with Nutanix. Support will coordinate with the third-party provider (if applicable) and provide an updated Block List file to include the new signature."
:
Nutanix Files Administration Guide, Version 4.0, Section: "Managing Ransomware Block Lists with Third- Party Solutions" (Nutanix Portal).
Nutanix Certified Professional - Unified Storage (NCP-US) Study Guide, Section: "Nutanix Files Ransomware Protection".

질문 # 46
.....

Nutanix NCP-US-6.5 시험환경에 적응하고 싶은 분은 pdf버전 구매시 온라인버전 또는 테스트엔진 버전을 추가구매하시면 됩니다. 문제는 pdf버전의 문제와 같지만 pdf버전의 문제를 마스터한후 실력테스 가능한 프로그램이기에 Nutanix NCP-US-6.5시험환경에 익숙해져 시험을 보다 릴렉스한 상태에서 볼수 있습니다.