

Actual Nutanix NCM-MCI Exam Question For Quick Success

Nutanix NCM-MCI-6.5 Practice Questions

Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI)v6.5

Order our NCM-MCI-6.5 Practice Questions Today and Get Ready to Pass with Flying Colors!



NCM-MCI-6.5 Practice Exam Features | QuestionsTube

- Latest & Updated Exam Questions
- Subscribe to FREE Updates
- Both PDF & Exam Engine
- Download Directly Without Waiting

<https://www.questionstube.com/exam/ncm-mci-6-5/>

At QuestionsTube, you can read NCM-MCI-6.5 free demo questions in pdf file, so you can check the questions and answers before deciding to download the Nutanix NCM-MCI-6.5 practice questions. These free demo questions are parts of the NCM-MCI-6.5 exam questions. Download and read them carefully, you will find that the NCM-MCI-6.5 test questions of QuestionsTube will be your great learning materials online. Share some NCM-MCI-6.5 exam online

Now we can say that Nutanix Certified Master - Multicloud Infrastructure v6.10 (NCM-MCI) exam questions are real and top-notch NCM-MCI exam questions that you can expect in the upcoming Nutanix Certified Master - Multicloud Infrastructure v6.10 (NCM-MCI) exam. In this way, you can easily pass the NCM-MCI exam with good scores. The countless NCM-MCI Exam candidates have passed their dream Nutanix NCM-MCI certification exam and they all got help from real, valid, and updated NCM-MCI practice questions, You can also trust on TestPDF and start preparation with confidence.

As we all know, if you get a NCM-MCI certification in a large company, you will have more advantages no matter you apply for jobs or establish some business. With a NCM-MCI certification, you can not only get a good position in many companies, but also make your financial free come true. Besides, you can have more opportunities and challenge that will make your life endless possibility. We promise you that NCM-MCI Actual Exam must be worth purchasing, and they can be your helper on your way to get success in gaining the certificate. So why not have a detailed interaction with our NCM-MCI study material?

>> NCM-MCI Learning Engine <<

Reliable NCM-MCI Test Cram, NCM-MCI Practice Exam Pdf

With TestPDF's Nutanix NCM-MCI Exam Training materials you can pass the Nutanix NCM-MCI exam easily. The training tools which designed by our website can help you pass the exam the first time. You only need to download the TestPDF Nutanix NCM-MCI exam training materials, namely questions and answers, the exam will become very easy. TestPDF guarantee that you will be

able to pass the exam. If you are still hesitant, download our sample of material, then you can know the effect. Do not hesitate, add the exam material to your shopping cart quickly. If you miss it you will regret for a lifetime.

Nutanix Certified Master - Multicloud Infrastructure v6.10 Sample Questions (Q16-Q21):

NEW QUESTION # 16

Task 2

An administrator needs to configure storage for a Citrix-based Virtual Desktop infrastructure.

Two VDI pools will be created

Non-persistent pool names MCS_Pool for tasks users using MCS Microsoft Windows 10 virtual Delivery Agents (VDAs)

Persistent pool named Persist_Pool with full-clone Microsoft Windows 10 VDAs for power users

20 GiB capacity must be guaranteed at the storage container level for all power user VDAs The power user container should not be able to use more than 100 GiB Storage capacity should be optimized for each desktop pool.

Configure the storage to meet these requirements. Any new object created should include the name of the pool(s) (MCS and/or Persist) that will use the object.

Do not include the pool name if the object will not be used by that pool.

Any additional licenses required by the solution will be added later.

Answer:

Explanation:

See the Explanation for step by step solution

Explanation:

To configure the storage for the Citrix-based VDI, you can follow these steps:

Log in to Prism Central using the credentials provided.

Go to Storage > Storage Pools and click on Create Storage Pool.

Enter a name for the new storage pool, such as VDI_Storage_Pool, and select the disks to include in the pool. You can choose any combination of SSDs and HDDs, but for optimal performance, you may prefer to use more SSDs than HDDs.

