

# Convenient and Accessible Nutanix NCP-BC-7.5 Exam Questions in PDF Format

NCP-MCI Multicloud Infrastructure Certification Details	
Exam Code	NCP-MCI
Full Exam Name	Nutanix Certified Professional - Multicloud Infrastructure
No. of Questions	75
Online Practice Exam	<a href="#">Nutanix Certified Professional - Multicloud Infrastructure (NCP-MCI) Practice Test</a>
Sample Questions	<a href="#">Nutanix NCP-MCI Sample Questions</a>
Passing Score	3000/1000-6000
Time Limit	120 minutes
Exam Fees	\$199 USD

Become successful with [VMEexam.com](#)

If you study with our NCP-BC-7.5 exam questions, then you are better than others, and of course you will get more opportunities. You will never be picked by others. You will become the target of business competition! This will be a happy event! You must understand what it means in this social opportunity. You can get your favorite project and get a higher salary! Our NCP-BC-7.5 simulating exam can give you more than just the success of an exam, but also the various benefits that come along with successful NCP-BC-7.5 exams.

No matter how much you study, it can be difficult to feel confident going into the Nutanix Certified Professional - Business Continuity (NCP-BC) 7.5 (NCP-BC-7.5) exam. However, there are a few things you can do to help ease your anxiety and boost your chances of success. First, make sure you prepare with Real NCP-BC-7.5 Exam Dumps. If there are any concepts you're unsure of, take the time to take NCP-BC-7.5 practice exams until you feel comfortable.

>> Valid NCP-BC-7.5 Exam Labs <<

## 2026 Valid NCP-BC-7.5 Exam Labs 100% Pass | Valid Pdf NCP-BC-7.5 Free: Nutanix Certified Professional - Business Continuity (NCP-BC) 7.5

Download the free NCP-BC-7.5 demo of whatever product you want and check its quality and relevance by comparing it with other available study contents within your access. TrainingDump's study guides and NCP-BC-7.5 Dump will prove their worth and excellence. Check also the feedback of our clients to know how our products proved helpful in passing the exam

### Nutanix Certified Professional - Business Continuity (NCP-BC) 7.5 Sample Questions (Q56-Q61):

#### NEW QUESTION # 56

While attempting to execute a Commvault backup plan, an administrator received the following error for several VMs: "Virtual Machine not found ". After confirming the VMs exist, the administrator finds the following related error message: " Event Code 91:4 Virtual machine [Nutanix-Web-Server] was not found.

Please verify that the virtual machine still exists and that the host is in the connected state. " Which action should the administrator take to enable successful backups?

- A. Upgrade Nutanix Guest Tools (NGT) on the VM to the latest version.
- B. Ensure the VM is created with local Key Management Server (KMS).
- C. Ensure primary and recovery clusters are not registered to the same KMS.
- D. Ensure Virtual Trusted Platform Module (vTPM) is disabled on the VMs.

**Answer: A**

Explanation:

Nutanix integration with third-party backup vendors like Commvault often relies on the Nutanix Guest Tools (NGT) to facilitate advanced backup features. NGT provides the necessary communication bridge between the guest VM 's internal state and the

Nutanix AOS storage layer. The "Virtual Machine not found" error in a Commvault context, despite the VM being visible in Prism, often indicates a breakdown in metadata communication or a mismatch in the guest agent's version. If NGT is outdated or its internal "Nutanix Guest Agent" (NGA) service is failing, the backup software may be unable to retrieve the correct VM UUID or state information required to initiate an application-consistent snapshot. Upgrading NGT to the latest version ensures that the guest VM has the most current VSS hardware providers and metadata handlers, which are required for modern backup orchestration. Furthermore, NGT upgrades often resolve internal registration issues where the cluster fails to recognize the VM's active state due to legacy driver conflicts. By ensuring the NGT version is current and the NGA service is healthy, the administrator establishes a reliable communication path, allowing Commvault to correctly identify and process the VM for backup operations. This highlights the importance of maintaining NGT as part of regular cluster maintenance to ensure consistent BCDR functionality.

### NEW QUESTION # 57

Refer to Exhibit:

An administrator is configuring Metro Availability in their environment, as shown in the diagram. What issue in the configuration will prevent Metro from working correctly?

- A. The Witness VM is located in a third site.
- B. Each site should have a Witness VM.
- C. The latency between Site 1 and Site 2 is too high.
- D. The latency from the Witness VM to both Site 1 and 2 is too high.

**Answer: C**

Explanation:

Nutanix Metro Availability and Synchronous Replication have very strict networking requirements to ensure that real-time data mirroring does not introduce unacceptable application latency. The industry-standard requirement for Nutanix synchronous operations is a maximum Round Trip Time (RTT) latency of 5ms between the two primary clusters (Site 1 and Site 2). According to the diagram provided in the question, the latency between Site 1 and Site 2 is 25ms RTT. This latency is significantly higher than the 5ms threshold and will prevent the Metro Availability configuration from functioning correctly. While the latency to the Witness VM (200ms RTT) is perfectly acceptable (Option D), and having a Witness at a third site (Option A) is a best practice, the "data path" between the storage clusters is the bottleneck here. If an administrator attempts to enable Metro with 25ms of latency, the guest VMs would experience severe performance degradation because every write would be delayed by the 25ms it takes to receive an acknowledgment from the remote site.

