

NCM-MCI-6.5^{Q&As}

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

Pass NCM-MCI-6.5 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/ncm-mci-6-5.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Official
Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



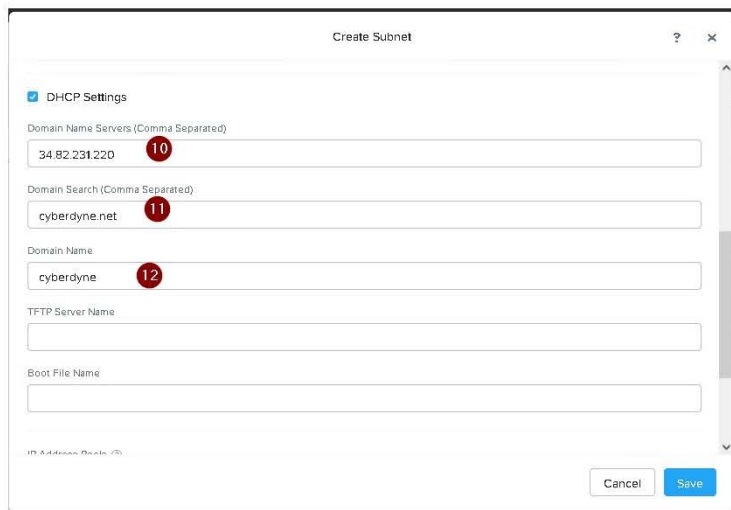
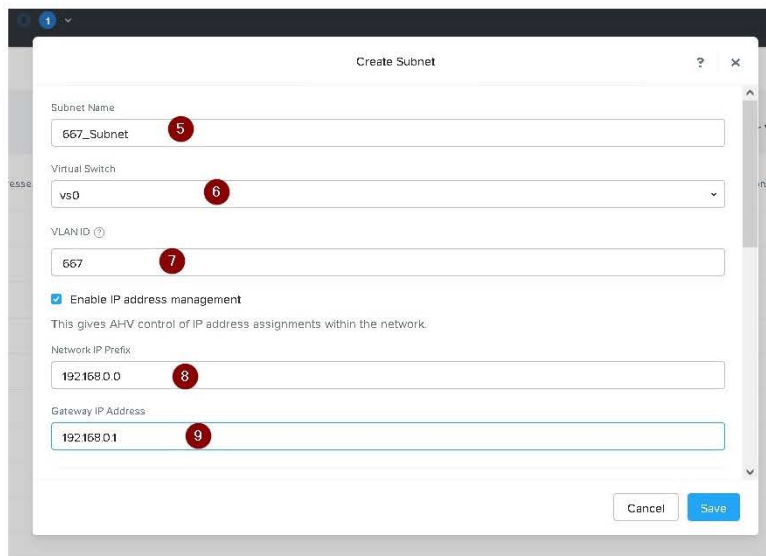
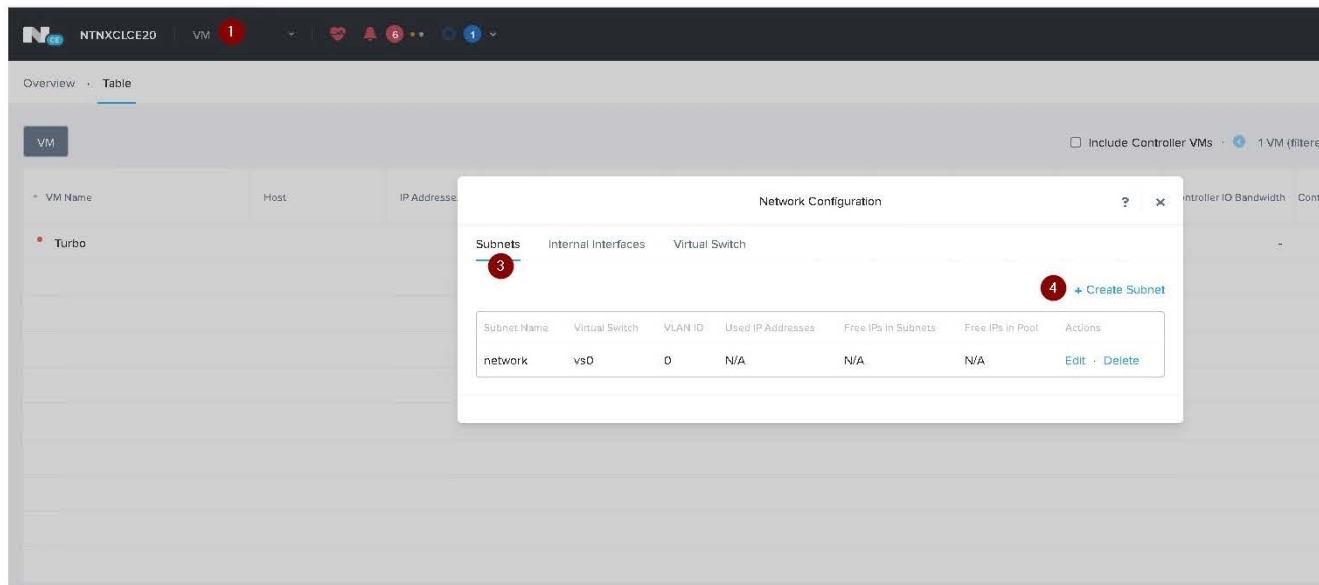
QUESTION 1

