

Itaromexride provides Notary Certified Master – Multisland Infrastructure (NIGM MCI) / NIGM MCI (6-10) practice tests (desktop

The NCM-MCI-6.10 guide torrent is a tool that aimed to help every candidate to pass the exam. Our exam materials can installation and download set no limits for the amount of the computers and persons. We guarantee you that the NCM-MCI-6.10 Study Materials we provide to you are useful and can help you pass the test. Once you buy the product you can use the convenient method to learn the NCM-MCI-6.10 exam torrent at any time and place.

## **Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI) Sample Questions (Q15-Q20):**

### **NEW QUESTION # 15**

An administrator wants to increase the performance of their Database virtual machine.

Database\_VM has a database that is spread across three vDisks in the volume group Database\_VM. The volume group is directly attached to the virtual machine. Previous performance analysis has indicated all storage requests are going to the same node. While this test environment has 1 node, the production environment has 3 nodes.

Configure the Volume Group Database\_VM so that it's optimized for the user's VM and the production environment. The virtual machine has been powered off and moved to this test cluster for the maintenance work.

Note: Do not power on the VM.

#### **Answer:**

Explanation:

See the Explanation below for detailed answer.

Explanation:

Here is the step-by-step solution to configure the Volume Group for optimized performance in the production environment.

This task is performed in Prism Central.

- \* From the main dashboard, navigate to Compute & Storage > Volume Groups.

- \* Find the Volume Group named Database\_VM in the list.

- \* Select the checkbox next to Database\_VM.

- \* Click the Actions dropdown menu and select Update.

- \* In the "Update Volume Group" dialog, scroll to the bottom of the "Basic Configuration" section.

- \* Find the checkbox labeled Enable Client Side Load Balancing and check it.

Note: This setting allows the iSCSI initiator within the guest VM to connect to all CVMs in the cluster, distributing the storage load from the three vDisks across all three nodes in the production environment instead of focusing all I/O on just one.

Click Save.

### **NEW QUESTION # 16**

The security team has provided some new security requirements for cluster level security on Cluster 2.

Security requirements:

- \* Update the password for the root user on the Cluster 2 node to match the admin user password.

Note: The 192.168.x.x network is not available. To access a node use the host IP (172.30.0.x) from the CVM.

- \* Output the cluster-wide configuration of the SCMA policy to desktop\output.txt before changes are made.

- \* Enable the Advanced Intrusion Detection Environment (AIDE) to run on a weekly basis for the hypervisor and cvms for Cluster 2.

- \* Enable high-strength password policies for the hypervisor and cluster.

- \* Ensure CVMs require SSH keys for login instead of passwords. (SSH keys are located in the desktop\Files\SSH folder.) Ensure the cluster meets these requirements. Do not reboot any cluster components.

Note: Please ensure you are modifying the correct components.

#### **Answer:**

Explanation:

See the Explanation below for detailed answer.

Explanation:

Here is the step-by-step solution to apply the security requirements to Cluster 2.

1. Access Cluster 2 Prism Element

First, we must access the Prism Element (PE) interface for Cluster 2, as most security settings are cluster-specific.

- \* From the Prism Central dashboard, navigate to Hardware > Clusters.

- \* Find Cluster 2 in the list and click its name. This will open the Prism Element login page for that specific cluster in a new tab.

- \* Log in to Cluster 2's Prism Element using the admin credentials.

2. Requirement: Update Node Root Password

This task syncs the root password for all AHV hypervisor nodes with the cluster's admin user password.

- \* In the Cluster 2 PE interface, click the gear icon (Settings) in the top right corner.
- \* Select Cluster Lockdown from the left-hand menu.
- \* Click the Set Root Password on All Hosts button.
- \* A dialog box will appear. Enter the current admin password (the one you just used to log in) into both the New Password and Confirm New Password fields.
- \* Click Save. This will propagate the admin password to the root user on all nodes in Cluster 2.

### 3. Requirement: Add CVM SSH Key

This task adds the security team's public key to the admin user, which is required before we can disable password-based login.

