# 2026 NCM-MCI Valid Dumps Demo 100% Pass | Latest Nutanix Nutanix Certified Master - Multicloud Infrastructure v6.10 Practice Braindumps Pass for sure



As the rapid development of the world economy and intense competition in the international, the leading status of knowledge-based economy is established progressively. A lot of people are in pursuit of a good job, a NCM-MCI certification, and a higher standard of life. It is very important for us to keep pace with the changeable world and update our knowledge if we want to get a good job, a higher standard of life and so on. First, we need to get a good NCM-MCI Quiz prep. Because we only pass NCM-MCI exam and get a certificate, we can have the chance to get a decent job and make more money.

## Nutanix NCM-MCI Exam Practice Test Helps You Ace Your Nutanix Certified Expert

Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI) exam is a challenging exam that needs you to perform with excellent knowledge. We recommend you to be prepared for the Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI) exam as it is crucial for your professional career.

Nutanix offers you a really easy way to prepare for your Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI) exam by providing the Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI) practice test software. This practice test software has everything that an individual requires to pass their certification exam in the first attempt. The questions offered in the practice test software are similar to those you can expect in the real Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI) exam scenario. The practice test software is also equipped with learning tools and features that will help you learn about your weak areas.

If you want to buy the high quality **Nutanix NCM-MCI Exam Dumps** for NCM-MCI exam, then TestBraindump is your first choice. Do not hesitate to choose us as your loyal partner because we are the only one can help you pass Nutanix Certified Master (NCM) - Multicloud Infrastructure (NCM-MCI) test successfully. At the same time, you can get 100% guaranteed NCM-MCI exam questions and answers with high accuracy and hit rate. NCM-MCI practice test is the best source to prepare for your Nutanix Certified Master (NCM) - Multicloud Infrastructure (NCM-MCI) Certification Exam for 100 percent results.

### What are the steps to follow for the registration of Microsoft Nutanix NCM-MCI Exam

- Review the Exam Day Checklist.
- Review the Exam Preparation Guide and Candidate Handbook.
- Email npx@nutanix.com to request a unique invitation link to register for your exam.
- Complete your exam at a mutually agreed upon time/date with your NCX/NPX Program Manager.

#### >> NCM-MCI Valid Dumps Demo <<

### Nutanix - NCM-MCI - Nutanix Certified Master - Multicloud Infrastructure v6.10 - The Best Valid Dumps Demo

May be you still strange to our NCM-MCI dumps pdf, you can download the free demo of the dump torrent before you buy. If you have any questions to our Nutanix exam questions torrent, please feel free to contact us and we will give our support immediately. You will be allowed to updating NCM-MCI Learning Materials one-year once you bought pdf dumps from our website.

### What is the salary of the Nutanix NCM-MCI Exam

The Average salary of different countries of Nutanix Certified Expert

- United States USD 116,178 per year
- UK Pounds 45,280 per year
- India INR 776,970 per year

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

### **NEW QUESTION #16**

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 noli 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 #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 os 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**

Task 9

Part1

An administrator logs into Prism Element and sees an alert stating the following:

Cluster services down on Controller VM (35.197.75.196)

Correct this issue in the least disruptive manner.

Part2

In a separate request, the security team has noticed a newly created cluster is reporting.

CVM [35.197.75.196] is using the default password.

They have provided some new security requirements for cluster level security.

Security requirements:

Update the default password for the root user on the node to match the admin user password: Note: 192.168.x.x is not available.

To access a node use the Host IP (172.30.0.x) from a CVM or the supplied external IP address.

Update the default password for the nutanix user on the CVM to match the admin user password.

Resolve the alert that is being reported.

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

Enable the Advance intrusion Detection Environment (AIDE) to run on a weekly basis for the cluster.

Enable high-strength password policies for the cluster.

Ensure CVMs require SSH keys for login instead of passwords. (SSH keys are located in the Desktop\Files\SSH folder).

Ensure the clusters meets these requirements. Do not reboot any cluster components.

