Boost up Your Certification Score

Nutanix

NCP-MCI-7.5

Nutanix Certified Professional - Multicloud Infrastructure (NCP-MCI) 7.5

For More Information – Visit link below:

https://www.examsboost.com/

Product Version

✓ Up to Date products, reliable and verified.
✓ Questions and Answers in PDF Format.

Visit us at: https://www.examsboost.com/test/ncp-mci-7-5

Latest Version: 6.0

Question: 1

An administrator wants to define a set of conditions and approvers that must be satisfied before a deployment can proceed.
Which component must be enabled?

A. Policy Engine
B. Nutanix Central
C. Marketplace
D. Power Monitor

Answer: A

Explanation:
Nutanix Self-Service and NCM documentation explains that approval policies are built around defined conditions and approvers, and those policies are part of the broader Policy Engine capability. Nutanix further documents that the Policy Engine is included in NCM and provides the governance framework for conditions-based approvals before deployment actions proceed. Since the question asks specifically about defining conditions and approvers that must be satisfied before deployment, the correct enabling component is Policy Engine.
Marketplace can host deployable items, but it does not by itself provide the approval-governance mechanism being asked about. Nutanix Central and Power Monitor are unrelated to approval workflows. The wording in the question almost mirrors Nutanix's own approval-policy description, which is why the intended answer is clear. To enforce conditional approvals before provisioning or deployment actions, administrators use Policy Engine. Therefore A is the authentic answer.

Question: 2

An administrator added an SSH public key and verified connectivity to CVMs and AHV hosts. What is the recommended next step to reduce interactive access risk?

A. Enable core dumps on AHV hosts for post-incident analysis.
B. Disable password authentication for all CVMs and AHV hosts.
C. Enable a login banner on Prism Central to acknowledge access terms.
D. Increase the number of concurrent Prism Central UI sessions.

Answer: B

Explanation:
Nutanix security guidance is explicit on this point. After adding an SSH public key and verifying connectivity, Nutanix recommends disabling password authentication for all CVMs and AHV hosts to reduce interactive access risk. The Security Guide notes that after the SSH key inclusion and connectivity

validation are complete, password authentication should be disabled as the next hardening step. That makes B the correct answer.
This is a straightforward hardening sequence question. The administrator has already completed the prerequisite—public-key access is working—so the next step is to remove the weaker interactive method. Core dumps, login banners, and UI session settings do not address SSH authentication exposure. Nutanix's security model favors moving from password-based remote shell access to key-based access only. Therefore B is the authentic and recommended next step.

Question: 3

An administrator would like to create a VM template for reusability, to simplify VM management, and improve security.
When should the administrator apply a guest customization profile to simplify VM management?

A. When deploying a VM with Cloud-Init guest customization
B. When deploying a VM with a customized guided script
C. When cloning a VM with Cloud-Init guest customization
D. When cloning a VM with Sysprep guest customization

Answer: A

Explanation:
Nutanix documentation describes guest customization profiles as reusable configuration settings that can be applied during VM deployment from a template and also during certain clone operations. For Linux-based cloud-init workflows, Nutanix explicitly shows that when deploying a VM from a template with Cloud-Init guest customization, administrators can apply or override the customization settings at deployment time. That makes option A the cleanest and most documentation-aligned answer. (portal.nutanix.com , portal.nutanix.com)
Why not the others? Nutanix does support guided setup and clone scenarios, but the wording "create a VM template for reusability" points most strongly to the template deployment workflow rather than one-off cloning. Cloud-init is also the Nutanix-native customization method for Linux initialization at first boot, which makes it especially suitable for standardized reusable templates. So if the goal is simple repeatable management with a template-driven lifecycle, the correct point to apply the guest customization profile is when deploying a VM with Cloud-Init guest customization, which is (portal.nutanix.com)

Question: 4

An administrator needs to protect a volume group using a protection policy that supports an RPO of 1 hour. The environment consists of two clusters in different geographic regions. Which replication type should be used?