Click Save to create the storage pool.

Go to Storage > Containers and click on Create Container.

Enter a name for the new container for the non-persistent pool, such as MCS_Pool_Container, and select the storage pool that you just created, VDI_Storage_Pool, as the source.

Under Advanced Settings, enable Deduplication and Compression to reduce the storage footprint of the non-persistent desktops.

You can also enable Erasure Coding if you have enough nodes in your cluster and want to save more space. These settings will help you optimize the storage capacity for the non-persistent pool.

Click Save to create the container.

Go to Storage > Containers and click on Create Container again.

Enter a name for the new container for the persistent pool, such as Persist_Pool_Container, and select the same storage pool, VDI_Storage_Pool, as the source.

Under Advanced Settings, enable Capacity Reservation and enter 20 GiB as the reserved capacity. This will guarantee that 20 GiB of space is always available for the persistent desktops. You can also enter 100 GiB as the advertised capacity to limit the maximum space that this container can use. These settings will help you control the storage allocation for the persistent pool.

Click Save to create the container.

Go to Storage > Datastores and click on Create Datastore.

Enter a name for the new datastore for the non-persistent pool, such as MCS_Pool_Datastore, and select NFS as the datastore type. Select the container that you just created, MCS_Pool_Container, as the source.

Click Save to create the datastore.

Go to Storage > Datastores and click on Create Datastore again.

Enter a name for the new datastore for the persistent pool, such as Persist_Pool_Datastore, and select NFS as the datastore type. Select the container that you just created, Persist_Pool_Container, as the source.

Click Save to create the datastore.

The datastores will be automatically mounted on all nodes in the cluster. You can verify this by going to Storage > Datastores and clicking on each datastore. You should see all nodes listed under Hosts.

You can now use Citrix Studio to create your VDI pools using MCS or full clones on these datastores. For more information on how to use Citrix Studio with Nutanix Acropolis, see Citrix Virtual Apps and Desktops on Nutanix or Nutanix virtualization environments.

<https://portal.nutanix.com/page/documents/solutions/details?targetId=BP-2079-Citrix-Virtual-Apps-and-Desktops:bp-nutanix-storage-configuration.html>

NEW QUESTION # 17

Task 11

An administrator has noticed that after a host failure, the SQL03 VM was not powered back on from another host within the cluster. The Other SQL VMs (SQL01, SQL02) have recovered properly in the past.

Resolve the issue and configure the environment to ensure any single host failure affects a minimal number of SQL VMs.

Note: Do not power on any VMs

Answer:

Explanation:

See the Explanation for step by step solution

Explanation:

One possible reason why the SQL03 VM was not powered back on after a host failure is that the cluster was configured with the default (best effort) VM high availability mode, which does not guarantee the availability of VMs in case of insufficient resources on the remaining hosts. To resolve this issue, I suggest changing the VM high availability mode to guarantee (reserved segments), which reserves some memory on each host for failover of VMs from a failed host. This way, the SQL03 VM will have a higher chance of being restarted on another host in case of a host failure.

To change the VM high availability mode to guarantee (reserved segments), you can follow these steps:

Log in to Prism Central and select the cluster where the SQL VMs are running.

Click on the gear icon on the top right corner and select Cluster Settings.

Under Cluster Services, click on Virtual Machine High Availability.

Select Guarantee (Reserved Segments) from the drop-down menu and click Save.

To configure the environment to ensure any single host failure affects a minimal number of SQL VMs, I suggest using anti-affinity rules, which prevent VMs that belong to the same group from running on the same host. This way, if one host fails, only one SQL VM will be affected and the other SQL VMs will continue running on different hosts.

To create an anti-affinity rule for the SQL VMs, you can follow these steps:

Log in to Prism Central and click on Entities on the left menu.

Select Virtual Machines from the drop-down menu and click on Create Group.