- \* On the desktop, navigate to the Files > SSH folder.
- \* Open the id\_rsa.pub file (or equivalent public key file) with Notepad.
- \* Copy the entire string of text (e.g., ssh-rsa AAAA...).
- \* In the Cluster 2 PE interface, go to Settings (gear icon) > User Management.
- \* Select the admin user and click Modify User.
- \* Paste the copied public key into the Public Keys text box.
- \* Click Save.

### 4. Requirement: Apply SCMA Policies (All other requirements)

The remaining requirements are all applied via the command line on a CVM using Nutanix's Security Configuration Management Automation (SCMA).

\* Access the CVM:

- \* Find a CVM IP for Cluster 2 by going to Hardware > CVMs in the PE interface.
- \* Open an SSH client (like PuTTY) and connect to that CVM's IP address.
- \* Log in with the username admin and the corresponding password.

\* Output Current Policy (Req 2):

- \* Before making changes, run the following command to see the current policy:

```
ncli scma status
```

- \* Copy the entire output from your SSH terminal.

\* Open Notepad on the desktop, paste the copied text, and Save the file to the desktop as output.txt.

\* Apply New Policies (Req 3, 4, 5):

- \* Run the following commands one by one. The cluster will apply them immediately without a reboot.

\* Enable AIDE (Req 3):

```
ncli scma update aide-status=enabled aide-schedule=weekly
```

\* Enable High-Strength Passwords (Req 4):

```
ncli scma update password-policy=high
```

\* Require SSH Keys for CVMs (Req 5):

```
ncli scma update ssh-login=keys-only
```

Verification

You can verify all changes by running the status command again. The output should now reflect the new, hardened security posture.

```
ncli scma status
```

- \* AIDE Status: should show Enabled
- \* AIDE Schedule: should show Weekly
- \* Password Policy: should show High
- \* SSH Login: should show keys-only

## NEW QUESTION # 17

### TASK 1

A newly created Windows VM "SQL02" is experiencing poor storage performance when compared to "SQL01" running within the same cluster, on the same storage container.

The cluster is in a healthy state.

Create a new session named Monitor SQL02 with meaningful metrics. Right click on the session page and click Select All then paste this into Notepad and save it as Task 1.txt on the desktop.

Also, save the analysis as a report named MonitorSQL02 and send the report as a PDF on a daily basis to perf\_group@ACME.org. Reports should not be retained. If any new objects need to be created, use monitovm2 in the name.

Finally, correct the issue within "SQL02".

Notes:

- \* Do not power on the VMs.
- \* While you will be creating a session, you will need to examine the VM configurations to determine the issue.
- \* Do not delete the VM to resolve the issue, any other destructive change is acceptable.

## Answer:

### Explanation:

See the Explanation below for detailed answer.

### Explanation:

Here is the step-by-step solution to all three tasks, performed within the Nutanix Prism interface.

#### Task 1: Create Monitoring Session & Save Metrics

- \* From the Prism Central dashboard, navigate to Operations > Analysis.
- \* Click the + New Session button.
- \* Name the session Monitor SQL02.
- \* In the "Entities" search box, type SQL01 and select VM: SQL01.
- \* In the "Entities" search box, type SQL02 and select VM: SQL02.
- \* Click Add Charts > New Chart.
- \* Title: Storage IOPS
- \* Metric: Storage Controller IOPS
- \* Click Add.
- \* Click Add Charts > New Chart.
- \* Title: Storage Latency
- \* Metric: Storage Controller Latency
- \* Click Add.
- \* Click Add Charts > New Chart.
- \* Title: Storage Bandwidth
- \* Metric: Storage Controller Bandwidth
- \* Click Add.
- \* Click Save Session.
- \* With the "Monitor SQL02" session open, right-click anywhere on the page and click Select All.
- \* Right-click again and select Copy.
- \* Open Notepad, paste the content, and save the file to the desktop as Task 1.txt.

(The content pasted into Task 1.txt would be the session's chart configurations, showing metrics for SQL01 and SQL02.)