#### Answer:

Explanation:

See the Explanation for step by step solution

Explanation:

To correct the issue of cluster services down on Controller VM (35.197.75.196) in the least disruptive manner, you need to do the following steps:

Log in to Prism Element using the admin user credentials.

Go to the Alerts page and click on the alert to see more details.

You will see which cluster services are down on the Controller VM. For example, it could be cassandra, curator, stargate, etc. To start the cluster services, you need to SSH to the Controller VM using the nutanix user credentials. You can use any SSH client such as PuTTY or Windows PowerShell to connect to the Controller VM. You will need the IP address and the password of the nutanix user, which you can find in Desktop\Files\SSH\nutanix.txt.

Once you are logged in to the Controller VM, run the command:

cluster status | grep -v UP

This will show you which services are down on the Controller VM.

To start the cluster services, run the command:

cluster start

This will start all the cluster services on the Controller VM.

To verify that the cluster services are running, run the command:

cluster status | grep -v UP

This should show no output, indicating that all services are up.

To clear the alert, go back to Prism Element and click on Resolve in the Alerts page.

To meet the security requirements for cluster level security, you need to do the following steps:

To update the default password for the root user on the node to match the admin user password, you need to SSH to the node using the root user credentials. You can use any SSH client such as PuTTY or Windows PowerShell to connect to the node. You will need the IP address and the password of the root user, which you can find in Desktop\Files\SSH\root.txt.

Once you are logged in to the node, run the command:

passwd

This will prompt you to enter a new password for the root user. Enter the same password as the admin user, which you can find in Desktop\Files\SSH\admin.txt.

To update the default password for the nutanix user on the CVM to match the admin user password, you need to SSH to the CVM using the nutanix user credentials. You can use any SSH client such as PuTTY or Windows PowerShell to connect to the CVM.

You will need the IP address and the password of the nutanix user, which you can find in Desktop\Files\SSH\nutanix.txt.

Once you are logged in to the CVM, run the command:

passwd

This will prompt you to enter a new password for the nutanix user. Enter the same password as the admin user, which you can find in Desktop\Files\SSH\admin.txt.

To resolve the alert that is being reported, go back to Prism Element and click on Resolve in the Alerts page.

To output the cluster-wide configuration of SCMA policy to Desktop\Files\output.txt before changes are made, you need to log in to Prism Element using the admin user credentials.

Go to Security > SCMA Policy and click on View Policy Details. This will show you the current settings of SCMA policy for each entity type.

Copy and paste these settings into a new text file named Desktop\Files\output.txt.

To enable AIDE (Advanced Intrusion Detection Environment) to run on a weekly basis for the cluster, you need to log in to Prism Element using the admin user credentials.

Go to Security > AIDE Configuration and click on Enable AIDE. This will enable AIDE to monitor file system changes on all CVMs and nodes in the cluster.

Select Weekly as the frequency of AIDE scans and click Save.

To enable high-strength password policies for the cluster, you need to log in to Prism Element using the admin user credentials.

Go to Security > Password Policy and click on Edit Policy. This will allow you to modify the password policy settings for each entity type.

For each entity type (Admin User, Console User, CVM User, and Host User), select High Strength as the password policy level and click Save.

To ensure CVMs require SSH keys for login instead of passwords, you need to log in to Prism Element using the admin user credentials.

Go to Security > Cluster Lockdown and click on Configure Lockdown. This will allow you to manage SSH access settings for the cluster.

Uncheck Enable Remote Login with Password. This will disable password-based SSH access to the cluster.

Click New Public Key and enter a name for the key and paste the public key value from Desktop\Files\SSH\id\_rsa.pub. This will add a public key for key-based SSH access to the cluster.