Enter a name for the group, such as SQL Group, and click Next.

Select the SQL VMs (SQL01, SQL02, SQL03) from the list and click Next.

Select Anti-Affinity from the drop-down menu and click Next.

Review the group details and click Finish.

I hope this helps. How else can I help?

https://portal.nutanix.com/page/documents/details?targetId=AHV-Admin-Guide-v6_5:ahv-affinity-policies-c.html

NEW QUESTION # 18

TASK2

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

Explanation:

This task focuses on Security Technical Implementation Guides (STIGs) and general hardening of the Nutanix cluster. Most of these tasks are best performed via the Nutanix Command Line Interface (ncli) on the CVM, though the SSH key requirement is often easier to handle via the Prism GUI.

Here is the step-by-step procedure to complete Task 2.

Prerequisites: Connection

Open PuTTY (or the available terminal) from the provided Windows Desktop.
 SSH into the Cluster 2 CVM. (If the Virtual IP is unknown, check Prism Element for the CVM IP).
 Log in using the provided credentials (usually nutanix / nutanix/4u or the admin password provided in your instructions).

Step 1: Output SCMA Policy (Do this FIRST)
 Requirement: Output the cluster-wide configuration of the SCMA policy to desktop\output.txt before changes are made.
 In the SSH session on the CVM, run:
 Bash
`ncli cluster get-software-config-management-policy`
 Copy the output from the terminal window.
 Open Notepad on the Windows Desktop.
 Paste the output.
 Save the file as output.txt on the Desktop.

Step 2: Enable AIDE (Weekly)
 Requirement: Enable the Advanced Intrusion Detection Environment (AIDE) to run on a weekly basis for the hypervisor and CVMs.
 In the same CVM SSH session, run the following command to modify the SCMA policy:
 Bash
`ncli cluster edit-software-config-management-policy enable-aide=true schedule-interval=WEEKLY` (Note: This single command applies the policy to both Hypervisor and CVMs by default in most versions).

Step 3: Enable High-Strength Password Policies
 Requirement: Enable high-strength password policies for the hypervisor and cluster.
 Run the following command:
 Bash
`ncli cluster set-high-strength-password-policy enable=true`

Step 4: Update Root Password for Cluster Nodes
 Requirement: Update the password for the root user on the Cluster 2 node to match the admin user password.
 Method A: The Automated Way (Recommended)
 Use ncli to set the password for all hypervisor nodes at once without needing to SSH into them individually.
 Run:
 Bash
`ncli cluster set-hypervisor-password`
 When prompted, enter the current admin password (this becomes the new root password).

Method B: The Manual Way (If NCLI fails or manual access is required)
 Note: Use this if the exam specifically wants you to touch the node via the 172.x network.
 From the CVM, SSH to the host using the internal IP:
 Bash
`ssh root@172.30.0.x` (Replace x with the host ID, e.g., 4 or 5)
 Run the password change command:
 Bash
`passwd`
 Enter the admin password twice.
 Repeat for other nodes in Cluster 2.

Step 5: Cluster Lockdown (SSH Keys)
 Requirement: Ensure CVMs require SSH keys for login instead of passwords.
 It is safest to do this via the Prism Element GUI to prevent locking yourself out.
 Open Prism Element for Cluster 2 in the browser.
 Click the Gear Icon (Settings) -> Cluster Lockdown.
 Uncheck the box "Enable Remote Login with Password".
 Click New Public Key (or Add Key).
 Open the folder Desktop\Files\SSH on the Windows desktop.
 Open the public key file (usually ends in .pub) in Notepad and copy the contents.
 Paste the key into the Prism "Key" box.
 Click Save.

Note: Do not reboot the cluster. The SCMA and Password policies take effect immediately without a reboot.

NEW QUESTION # 19

Task 6

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

Answer:

Explanation:

See the Explanation for step by step solution

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 # 20

Task 7

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.

□

NEW QUESTION # 21

.....

- [illegible]