CORRECT TEXT Task 5 An administrator has been informed that a new workload requires a logically segmented network to meet security requirements. Network configuration: VLAN: 667 Network: 192.168.0.0 Subnet Mask: 255.255.255.0 DNS server: 34.82.231.220 Default Gateway: 192.168.0.1 Domain: cyberdyne.net IP Pool: 192.168.9.100-200 DHCP Server IP: 192.168.0.2 Configure the cluster to meet the requirements for the new workload if new objects are required, start the name with 667.

A. Answer: See the for step by step solution.

Correct Answer: A

To configure the cluster to meet the requirements for the new workload, you need to do the following steps: Create a new VLAN with ID 667 on the cluster. You can do this by logging in to Prism Element and going to Network Configuration > VLANs > Create VLAN. Enter 667 as the VLAN ID and a name for the VLAN, such as 667_VLAN. Create a new network segment with the network details provided. You can do this by logging in to Prism Central and going to Network > Network Segments > Create Network Segment. Enter a name for the network segment, such as 667_Network_Segment, and select 667_VLAN as the VLAN. Enter 192.168.0.0 as the Network Address and 255.255.255.0 as the Subnet Mask. Enter 192.168.0.1 as the Default Gateway and 34.82.231.220 as the DNS Server. Enter cyberdyne.net as the Domain Name. Create a new IP pool with the IP range provided. You can do this by logging in to Prism Central and going to Network > IP Pools > Create IP Pool. Enter a name for the IP pool, such as 667_IP_Pool, and select 667_Network_Segment as the Network Segment. Enter 192.168.9.100 as the Starting IP Address and 192.168.9.200 as the Ending IP Address. Configure the DHCP server with the IP address provided. You can do this by logging in to Prism Central and going to Network > DHCP Servers > Create DHCP Server. Enter a name for the DHCP server, such as 667_DHCP_Server, and select 667_Network_Segment as the Network Segment. Enter 192.168.0.2 as the IP Address and select 667_IP_Pool as the IP Pool.



Create Subnet

?

×

cyberdyne.net

Domain Name

cyberdyne

TFTP Server Name

Boot File Name

IP Address Pools ?

+ Create Pool

13

No pools added.

☐ Override DHCP server ?

Cancel

Save

Create Subnet

Boot File Name

IP Address Pools ?

+ Create Pool

Start Address

End Address

192.168.9.100

14

192.168.9.200

☒ Override DHCP server 15

DHCP Server IP Address

192.168.0.2

16

Cancel

Save 17

QUESTION 2

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

A. Answer: See the for step by step solution.

Correct Answer: A

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>

QUESTION 3

CORRECT TEXT

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 toappdev@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. Answer: See the for step by step solution.

Correct Answer: A

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 ORA. 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.

ADD VIEWS

Custom Predefined All

Q Type to filter...

CUSTOM VIEWS

- Bar Chart
- Line Chart
- Histogram
- Data Table
- Configuration Summary
- Metric Summary
- Entity Count
- Title and Description
- Group

Report Preview

Add Data Table

Select the entities that need to be reported in the view.

ENTITY TYPE

Nutanix Entities : VM

☐ All vms

☒ Specific vms

Rules

In case of multiple rules, a conjunction (AND operator) will be applied between them

Name : Starts with : ORA **OR**

Columns

FOCUS Custom Columns

Custom

Column Name	Aggregation
CPU Usage	Max
Controller Read IO Latency	Max
CPU Ready Time	Average
Name	-

Sorting

Cancel Add

QUESTION 4

CORRECT TEXT

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.