Click Save and Apply Lockdown. This will apply the changes and ensure CVMs require SSH keys for login instead of passwords. Part1

Enter CVM ssh and execute:

cluster status | grep -v UP

cluster start

If there are issues starting some services, check the following:

Check if the node is in maintenance mode by running the ncli host Is command on the CVM. Verify if the parameter Under Maintenance Mode is set to False for the node where the services are down. If the parameter Under Maintenance Mode is set to True, remove the node from maintenance mode by running the following command:

- \* nutanix@cvm\\$ ncli host edit id=<host id> enable-maintenance-mode=false You can determine the host ID by using ncli host ls. See the troubleshooting topics related to failed cluster services in the Advanced Administration Guide available from the Nutanix Portal's Software Documentation page. (Use the filters to search for the guide for your AOS version). These topics have information about common and AOS-specific logs, such as Stargate, Cassandra, and other modules.
- \* Check for any latest FATALs for the service that is down. The following command prints all the FATALs for a CVM. Run this command on all CVMs.

nutanix@cvm\$ for i in `svmips`; do echo "CVM: \$i"; ssh \$i "ls -ltr /home/nutanix/data/logs/\*.FATAL"; done NCC Health Check: cluster\_services\_down\_check (nutanix.com) Part2 Update the default password for the root user on the node to match the admin user password echo -e "CHANGING ALL AHV HOST ROOT PASSWORDS.\nPlease input new password: "; read -rs password1; echo "Confirm new password: "; read -rs password2; if [ "\$password1" == "\$password2" ]; then for host in \$(hostips); do echo Host \$host; echo \$password1 | ssh root@\$host "passwd --stdin root"; done; else echo "The passwords do not match"; fi Update the default password for the nutanix user on the CVM sudo passwd nutanix Output the cluster-wide configuration of the SCMA policy ncli cluster get-hypervisor-security-config Output Example:

nutanix@NTNX-372a19a3-A-CVM:10.35.150.184:~\$ ncli cluster get-hypervisor-security-config Enable Aide: false Enable Core: false Enable High Strength P...: false Enable Banner: false Schedule: DAILY Enable: TLB Multihit M...: false Enable the Advance intrusion Detection Environment (AIDE) to run on a weekly basis for the cluster.

ncli cluster edit-hypervisor-security-params enable-aide=true

ncli cluster edit-hypervisor-security-params schedule=weekly

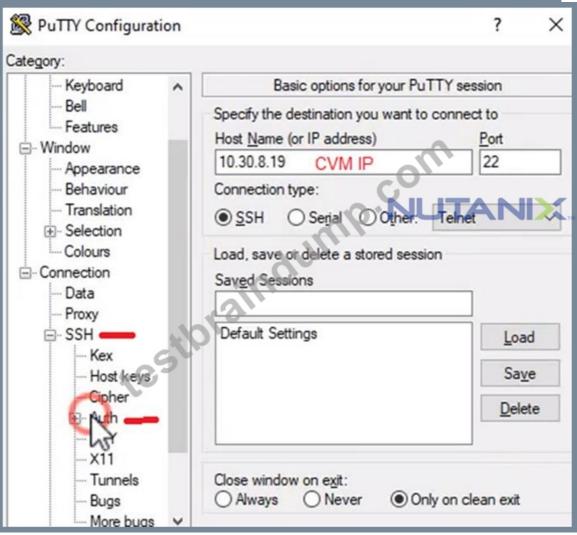
Enable high-strength password policies for the cluster.

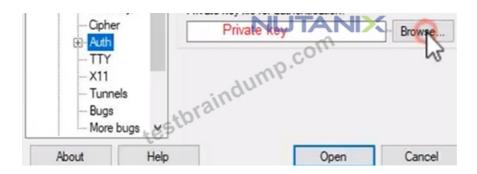
ncli cluster edit-hypervisor-security-params enable-high-strength-password=true Ensure CVMs require SSH keys for login instead of passwords

https://portal.nutanix.com/page/documents/kbs/details?targetId=kA060000008gb3CAA









#### **NEW QUESTION #19**

Task 15

An administrator found a CentOS VM, Cent\_Down, on the cluster with a corrupted network stack. To correct the issue, the VM will need to be restored from a previous snapshot to become reachable on the network again.

VM credentials: Username: root Password: nutanix/4u

Restore the VM and ensure it is reachable on the network by pinging 172.31.0.1 from the VM.

Power off the VM before proceeding.

#### Answer:

Explanation:

See the Explanation for step by step solution

Explanation:

To restore the VM and ensure it is reachable on the network, you can follow these steps:

Log in to the Web Console of the cluster where the VM is running.

