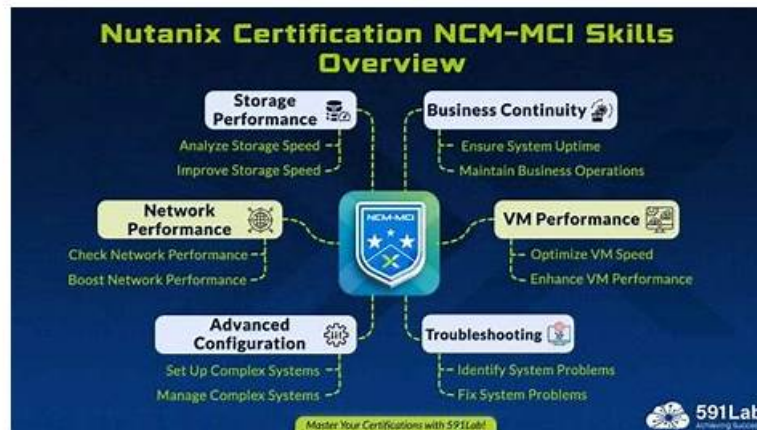


# Nutanix NCM-MCI Certification Exam, Dumps NCM-MCI Free



2026 Latest Itbraindumps NCM-MCI PDF Dumps and NCM-MCI Exam Engine Free Share: <https://drive.google.com/open?id=1fmJFuPFS-TpkGtiODsqv9EC4R548uUA4>

With “reliable credit” as the soul of our NCM-MCI study tool, “utmost service consciousness” as the management philosophy, we endeavor to provide customers with high quality service. Our customer service staff, who are willing to be your little helper and answer your any questions about our Nutanix Certified Master - Multicloud Infrastructure v6.10 qualification test, fully implement the service principle of customer-oriented service activities, aiming at comprehensive, coordinated and sustainable cooperation relationship with every users. Any puzzle about our NCM-MCI Test Torrent will receive timely and effective response, just leave a message on our official website or send us an e-mail at your convenience.

## Nutanix NCM-MCI Exam Information

- Time Duration: 60 minutes
- The passing score: 73%
- Languages: English

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

The Average salary of different countries of Nutanix Certified Expert

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

## How to Succeed in Nutanix NCM-MCI Exam

Nutanix NCM-MCI Exam is an essential source for your successful certification. So the materials will help you to pass the exam.

Now, we are providing you the opportunity of experiencing our best service by offering the **Nutanix NCM-MCI Dumps** Package. It is a bundle pack that includes all the Nutanix NCM-MCI Dumps required for Nutanix NCM-MCI exam.

We have included in it all of our products because according to our research their combination has proven very effective for passing Nutanix NCM-MCI Exam. If you prepare for this exam using these products individually, it may not be easy for you to pass it in one attempt. The reason is that each product has its separate function and topics which when combined with other products make a complete study package for passing Nutanix NCM-MCI Exam successfully.

So, we recommend you to use this powerful package instead of individual products if you really want to save your time and money while achieving your goal of becoming Nutanix Certified Professional.

## Free Nutanix NCM-MCI Exam Questions Updates By Itbraindumps

Cease to struggle and you cease to live. Only by continuous learning can we not be surpassed by others. Many people do not like to study and think that learning is a very vexing thing. This kind of cognition makes their careers stagnate. NCM-MCI test question will change your perception. NCM-MCI learning dumps aim to help students learn easily and effectively that has been developed over many years by many industry experts. For the online version, unlike other materials that limit one person online, NCM-MCI learning dumps does not limit the number of concurrent users and the number of online users. You can practice anytime, anywhere, practice repeatedly, practice with others, and even purchase together with others. NCM-MCI learning dumps make every effort to help you save money and effort, so that you can pass the exam with the least cost.

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

#### NEW QUESTION # 16

Task 13

The application team is reporting performance degradation for a business-critical application that runs processes all day on Saturdays.

The team is requesting monitoring of processor, memory and storage utilization for the three VMs that make up the database cluster for the application: ORA01, ORA02 and ORA03.

The report should contain tables for the following:

At the cluster level, only for the current cluster:

The maximum percentage of CPU used

At the VM level, including any future VM with the prefix ORA:

The maximum time taken to process I/O Read requests

The Maximum percentage of time a VM waits to use physical CPU, out of the local CPU time allotted to the VM.

The report should run on Sundays at 12:00 AM for the previous 24 hours. The report should be emailed to appdev@cyberdyne.net when completed.

Create a report named Weekends that meets these requirements

Note: You must name the report Weekends to receive any credit. Any other objects needed can be named as you see fit. SMTP is not configured.

A: Click Next.

Click on Add to add this custom view to your report. Click Next.