A. Answer: See the for step by step solution.

Correct Answer: A

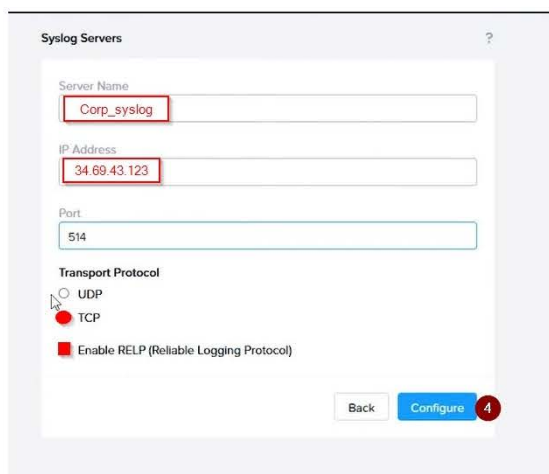
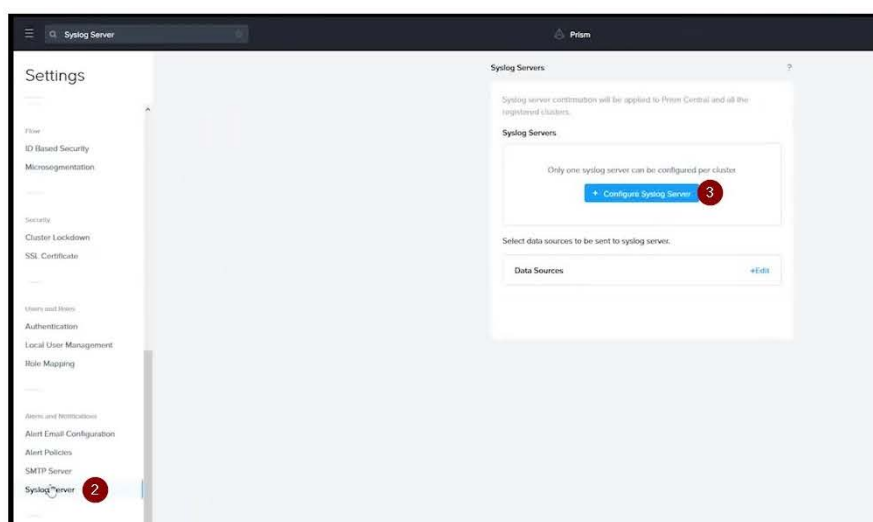
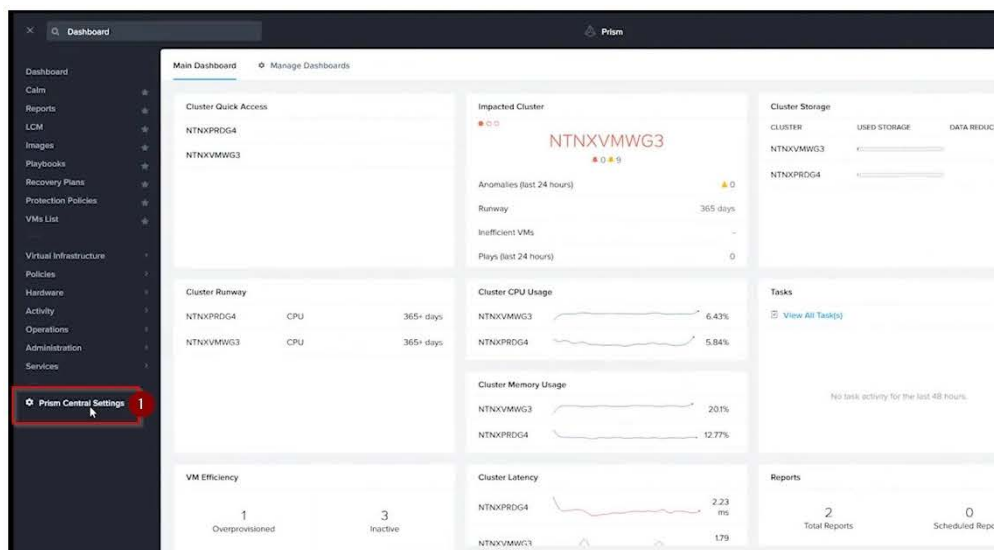
To configure the cluster to meet the requirements of the infosec team, you need to do the following steps:

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.



