NCP-US-6.5 Q&As

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

Pass Nutanix NCP-US-6.5 Exam with 100% Guarantee

QUESTION 1

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.

Correct Answer: C

Explanation: 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. References: Nutanix Volumes Administration Guide1

QUESTION 2

An administrator has received an alert AI303551 ?VolumeGroupProtectionFailed details of alerts as follows:

Which error logs should the administrator be reviewing to determine why the relative service is down:

A. solver.log

B. arithmos.ERROR

Correct Answer: B

Explanation: The error log that the administrator should review to determine why the relative service is down is arithmos.ERROR. Arithmos is a service that runs on each CVM and provides volume group protection functionality for Volumes. Volume group protection is a feature that allows administrators to create protection policies for volume groups, which define how often snapshots are taken, how long they are retained, and where they are replicated. If arithmos.ERROR log shows any errors or exceptions related to volume group protection, it can indicate that the relative service is down or not functioning properly. References: Nutanix Volumes Administration Guide, page 29; Nutanix Volumes Troubleshooting Guide

QUESTION 3

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

Correct Answer: A

Explanation: 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. References: Nutanix Files Administration Guide2

QUESTION 4

What is the network requirement for a File Analytics deployment?

A. Must use the CVM not work

B. Must use the Backplane network

C. Must use the Storage-side network

D. Must use the Client-side network

Correct Answer: D

Explanation: Nutanix File Analytics is a feature that provides insights into the usage and activity of file data stored on Nutanix 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. The FAVM collects metadata and statistics from the FSVMs and displays them in a graphical user interface (GUI). The FAVM must be deployed on the same network as the FSVMs, which is the Client-side network. This network is used for communication between File Analytics and FSVMs, as well as for accessing the File Analytics UI from a web browser. The Client-side network must have DHCP enabled and must be routable from the external hosts that access the file shares and File Analytics UI. References: Nutanix Files Administration Guide, page 93; Nutanix File Analytics Deployment Guide

QUESTION 5

An administrator wants to provide security against ransomware attacks in Files. The administrator wants to configure the environment to scan files for ransomware in real time and provide notification in the event of a ransomware attack. Which component should the administrator use to meet this requirement?

A. File Analytics

B. Syslog Server

C. Files Console

D. Protection Domain

Correct Answer: A

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 also provides security against ransomware attacks by scanning files for ransomware in real time and providing notification in the event of a ransomware attack. File Analytics can detect ransomware based on file extensions, file signatures, or third-party solutions2. References: Nutanix File Analytics Administration Guide2