Click on Virtual Machines on the left menu and find Cent Down from the list. Click on the power icon to power off the VM.

Click on the snapshot icon next to the power icon to open the Snapshot Management window.

Select a snapshot from the list that was taken before the network stack was corrupted. You can use the date and time information to choose a suitable snapshot.

Click on Restore VM and confirm the action in the dialog box. Wait for the restore process to complete.

Click on the power icon again to power on the VM.

Log in to the VM using SSH or console with the username and password provided.

Run the command ping 172.31.0.1 to verify that the VM is reachable on the network. You should see a reply from the destination IP address.

Go to VMS from the prism central gui

Select the VMand go to More -> Guest Shutdown

Go to Snapshots tab and revert to latest snapshot available

power on vm and verify if ping is working

#### **NEW QUESTION #20**

Task 3

An administrator needs to assess performance gains provided by AHV Turbo at the guest level. To perform the test the administrator created a Windows 10 VM named Turbo with the following configuration.

1 vCPU

8 GB RAM

SATA Controller

40 GB vDisk

The stress test application is multi-threaded capable, but the performance is not as expected with AHV Turbo enabled. Configure the VM to better leverage AHV Turbo.

Note: Do not power on the VM. Configure or prepare the VM for configuration as best you can without powering it on.

#### Answer:

Explanation:

See the Explanation for step by step solution

Explanation:

To configure the VM to better leverage AHV Turbo, you can follow these steps:

Log in to Prism Element of cluster A using the credentials provided.

Go to VM > Table and select the VM named Turbo.

Click on Update and go to Hardware tab.

Increase the number of vCPUs to match the number of multiqueues that you want to enable. For example, if you want to enable 8 multiqueues, set the vCPUs to 8. This will improve the performance of multi-threaded workloads by allowing them to use multiple processors.

Change the SCSI Controller type from SATA to VirtIO. This will enable the use of VirtIO drivers, which are required for AHV Turbo.

Click Save to apply the changes.

Power off the VM if it is running and mount the Nutanix VirtIO ISO image as a CD-ROM device. You can download the ISO image from Nutanix Portal.

Power on the VM and install the latest Nutanix VirtIO drivers for Windows 10. You can follow the instructions from Nutanix Support Portal.

After installing the drivers, power off the VM and unmount the Nutanix VirtIO ISO image.

Power on the VM and log in to Windows 10.

Open a command prompt as administrator and run the following command to enable multiqueue for the VirtIO NIC: ethtool -L eth0 combined 8

Replace eth0 with the name of your network interface and 8 with the number of multiqueues that you want to enable. You can use ipconfig/all to find out your network interface name.

Restart the VM for the changes to take effect.

You have now configured the VM to better leverage AHV Turbo. You can run your stress test application again and observe the performance gains.

https://portal.nutanix.com/page/documents/kbs/details?targetId=kA00e000000LKPdCAO change vCPU to 2/4?