A. NearSync
B. Synchronous
C. Metro Availability
D. Asynchronous

Answer: D

Explanation:
Nutanix DR documentation for volume groups distinguishes replication types by RPO range. Nutanix documents Asynchronous Replication as the model for 1 hour or more RPO, while NearSync covers 1 minute to 15 minutes, and synchronous/Metro designs target near-zero or zero-RPO behavior with tighter latency expectations. Since the requirement here is 1 hour and the clusters are in different geographic regions, Asynchronous is the correct fit. That makes D the right answer.
The geography in the question is also a clue. Synchronous and Metro Availability are usually associated with low-latency links and more demanding network requirements, which are not implied by "different geographic regions." NearSync is too aggressive for a 1-hour target and is documented for much shorter RPO windows. Nutanix's own replication taxonomy places 1 hour or more squarely in the Asynchronous category, so D is the authentic answer.

Question: 5

Faced with prolonged times for hardware delivery, an administrator is looking for a way to be informed on time when cluster storage capacity is running low. In order for new hard disks to be delivered on time, the administrator needs to get a warning earlier than it is set currently.
Which action should the administrator take to receive a warning about cluster storage capacity running low earlier?

A. Enable early warning Storage Container alert.
B. Increase frequency of Storage Pool alerts.
C. Decrease Storage Container Space Usage Exceeded alert Warning threshold.
D. Decrease Storage Pool Capacity Usage Exceeded alert Critical threshold.

Answer: C

Explanation:
To receive an alert earlier, the administrator must lower the threshold at which the alert's warning state is triggered. Nutanix alerting works by comparing utilization against configured warning and critical thresholds. If the threshold is lowered, the system reaches it sooner, which gives the administrator more lead time before the environment becomes capacity-constrained. Among the given options, the one that directly performs that function is decreasing the Storage Container Space Usage Exceeded alert Warning threshold, which is option
The other choices are weaker or misaligned. There is no meaningful "increase frequency" adjustment that changes when capacity is considered low; it would only change how often checks occur, not the trigger point. Changing the critical threshold does not provide earlier warning notice, which is what the question asks for. The wording also points more naturally to a threshold-based action rather than enabling a different alert family. In Nutanix monitoring, earlier warnings come from making the warning trigger more conservative. Therefore C is the best answer because it causes the alert to fire at a lower usage percentage and provides earlier operational notice.

Question: 6

An administrator needs to configure OpenLDAP in Prism Central.
Which type of account should the administrator use?

A. Nutanix Account
B. Root Account
C. Admin Account
D. Service Account

Answer: D

Explanation:
Nutanix security documentation for configuring OpenLDAP authentication in Prism Central clearly states that Prism Central uses a service account to query the OpenLDAP directory and that this service account must have the required read permissions on the directory service. That means the correct account type is not a generic admin, root, or Nutanix local account, but a dedicated service account created for the integration. Therefore D is the authentic answer.
This is an important design principle in Nutanix authentication integration. A service account is preferred because it supports controlled, non-interactive access with appropriate least-privilege permissions and stable directory lookup behavior. Using a root or broad admin account would be poor security practice and is not how Nutanix documents the setup. The service account's role is not to log into Prism as a user but to let Prism Central query the directory safely and consistently. Because the official documentation names that account type directly, Service Account is the correct exam answer.

Question: 7

An administrator is troubleshooting intermittent VM I/O stalls that appear across hosts and clusters. The issue is sporadic, and the administrator needs to rapidly collect the correct platform logs for deeper analysis and possible escalation. The administrator wants to use a supported mechanism designed for efficient log collection, and must ensure the environment prerequisites are met so the tool can be used successfully.
Which option correctly describes the supported approach and a key prerequisite?

A. Use Logbay to collect logs, which is available once the node has a CVM deployed or the AHV compute node has been added to the cluster.
B. Use Panacea to troubleshoot the incident, retrieving the required host and CVM logs directly, without first collecting a log bundle from the cluster.
C. Use storage policy compliance reports and evaluations, include the underlying system logs needed to diagnose performance issues.
D. Use ADS to export diagnostic bundles automatically whenever built-in log collection function detects contention hotspots.

