

# ハイパスレートのNCM-MCI専門試験一回合格-効果的なNCM-MCI日本語独学書籍

## 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

当社は、NCM-MCI学習教材の新しいバージョンのリリースに成功しました。おそらく、NCM-MCI試験の準備に深く悩まされているでしょう。これで、NCM-MCI学習教材の助けを借りて、完全にリラックスした気分になります。当社の製品は信頼性が高く、優れています。さらに、当社のNCM-MCI学習教材の合格率は市場で最高です。NCM-MCI学習教材を購入することは、あなたが半分成功したことを意味します。NCM-MCI試験に初めて合格する場合、適切な決定は非常に重要です。

当社Tech4Examは多くの優秀な専門家や教授がいます。過去数年、これらの専門家と教授は、すべての顧客向けにNCM-MCI試験問題を設計するために最善を尽くしました。さらに重要なことは、最終的にNCM-MCI試験問題でNCM-MCI認定を取得すると、人生の楽しみと人間関係の改善、ストレスの軽減、全体的な生活の質の向上という大きなメリットが得られることです。そのため、NCM-MCI試験に合格し、関連する認定を取得するために全力を尽くすことは非常に重要です。

>> NCM-MCI専門試験 <<

## 正確的なNutanix NCM-MCI専門試験 & 合格スムーズNCM-MCI日本語独学書籍 | 完璧なNCM-MCI日本語参考

NCM-MCI学習教材を練習した後、NCM-MCI試験トレントから試験ポイントをマスターできます。その後、

NCM-MCI試験に合格するのに十分な自信があります。ひとつのことに努力すれば成功できます。安全な環境と効果的な製品については、NCM-MCIテスト問題を試してみてください。決して失望させないでください。購入する前に、NCM-MCIトレーニング資料の無料デモがあります。ご購入前に、NCM-MCIガイドの質問の質を早く知ることができます。

## Nutanix NCM-MCI 認定試験の出題範囲:

トピック	出題範囲
トピック 1	<ul style="list-style-type: none"><li>高度な構成とトラブルシューティング:このトピックでは、API 呼び出しの実行、サードパーティ統合の構成、AOS セキュリティ体制の分析、およびビジネス ニーズの技術的ソリューションへの変換に関するサブトピックを取り上げます。最後に、Nutanix サービスのトラブルシューティングについても説明します。</li></ul>
トピック 2	<ul style="list-style-type: none"><li>ネットワーク パフォーマンスの分析と最適化:このトピックの焦点は、オーバーレイ ネットワーク、物理ネットワーク、仮想ネットワーク、ネットワーク構成、およびフロー ポリシーです。さらに、構成に関する質問も表示されます。</li></ul>
トピック 3	<ul style="list-style-type: none"><li>ビジネス継続性:ビジネス継続性のトピックでは、コンプライアンスのための BCDR 計画の分析と、特定のワークロードの BCDR 計画の評価に関する知識を測定します。</li></ul>
トピック 4	<ul style="list-style-type: none"><li>VM パフォーマンスの分析と最適化:このトピックでは、リソース使用率のための VM 構成の操作について説明します。また、VM、ノード、クラスターのメトリックの解釈についても説明します。</li></ul>
トピック 5	<ul style="list-style-type: none"><li>ストレージ パフォーマンスの分析と最適化:ストレージ設定、ワークロード要件、ストレージ内部について説明します。</li></ul>

## Nutanix Certified Master - Multicloud Infrastructure v6.10 認定 NCM-MCI 試験問題 (Q14-Q19):

### 質問 # 14

#### 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.

### 正解:

#### 解説:

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 VM and go to More -> Guest Shutdown

Go to Snapshots tab and revert to latest snapshot available  
power on vm and verify if ping is working

### 質問 # 15

#### Task 16

Running NCC on a cluster prior to an upgrade results in the following output FAIL: CVM System Partition /home usage at 93% (greater than threshold, 90%) Identify the CVM with the issue, remove the file causing the storage bloat, and check the health again by running the individual disk usage health check only on the problematic CVM do not run NCC health check Note: Make sure only the individual health check is executed from the affected node

#### 正解:

#### 解説:

See the Explanation for step by step solution

#### Explanation:

To identify the CVM with the issue, remove the file causing the storage bloat, and check the health again, 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 find the NCC health check output file from the list. You can use the date and time information to locate the file. The file name should be something like ncc-output-YYYY-MM-DD-HH-MM-SS.log

Open the file and look for the line that says FAIL: CVM System Partition /home usage at 93% (greater than threshold, 90%). Note down the IP address of the CVM that has this issue. It should be something like X.X.X.X.