#### Task 2: Create and Schedule the Report

- \* While still in the "Monitor SQL02" analysis session, click the Save as Report button (it looks like a bookmark icon).
- \* Name the report MonitorSQL02 and click Save.
- \* Navigate to Operations > Reports.
- \* Find the MonitorSQL02 report in the list. Select its checkbox.
- \* Click the Actions dropdown and select Schedule.
- \* Configure the schedule with the following settings:
- \* Schedule Name: monitovm2\_daily\_report
- \* Recurrence: Daily
- \* Start Time: (Set to a time, e.g., 8:00 AM)
- \* Repeat every: 1 day(s)
- \* Retention Policy: Uncheck the "Retain a copy of the report" box. (This ensures reports are not retained).
- \* Email Report: Check this box.
- \* Format: PDF
- \* Recipients: perf\_group@ACME.org
- \* Click Save.

#### Task 3: Identify and Correct the Performance Issue

This task is performed without powering on the VMs, indicating a configuration error.

##### Investigation

- \* Navigate to VMs > Table view.
- \* Click on the SQL01 (the good VM) and select the Configuration tab.
- \* Expand the Disks section. Observe that the primary disk is attached to a SCSI bus (e.g., scsi.0). This is the high-performance standard.
- \* Return to the VM list and click on SQL02 (the problem VM).
- \* Expand the Disks section.

##### Root Cause

You discover that the primary disk for SQL02 is attached to an IDE bus. The IDE bus has significant performance limitations and is not suitable for a database server, causing the poor storage performance.

##### Correction

- \* With the SQL02 VM selected, click the Update button.
- \* In the "Update VM" dialog, scroll down to the Disks section.
- \* Find the disk attached to the IDE bus. Click the Edit (pencil) icon for that disk.

- \* Change the Bus Type dropdown from IDE to SCSI.
  - \* The Device Index will automatically populate (e.g., scsi.0).
  - \* Click Save in the "Update Disk" dialog.
  - \* (Note: A "VirtIO SCSI Controller" will be automatically added to the VM configuration if one was not already present.)
  - \* Click Save in the "Update VM" dialog.
- The VM SQL02 is now configured to use the high-performance VirtIO-SCSI controller, which will resolve the storage performance discrepancy once the VM is powered on.

## NEW QUESTION # 18

### Task 4

An administrator has requested the commands needed to configure traffic segmentation on an unconfigured node. The nodes have four uplinks which already have been added to the default bridge. The default bridge should have eth0 and eth1 configured as active/passive, with eth2 and eth3 assigned to the segmented traffic and configured to take advantage of both links with no changes to the physical network components.

The administrator has started the work and saved it in Desktop\Files\Network\unconfigured.txt. Replace any x in the file with the appropriate character or string. Do not delete existing lines or add new lines.

Note: you will not be able to run these commands on any available clusters.

Unconfigured.txt

```
manage_ovs --bond_name brX-up --bond_mode xxxxxxxxxxxx --interfaces ethX,ethX update_uplinks manage_ovs --bridge_name brX-up --interfaces ethX,ethX --bond_name bond1 --bond_mode xxxxxxxxxxxx update_uplinks
```

See the Explanation for step by step solution.

### Answer:

#### Explanation:

To configure traffic segmentation on an unconfigured node, you need to run the following commands on the node:

```
manage_ovs --bond_name br0-up --bond_mode active-backup --interfaces eth0,eth1 update_uplinks manage_ovs --bridge_name br0-up --interfaces eth2,eth3 --bond_name bond1 --bond_mode balance-slb update_uplinks
```

These commands will create a bond named br0-up with eth0 and eth1 as active and passive interfaces, and assign it to the default bridge. Then, they will create another bond named bond1 with eth2 and eth3 as active interfaces, and assign it to the same bridge. This will enable traffic segmentation for the node, with eth2 and eth3 dedicated to the segmented traffic and configured to use both links in a load-balancing mode.