Syslog Servers

Syslog server confirmation will be applied to Prism Central and all the registered clusters.

Syslog Servers [+Configure Syslog Server](#)

Name	Server IP
Corp_syslog	34.69.43.123

Select data sources to be sent to syslog server.

Data Sources
[+Edit](#)

Prism

Syslog Servers

Data Sources and Respective Severity Level

Module Name	Severity Level
<input checked="" type="checkbox"/> API Audit	<div>Select Severity Level</div> <div> 0 - Emergency: system is unusable 1 - Alert: action must be taken immediately 2 - Critical: critical conditions 3 - Error: error conditions 4 - Warning: warning conditions 5 - Notice: normal but significant condition 6 - Informational: informational messages 7 - Debug: debug-level messages </div>

| ☒ Audit | |
| ☒ Flow | |

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.

nccli

```
rsyslog-config set-status enable=false
```

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

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

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

```
rsyslog-config set-status enable=true
```

<https://portal.nutanix.com/page/documents/kbs/details?targetId=kA00e0000009CEECA2>

QUESTION 5**CORRECT TEXT****Task 12**

An administrator needs to create a report named VMs_Power_State that lists the VMs in the cluster and their basic details including the power state for the last month.

No other entities should be included in the report.

The report should run monthly and should send an email to admin@syberdyne.net when it runs.

Generate an instance of the report named VMs_Power_State as a CSV and save the zip file as Desktop\Files\VMs_Power_state.zip

Note: Make sure the report and zip file are named correctly. The SMTP server will not be configured.

A. Answer: See the for step by step solution.

Correct Answer: A

To create a report named VMs_Power_State that lists the VMs in the cluster and their basic details including the power state for the last month, 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 VMs_Power_State 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 VM. Click Next. Under the Custom Columns option, add the following variables: Name, Cluster Name, vCPUs, Memory, Power State. Click Next.

Under the Time Period option, select Last Month. Click Next. Under the Report Settings option, select Monthly from the Schedule drop-down menu. Enter admin@syberdyne.net as the Email Recipient. Select CSV as the Report Output

Format. Click Next.

Review the report details and click Finish.

To generate an instance of the report named VMs_Power_State as a CSV and save the zip file as Desktop\Files\VMs_Power_state.zip, you can follow these steps:

Log in to Prism Central and click on Operations on the left menu. Select Reports from the drop-down menu and find the VMs_Power_State report from the list. Click on Run Now.

Wait for the report to be generated and click on Download Report. Save the file as Desktop\Files\VMs_Power_state.zip.

1. Open the Report section on Prism Central (Operations > Reports) 2. Click on the New Report button to start the creation of your custom report 3. Under the Custom Views section, select Data Table 4. Provide a title to your custom report, as

well as a description if required.

5. Under the Entity Type option, select VM

6. This report can include all as well as a selection of the VMs 7. Click on the Custom Columns option and add the below

variables:

a.Name - Name of the listed Virtual Machine

b.vCPUs - A combination of the vCores and vCPU's assigned to the Virtual Machine c.Memory - Amount of memory assigned to the Virtual Machine d.Disk Capacity - The total amount of assigned virtual disk capacity e.Disk Usage - The total

used virtual disk capacity f.Snapshot Usage - The total amount of capacity used by snapshots (Excluding Protection Domain snapshots)

8.Under the Aggregation option for Memory and Disk Usage accept the default Average option

Columns

FOCUS

Custom Columns

Custom	
Column Name	Aggregation
Name	-
vCPUs	-
Memory	Average ▾
Disk Capacity	-
Disk Usage	Average ▾
Snapshot Usage	-

9.Click on the Add button to add this custom selection to your report 10.Next click on the Save and Run Now button on the bottom right of the screen 11.Provide the relevant details on this screen for your custom report:

12.You can leave the Time Period For Report variable at the default of Last 24 Hours 13.Specify a report output of preference (PDF or CSV) and if required Additional Recipients for this report to be mailed to. The report can also simply be

downloaded after this creation and initial run if required

14. Below is an example of this report in a CSV format:

[NCM-MCI-6.5 PDF Dumps](#)

[NCM-MCI-6.5 VCE Dumps](#)

[NCM-MCI-6.5 Braindumps](#)