Therefore, the high latency between the data-serving sites is the primary configuration issue that must be resolved, typically by moving the clusters closer together or upgrading the inter-site fiber connection.

### NEW QUESTION # 58

An administrator migrates a guest VM from a legacy Protection Domain-based DR configuration to a Prism Central (PC)-based Protection Policy. Immediately after migration, the administrator considers deleting the legacy Protection Domain snapshots to reclaim storage. According to Nutanix guidance, when is it safe to delete the legacy Protection Domain snapshots?

- A. After performing a planned failover
- B. Immediately after assigning the VM to a Protection Policy
- C. After the first recovery point for the VM is available in PC
- D. After validating the recovery plan

**Answer: C**

Explanation:

Transitioning from legacy Protection Domains (which are cluster-centric) to modern Prism Central-based Protection Policies (which are management-plane centric) is a common task during Nutanix environment upgrades. This migration involves a "handoff" where the responsibility for snapshots and replication shifts from the local Cerebro service on the cluster to the global orchestration provided by Prism Central.

The primary risk during this migration is the creation of a "protection gap." If an administrator deletes the legacy snapshots immediately after assigning a new policy, and that new policy has not yet successfully completed its first replication cycle, the virtual machine is effectively unprotected. If a disaster occurs at that exact moment, there would be no valid recovery points at the destination site to restore from. Nutanix best practice dictates that legacy artifacts must be preserved until the new system is verified as operational. Once the first recovery point for the VM appears in the Prism Central "Recovery Points" tab, it confirms that the new Protection Policy has successfully captured the VM's state and replicated it to the recovery AZ. At this stage, the legacy

snapshots in the Protection Domain become redundant and can be safely deleted to reclaim storage space without compromising the organization's ability to meet its Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

#### NEW QUESTION # 59

What is the expected outcome that the administrator must manage?

- A. Both sites will attempt to acquire the lock, but the primary site will acquire the lock and continue to serve I/O locally to prevent downtime.
- B. The secondary site will acquire the lock after a built-in delay, and the primary site will halt all I/O.
- C. The primary site will continue to serve I/O locally to prevent downtime, while the secondary site remains in standby.
- D. The Witness will automatically shut down the secondary site to protect data integrity on the primary site.

**Answer: A**

Explanation:

This question refers to the behavior of Nutanix Metro Availability in conjunction with a Witness VM during a site-to-site communication failure. Metro Availability provides a zero-RPO, synchronous replication solution.

To prevent "split-brain" (where both sites try to serve the same data independently), the Witness VM acts as a tie-breaker. When the two clusters lose connectivity with each other, both will immediately attempt to contact the Witness to "acquire the lock" on the protection domain. The Witness is programmed to prioritize the original "Active" site. If the primary cluster can reach the Witness, it will successfully acquire the lock and continue serving I/O locally to the guest VMs, ensuring zero downtime for the applications. The secondary site, unable to reach the primary or acquire the lock from the Witness, will transition its storage container to an "Inactive" state to protect data integrity. The administrator must manage this state by ensuring the Witness is always reachable from both clusters via independent network paths. If the primary site cannot reach the Witness, it will stop serving I/O to prevent inconsistent data states, highlighting the critical importance of Witness availability in a high-availability BCDR design.

#### NEW QUESTION # 60

What snapshot recovery point interval does Self-Service Restore support in a NearSync setup?

- A. 4 hours
- B. 1 hour
- C. 15 minutes
- D. 30 minutes

**Answer: B**

Explanation:

Self-Service Restore (SSR) is a Nutanix feature that allows end-users to recover individual files by mounting a recovery point as a local drive within the guest VM. NearSync replication provides high-frequency protection with Recovery Point Objectives (RPOs) as low as 1 minute using Lightweight Snapshots (LWS).

However, there is a technical distinction in how these high-frequency points are handled for end-user recovery.

In a NearSync configuration, the system generates dozens of LWS throughout an hour. While these are available for full VM disaster recovery, Nutanix limits the "granularity" available for Self-Service Restore to manage metadata overhead and guest agent performance. By default, SSR in a NearSync environment typically supports recovery point intervals of 1 hour. This means that while an administrator can restore the entire VM to a state from 5 minutes ago, an end-user using the SSR browser inside the VM will see recovery points at 1-hour increments (the "consolidated" points). This design balances the need for high-frequency disaster protection with the operational efficiency of file-level recovery. If a user needs a file from a point between the hourly intervals, an administrator may need to perform a full VM clone or an "Out-of-place" restore to provide access to those more granular lightweight recovery points.

#### NEW QUESTION # 61

.....

You buy our TrainingDump Nutanix NCP-BC-7.5 Certification which is 100% risk free. Before you decide to use TrainingDump Nutanix NCP-BC-7.5 dumps, you can try our free demo and pdf. Click TrainingDump, download it now! Affordable, and good service – free update for a year. Quality first. Welcomes your order. Thank you.