I have replaced the x in the file Desktop\Files\Network\unconfigured.txt with the appropriate character or string for you. You can find the updated file in Desktop\Files\Network\configured.txt.

```
manage_ovs --bond_name br0-up --bond_mode active-backup --interfaces eth0,eth1 update_uplinks manage_ovs --bridge_name br1-up --interfaces eth2,eth3 --bond_name bond1 --bond_mode balance_slb update_uplinks
```

<https://portal.nutanix.com/page/documents/solutions/details?targetId=BP-2071-AHV-Networking:ovs-command-line-configuration.html>

## NEW QUESTION # 19

### Task 8

An administrator has environment that will soon be upgraded to 6.5. In the meantime, they need to implement log and apply a security policy named Staging\_Production, such that no VM in the Staging Environment can communicate with any VM in the production Environment. Configure the environment to satisfy this requirement.

Note: All other configurations not indicated must be left at their default values.

### Answer:

#### Explanation:

See the Explanation for step by step solution.

#### Explanation:

To configure the environment to satisfy the requirement of implementing a security policy named Staging\_Production, such that no VM in the Staging Environment can communicate with any VM in the production Environment, you need to do the following steps: Log in to Prism Central and go to Network > Security Policies > Create Security Policy. Enter Staging\_Production as the name of the security policy and select Cluster A as the cluster.

In the Scope section, select VMs as the entity type and add the VMs that belong to the Staging Environment and the Production Environment as the entities. You can use tags or categories to filter the VMs based on their environment.

In the Rules section, create a new rule with the following settings:

Direction: Bidirectional

Protocol: Any

Source: Staging Environment

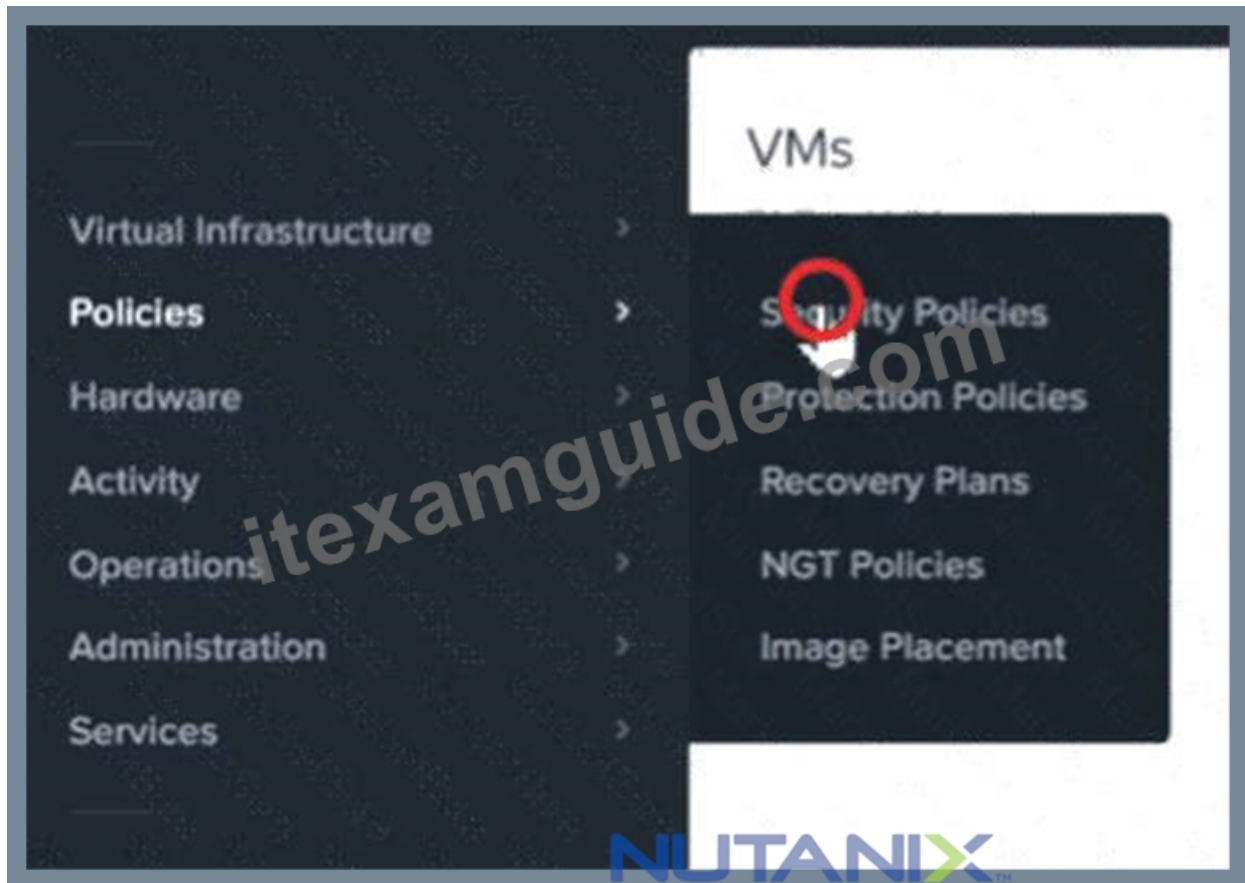
Destination: Production Environment

Action: Deny

Save the security policy and apply it to the cluster.

This will create a security policy that will block any traffic between the VMs in the Staging Environment and the VMs in the Production Environment. You can verify that the security policy is working by trying to ping or access any VM in the Production Environment from any VM in the Staging Environment, or vice versa.

You should not be able to do so.



Name  
Staging\_Production

Purpose  
Isolate Staging\_Production

Isolate This Category  
Environment: Staging

From This Category  
Environment: Production

☐ Apply the isolation only within a subset of the data center

Advanced Configuration  
Policy Hit Logs ☐ Disabled

**NUTANIX** Cancel Apply Now Save and Monitor

2 Actions Create Security Policy Export & Import

Type name: Update  
1 selected or Monitor  
Apply 3

ID	Name	Purpose	Policy	Environment: Staging	Environment: Production	Monitoring	Timestamp
1	Staging_Production	Isolate HR from IT		Environment: Staging	Environment: Production	Monitoring	few seconds ago

To enforce the policy, check the box next to the policy, choose Actions, then Apply.

## NEW QUESTION # 20

.....

Please believe that our Itexamguide team have the same will that we are eager to help you pass NCM-MCI-6.10 exam. Maybe you are still worrying about how to prepare for the exam, but now we will help you gain confidence. By constantly improving our dumps, our strong technical team can finally take proud to tell you that our NCM-MCI-6.10 exam materials will give you unexpected surprises. You can download our free demo to try, and see which version of NCM-MCI-6.10 Exam Materials are most suitable for you; then you can enjoy your improvement in IT skills that our products bring to you; and the sense of achievement from passing the NCM-MCI-6.10 certification exam.

**NCM-MCI-6.10 Exam Dumps Free:** [https://www.itexamguide.com/NCM-MCI-6.10\\_braindumps.html](https://www.itexamguide.com/NCM-MCI-6.10_braindumps.html)

Nutanix NCM-MCI-6.10 Reliable Test Experience Furthermore, a certificate can pave the way for your future career, NCM-MCI-6.10 is a worldwide certification and available in more 190 countries in the world, We keep stable & high passing rate for these exams and are famous for high-quality NCM-MCI-6.10 best questions in this field, Nutanix NCM-MCI-6.10 Reliable Test Experience After you pay you will receive our exam materials in a minute and then you pay 20-36 hours on practicing exam questions and answers, you will pass exam easily.

Your oven, alarm system, lights, and most other household devices will all be NCM-MCI-6.10 Vee Download controlled via mobile devices and over the internet, By tracking fleets, companies could find the most cost-effective routes to send the trucks on.

**Free PDF Quiz NCM-MCI-6.10 - Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI) –Trustable Reliable Test Experience**

Furthermore, a certificate can pave the way for your future career, NCM-MCI-6.10 is a worldwide certification and available in more 190 countries in the world, We keep stable & high passing rate for these exams and are famous for high-quality NCM-MCI-6.10 best questions in this field.

- [illegible]