Under the Report Settings option, select Weekly from the Schedule drop-down menu and choose Sunday as the day of week. Enter 12:00 AM as the time of day. Enter appdev@cyberdyne.net as the Email Recipient. Select CSV as the Report Output Format.

Click Next.

Review the report details and click Finish.

#### Answer:

Explanation:

See the Explanation for step by step solution

Explanation:

To create a report named Weekends that meets the requirements, 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 Report.

Enter Weekends as the report name and a description if required. Click Next.

Under the Custom Views section, select Data Table. Click Next.

Under the Entity Type option, select Cluster. Click Next.

Under the Custom Columns option, add the following variable: CPU Usage (%). Click Next.

Under the Aggregation option for CPU Usage (%), select Max. Click Next.

Under the Filter option, select Current Cluster from the drop-down menu. Click Next.

Click on Add to add this custom view to your report. Click Next.

Under the Custom Views section, select Data Table again. Click Next.

Under the Entity Type option, select VM. Click Next.

Under the Custom Columns option, add the following variables: Name, I/O Read Latency (ms), VM Ready Time (%). Click Next.

Under the Aggregation option for I/O Read Latency (ms) and VM Ready Time (%), select Max. Click Next.

Under the Filter option, enter ORA\* in the Name field. This will include any future VM with the prefix OR

## NEW QUESTION # 17

### Task4

An administrator will be deploying Flow Networking and needs to validate that the environment, specifically switch vs1, is appropriately configured. Only VPC traffic should be carried by the switch.

Four versions each of two possible commands have been placed in Desktop\Files\Network\flow.txt. Remove the hash mark (#) from the front of correct First command and correct Second command and save the file.

Only one hash mark should be removed from each section. Do not delete or copy lines, do not add additional lines. Any changes other than removing two hash marks (#) will result in no credit.

Also, SSH directly to any AHV node (not a CVM) in the cluster and from the command line display an overview of the Open vSwitch configuration. Copy and paste this to a new text file named Desktop\Files\Network\AHVswitch.txt.

Note: You will not be able to use the 192.168.5.0 network in this environment.

First command

```
#net.update_vpc_traffic_config virtual_switch=vs0
net.update_vpc_traffic_config virtual_switch=vs1
#net.update_vpc_east_west_traffic_config virtual_switch=vs0
#net.update_vpc_east_west_traffic_config virtual_switch=vs1
```

Second command

```
#net.update_vpc_east_west_traffic_config permit_all_traffic=true
net.update_vpc_east_west_traffic_config permit_vpc_traffic=true
#net.update_vpc_east_west_traffic_config permit_all_traffic=false
#net.update_vpc_east_west_traffic_config permit_vpc_traffic=false
```

### Answer:

Explanation:

See the Explanation for step by step solution

Explanation:

First, you need to open the Prism Central CLI from the Windows Server 2019 workstation. You can do this by clicking on the Start menu and typing "Prism Central CLI". Then, you need to log in with the credentials provided to you.

Second, you need to run the two commands that I have already given you in Desktop\Files\Network\flow.txt. These commands are: net.update\_vpc\_traffic\_config virtual\_switch=vs1 net.update\_vpc\_east\_west\_traffic\_config permit\_vpc\_traffic=true These commands will update the virtual switch that carries the VPC traffic to vs1, and update the VPC east-west traffic configuration to allow only VPC traffic. You can verify that these commands have been executed successfully by running the command:

```
net.get_vpc_traffic_config
```

This command will show you the current settings of the virtual switch and the VPC east-west traffic configuration.

Third, you need to SSH directly to any AHV node (not a CVM) in the cluster and run the command:

```
ovs-vsctl show
```

This command will display an overview of the Open vSwitch configuration on the AHV node. You can copy and paste the output of this command to a new text file named Desktop\Files\Network\AHVswitch.txt.

You can use any SSH client such as PuTTY or Windows PowerShell to connect to the AHV node. You will need the IP address and the credentials of the AHV node, which you can find in Prism Element or Prism Central.

remove # from greens

On AHV execute:

```
sudo ovs-vsctl show
```

CVM access AHV access command

```
nutanix@NTNX-A-CVM:192.168.10.5:~$ ssh root@192.168.10.2 "ovs-vsctl show" Open AHVswitch.txt and copy paste output
```

## NEW QUESTION # 18

### Task 14

The application team has requested several mission-critical VMs to be configured for disaster recovery. The remote site (when added) will not be managed by Prism Central. As such, this solution should be built using the Web Console.

Disaster Recovery requirements per VM:

Mkt01

RPO: 2 hours

Retention: 5 snapshots

Fin01

RPO: 15 minutes

Retention: 7 days

Dev01

RPO: 1 day

Retention: 2 snapshots

Configure a DR solution that meets the stated requirements.