Change SATA Controller to SCSI:

```
acli vm.get Turbo
Output Example:
Turbo {
config {
agent_vm: False
allow_live_migrate: True
boot {
boot device order: "kCdrom"
boot device order: "kDisk"
boot device order: "kNetwork"
uefi boot: False
cpu passthrough: False
disable branding: False
disk list {
addr {
bus: "ide"
index: 0
cdrom: True
device uuid: '994b7840-dc7b-463e-a9bb-1950d7138671"
empty: True
disk list {
addr {
bus: "sata"
index: 0
container id: 4
container uuid: "49b3e1a4-4201-4a3a-8abc-447c663a2a3e"
device uuid: "622550e4-fb91-49dd-8fc7-9e90e89a7b0e"
naa id: "naa.6506b8dcda1de6e9ce911de7d3a22111"
storage vdisk uuid: "7e98a626-4cb3-47df-a1e2-8627cf90eae6"
vmdisk size: 10737418240
vmdisk uuid: "17e0413b-9326-4572-942f-68101f2bc716"
}
```

```
flash mode: False
hwclock timezone: "UTC"
machine type: "pc"
memory mb: 2048
name: "Turbo"
nic list {
connected: True
mac addr: "50:6b:8d:b2:a5:e4"
network name: "network"
network type: "kNativeNetwork"
network uuid: "86a0d7ca-acfd-48db-b15c-5d654ff39096"
type: "kNormalNic"
uuid: "b9e3e127-966c-43f3-b33c-13608154c8bf"
vlan mode: "kAccess"
num cores per vcpu: 2
num threads per core: 1
num vcpus: 2
num vnuma nodes: 0
vga console: True
vm type: "kGuestVM"
is rfl vm: False
logical timestamp: 2
state: 'Off'
uuid: "9670901f-8c5b-4586-a699-41f0c9ab26c3"
acli vm.disk create Turbo clone from vmdisk=17e0413b-9326-4572-942f-68101f2bc716 bus=scsi remove the old disk acli
vm.disk delete 17e0413b-9326-4572-942f-68101f2bc716 disk addr=sata.0
NEW QUESTION #21
NCM-MCI Practice Braindumps: https://www.testbraindump.com/NCM-MCI-exam-prep.html
   • New NCM-MCI Test Topics □ Top NCM-MCI Questions □ Exam NCM-MCI Materials □ Search for □ NCM-
     MCI □ and obtain a free download on 「 www.testkingpass.com 」 □NCM-MCI Reliable Test Labs
   • Pdfvce Nutanix NCM-MCI Desktop Practice Exam □ Enter □ www.pdfvce.com □ and search for ➤ NCM-MCI □ to
     download for free □New NCM-MCI Cram Materials

    Latest NCM-MCI Test Pdf □ Exam NCM-MCI Materials □ Dump NCM-MCI File □ Search on ►

     www.pass4test.com □ for ( NCM-MCI ) to obtain exam materials for free download □Valid NCM-MCI Test Cost
   • Latest NCM-MCI Exam Practice □ Dump NCM-MCI File □ Reliable NCM-MCI Test Preparation □ Go to website
     ⇒ www.pdfvce.com ∈ open and search for □ NCM-MCI □ to download for free □New NCM-MCI Test Topics
   search for ► NCM-MCI 	for free download on [ www.dumpsmaterials.com ] □Reliable NCM-MCI Dumps Free
   • Free PDF Newest NCM-MCI - Nutanix Certified Master - Multicloud Infrastructure v6.10 Valid Dumps Demo 

Open {
     www.pdfvce.com } enter □ NCM-MCI □ and obtain a free download ⊚ Exam NCM-MCI Materials
   • New NCM-MCI Test Topics □ NCM-MCI Latest Version □ NCM-MCI Latest Version □ Search for ✔ NCM-
     MCI \square \checkmark \square and download exam materials for free through \Longrightarrow www.verifieddumps.com \square \squareNew NCM-MCI Test
   • Latest Braindumps NCM-MCI Ebook ☐ Latest NCM-MCI Exam Practice ☐ Free NCM-MCI Exam Questions ☐
     Open ➡ www.pdfvce.com □ enter ➡ NCM-MCI □ and obtain a free download □Reliable NCM-MCI Study
     Materials
   • TOP NCM-MCI Valid Dumps Demo: Nutanix Certified Master - Multicloud Infrastructure v6.10 - Trustable Nutanix
     NCM-MCI Practice Braindumps □ Easily obtain ⇒ NCM-MCI ∈ for free download through 【
     www.dumpsquestion.com ] \square Reliable NCM-MCI Dumps Free
   • Free PDF Quiz Nutanix - NCM-MCI – Trustable Valid Dumps Demo 🗆 Enter ( www.pdfvce.com ) and search for 🗢
     NCM-MCI □ to download for free □Valid NCM-MCI Test Cost
   • Latest NCM-MCI Exam Practice □ Reliable NCM-MCI Test Preparation □ Reliable NCM-MCI Study Materials □
```

The page for free download of ⇒ NCM-MCI ∈ on ( www.testkingpass.com ) will open immediately □Exam NCM-MCI

#### Materials

• myportal.utt.edu.tt, myporta