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

Run the command `du -sh /home/*` to see the disk usage of each file and directory under /home. Identify the file that is taking up most of the space. It could be a log file, a backup file, or a temporary file. Make sure it is not a system file or a configuration file that is needed by the CVM.

Run the command `rm -f /home/<filename>` to remove the file causing the storage bloat. Replace <filename> with the actual name of the file.

Run the command `ncc health_checks hardware_checks disk_checks disk_usage_check --cvm_list=X.X.X.X` to check the health again by running the individual disk usage health check only on the problematic CVM. Replace X.X.X.X with the IP address of the CVM that you noted down earlier.

Verify that the output shows PASS: CVM System Partition /home usage at XX% (less than threshold, 90%). This means that the issue has been resolved.

#access to CVM IP by Putty

allssh df -h #look for the path /dev/sdb3 and select the IP of the CVM

ssh CVM\_IP

ls

cd software\_downloads

ls

cd nos

ls -l -h

rm files\_name

df -h

ncc health\_checks hardware\_checks disk\_checks disk\_usage\_check

### 質問 # 16

Refer to the exhibit.

□  
□  
□

#### Task1

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 monitorvm2 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

**正解:**

**解説:**

See the Explanation

Explanation:

This is a classic Nutanix performance troubleshooting scenario. The issue is almost certainly that the VM was created using the wrong Disk Bus Type (IDE or SATA instead of SCSI).

Here is the step-by-step solution to complete Task 1.

Part 1: Analysis and Reporting

Create the Session

Log in to Prism Central (or Prism Element, depending on the exam environment, but Analysis is usually a PC feature).

Navigate to Operations -> Analysis.

Click New Session.

Name: Monitor SQL02

Entity: Search for and select the VM named SQL02.

Metrics: Since the issue is storage performance, search for and add these specific metrics:

Hypervisor IOPS (or Controller IOPS)

Hypervisor IO Latency (or Controller IO Latency)

Hypervisor IO Bandwidth

Click Save.

Save Session Data (Task 1.txt)

Open the "Monitor SQL02" session you just created.

(Per instructions): Right-click anywhere on the chart/data area -> Click Select All.

Copy the selected text (Ctrl+C).

Open Notepad on the provided desktop.

Paste the data.

Save the file as Task 1.txt on the Desktop.

Create and Schedule the Report

While still in the Analysis session, click the Create Report (or "Add to Report") button.

Report Name: MonitorSQL02

Report Settings:

Format: PDF

Frequency: Daily

Email Recipient: perf\_group@ACME.org

Retention: 0 (or "Do not retain", as requested).

Note: If the system forces you to create a new Report object and MonitorSQL02 is rejected, use monitorvm2 as the name per the instructions.

Save/Schedule the report.

Part 2: Diagnose and Fix the Issue

The Issue:

VM SQL02 was likely created with its data disks set to IDE or SATA.

Why this causes poor performance: IDE/SATA are emulated hardware with high CPU overhead and low queue depths (single-threaded).

The Standard: SQL01 (the healthy VM) is using SCSI, which is multithreaded and optimized for virtualization.

The Fix (Steps):

Navigate to the VM list in Prism.

Select SQL02 and click Update (or Edit).

Scroll down to the Disks section.

Identify the data disk(s). You will see the Bus Type listed as IDE or SATA.

Do not delete the VM. instead, perform a disk conversion (destructive change to the disk is allowed, but we want to keep the data).

Method to Convert (Clone to SCSI):

Hover over the IDE/SATA disk to see the path/filename of the vDisk (or write it down).

Click Add New Disk.

Operation: select Clone from ADSF file.

Path: Browse to the storage container and select the file associated with the current IDE disk.

Bus Type: Select SCSI (This is the critical fix).

Index: Ensure it doesn't conflict with existing disks (usually index 1 or higher for data).

Click Add.

Once the new SCSI disk is added, find the original IDE/SATA disk and click the X to remove it.

Click Save.

Note: You do not need to power on the VM to verify. The change from IDE to SCSI allows the VM to use the Nutanix VirtIO drivers for maximum storage performance.

## 質問 # 17

### 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.

### 正解:

#### 解説:

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 ls` 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 `svnips`; 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 iTLB 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=kA0600000008gb3CAA>

11

## 質問 # 18

### 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.

### 正解:

### 解説:

See the Explanation for step by step solution

#### Explanation:

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

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:

## 質問 # 19

.....

この知識が支配的な世界では、知識と実用的な作業能力の組み合わせが非常に重要視されています。Tech4Exam 実際の能力を向上させたい場合は、NCM-MCI認定試験に参加できます。NCM-MCI認定に合格すると、実践能力と知識の両方を高めることができます。また、NCM-MCIの最新の質問を購入すると、NCM-MCI試験にスムーズに合格します。