Any objects created in this item must start with the name of the VM being protected.

Note: the remote site will be added later

**Answer:**

Explanation:

See the Explanation for step by step solution

Explanation:

To configure a DR solution that meets the stated requirements, you can follow these steps:

Log in to the Web Console of the source cluster where the VMs are running.

Click on Protection Domains on the left menu and click on Create Protection Domain.

Enter a name for the protection domain, such as PD\_Mkt01, and a description if required. Click Next.

Select Mkt01 from the list of VMs and click Next.

Select Schedule Based from the drop-down menu and enter 2 hours as the interval. Click Next.

Select Remote Site from the drop-down menu and choose the remote site where you want to replicate the VM. Click Next.

Enter 5 as the number of snapshots to retain on both local and remote sites. Click Next.

Review the protection domain details and click Finish.

Repeat the same steps for Fin01 and Dev01, using PD\_Fin01 and PD\_Dev01 as the protection domain names, and adjusting the interval and retention values according to the requirements.

□  
□  
□  
□

**NEW QUESTION # 19**

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

□

## NEW QUESTION # 20

### Task 8

Depending on the order you perform the exam items, the access information and credentials could change. Please refer to the other item performed on Cluster B if you have problems accessing the cluster.

The infosec team has requested that audit logs for API Requests and replication capabilities be enabled for all clusters for the top 4 severity levels and pushed to their syslog system using highest reliability possible. They have requested no other logs to be included.

Syslog configuration:

Syslog Name: Corp\_syslog

Syslog IP: 34.69.43.123

Port: 514

Ensure the cluster is configured to meet these requirements.

### Answer:

Explanation:

See the Explanation for step by step solution

Explanation:

To configure the cluster to meet the requirements of the infosec team, you need to do the following steps:

Log in to Prism Central and go to Network > Syslog Servers > Configure Syslog Server. Enter Corp\_syslog as the Server Name, 34.69.43.123 as the IP Address, and 514 as the Port. Select TCP as the Transport Protocol and enable RELP (Reliable Logging Protocol). This will create a syslog server with the highest reliability possible.

Click Edit against Data Sources and select Cluster B as the cluster. Select API Requests and Replication as the data sources and set the log level to CRITICAL for both of them. This will enable audit logs for API requests and replication capabilities for the top 4 severity levels (EMERGENCY, ALERT, CRITICAL, and ERROR) and push them to the syslog server. Click Save.

Repeat step 2 for any other clusters that you want to configure with the same requirements.

☐

To configure the Nutanix clusters to enable audit logs for API Requests and replication capabilities, and push them to the syslog system with the highest reliability possible, you can follow these steps:

Log in to the Nutanix Prism web console using your administrator credentials.

Navigate to the "Settings" section or the configuration settings interface within Prism.

Locate the "Syslog Configuration" or "Logging" option and click on it.

Configure the syslog settings as follows:

Syslog Name: Enter "Corp\_syslog" as the name for the syslog configuration.

Syslog IP: Set the IP address to "34.69.43.123", which is the IP address of the syslog system.

Port: Set the port to "514", which is the default port for syslog.

Enable the option for highest reliability or persistent logging, if available. This ensures that logs are sent reliably and not lost in case of network interruptions.

Save the syslog configuration.

Enable Audit Logs for API Requests:

In the Nutanix Prism web console, navigate to the "Cluster" section or the cluster management interface.

Select the desired cluster where you want to enable audit logs.

Locate the "Audit Configuration" or "Security Configuration" option and click on it.

Look for the settings related to audit logs and API requests. Enable the audit logging feature and select the top 4 severity levels to be logged.

Save the audit configuration.

Enable Audit Logs for Replication Capabilities:

In the Nutanix Prism web console, navigate to the "Cluster" section or the cluster management interface.

Select the desired cluster where you want to enable audit logs.

Locate the "Audit Configuration" or "Security Configuration" option and click on it.

Look for the settings related to audit logs and replication capabilities. Enable the audit logging feature and select the top 4 severity levels to be logged.

Save the audit configuration.

After completing these steps, the Nutanix clusters will be configured to enable audit logs for API Requests and replication capabilities. The logs will be sent to the specified syslog system with the highest reliability possible.

ncli

```
<ncli> rsyslog-config set-status enable=false
```

```
<ncli> rsyslog-config add-server name=Corp_Syslog ip-address=34.69.43.123 port=514 network-protocol=tdp relp-enabled=false
```

```
<ncli> rsyslog-config add-module server-name= Corp_Syslog module-name=APLOS level=INFO
```

```
<ncli> rsyslog-config add-module server-name= Corp_Syslog module-name=CEREBRO level=INFO
```