Answer: A

Explanation:

Nutanix documents Logbay as the preferred and supported mechanism for efficient platform log collection. The AHV administration guide states that you can use Logbay only after the CVM is installed on the node or the AHV compute node has been added to the cluster, which directly matches the wording in option Nutanix's web-console guidance also points administrators toward Logbay as the preferred collection method rather than relying only on manual UI collection.
The other options describe tools or behaviors that do not match Nutanix's documented collection path for this scenario. Panacea is not the standard answer for supported cluster log-bundle collection in the way described. Storage policy reports are not substitutes for host/CVM diagnostic logs, and ADS does not function as an automatic diagnostic bundle exporter for arbitrary contention events. Because the question asks for both the supported approach and a key prerequisite, Logbay with the documented availability condition is the most precise Nutanix answer. Therefore A is correct.

Question: 8

An administrator needs to be able to use remaining capacity for storage and memory.
What settings should the administrator set to accomplish this?

A. Capacity High Availability and Memory Reservation
B. Storage Capacity and Memory High Availability
C. Rebuild Capacity Reservation and High Availability
D. Rebuild Capacity Reservation and Memory Reservation

Answer: C

Explanation:
Nutanix separates storage resiliency reservation from compute high availability. For storage, the relevant setting is Rebuild Capacity Reservation, which reserves storage space so the cluster can self-heal and rebuild after node, block, or rack failure. For memory and compute, the relevant concept is High Availability, which reserves or accounts for host resources needed to restart workloads after a host failure. Putting those together gives the combination that best governs the remaining usable storage and memory capacity while preserving fault tolerance. That makes C the most correct answer.
The distractors either use non-standard phrasing or split the concepts incorrectly. "Memory Reservation" by itself is not the standard Nutanix answer when the exam is asking about cluster-wide restart capacity and usable memory after failure accounting. Nutanix administrators think in terms of HA for compute-memory protection and rebuild capacity reservation for storage protection. If the goal is to manage the usable remaining capacity for both storage and memory correctly, the right pair is Rebuild Capacity Reservation and High Availability. Therefore C is the authentic answer.

Question: 9

A database server has a corrupt database after a VM was restored from a recovery point. The database VM is part of the VIP_VMS category that is protected by a Protection Policy with asynchronous schedule. After checking the state of NGT tools, an administrator is investigating the Protection Policy looking for the root cause of the database corruption.
What is the most probably cause?

A. Set RPO is too high for protecting database VMs.
B. Roll-up schedule is used in Protection Policy instead of Linear.
C. The VM should have been added to the Applications category.
D. Take App-Consistent Recovery Point option is not selected.

Answer: D

Explanation:
For database workloads, Nutanix documentation distinguishes between crash-consistent and application-consistent recovery points. If the Take App-Consistent Recovery Points option is not selected, the recovery point may capture storage in a crash-consistent state only. For transactional databases, that can lead to corruption, incomplete writes, or recovery issues after restore. Nutanix specifically documents that selecting the app-consistent option creates application-consistent recovery points; if you do not select it, the recovery points are crash-consistent. That makes D the most likely root cause. (portal.nutanix.com , portal.nutanix.com)
The mention that NGT was checked is important because NGT participation is commonly part of quiesced and app-consistent protection workflows. A high RPO can increase data loss, but it does not by itself explain logical corruption inside the restored database. Category choice and roll-up schedule are also not the primary issue. Nutanix best practice for databases is to ensure application-consistent protection is enabled wherever supported. Therefore D is the correct answer.

Question: 10

An administrator needs to migrate an existing VM from a 3-tier ESXi environment to Nutanix AHV.
What should be used to minimize downtime during the migration?

A. Nutanix CCLM
B. Nutanix Move Agent
C. Backup and restore the VM
D. Nutanix Move

Answer: D

Explanation:
Nutanix's recommended migration tool for moving VMs into AHV is Nutanix Move. Official Nutanix guidance and migration material specifically recommend Move as the preferred mechanism for migrating VMs to AHV, especially when the goal is to reduce disruption compared with coarse methods like backup-and-restore. Move is purpose-built for this scenario and supports migration workflows from platforms such as VMware into Nutanix AHV with minimized downtime during cutover. (Nutanix)
The distractors highlight common confusion between the overall product and helper components. Move Agent may be involved in certain source-platform workflows, but the question asks what should be used to minimize downtime at the solution level. The correct answer is the migration platform itself: Nutanix Move. Backup and restore is usually more disruptive and manual. CCLM is unrelated here. Nutanix positioning is very clear that the standard, supported, low-downtime migration path from a third-party virtual environment to AHV is Move, so D is correct. (Nutanix)

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer

