

NCM-MCI日本語参考 & NCM-MCI日本語対策問題集



2026年MogiExamの最新NCM-MCI PDFダンプおよびNCM-MCI試験エンジンの無料共有: <https://drive.google.com/open?id=1eX3QAmGut3DSKhCoh9RNVdGDAU8oX-92>

NutanixのNCM-MCI認定試験はMogiExamの最優秀な専門家チームが自分の知識と業界の経験を利用してどんどん研究した、満足Nutanix認証受験生の需要に満たすの書籍がほかのサイトにも見えますが、MogiExamの商品が最も保障があって、君の最良の選択になります。

試験は簡単ではないことは広く認められていますが、この分野の労働者にとって関連するNCM-MCI認定は非常に重要であるため、多くの労働者がこの課題に対処する必要があります。より効率的で簡単な方法で試験に合格し、関連する認定を取得する必要があります。最近の10年間で、NCM-MCI試験問題は、国際市場での温かい歓迎と迅速な販売に対応しました。NCM-MCI学習教材は、他のメーカーと同じくらいリーズナブルな価格であるだけでなく、次の点で明らかに優れています。

>> NCM-MCI日本語参考 <<

NCM-MCI日本語対策問題集、NCM-MCI日本語版テキスト内容

資格試験の意味は、いくつかの点で、さまざまな専門分野での能力を示す資格を取得する候補者の能力を証明することです。NCM-MCI学習ガイドの教材を選択すると、限られた学習時間でより多くの価値を生み出し、より多くの知識を学び、NCM-MCI試験を受けることができます。認定試験を通して、これはNCM-MCIの実際の質問であり、すべてのユーザーの共通の目標であり、信頼できるヘルパーです。NCM-MCI資格証明書の取得は、ユーザーのキャリア開発のニーズによりよく応えることができます。

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	• 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。
トピック 2	• 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。
トピック 3	• 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。

トピック 4	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。
トピック 5	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。

Nutanix Certified Master - Multicloud Infrastructure v6.10 認定 NCM-MCI 試験問題 (Q10-Q15):

質問 # 10

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 # 11

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.

正解:

解説:

See the Explanation for step by step solution

Explanation:

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.

□

質問 # 12

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 # 13

Task 2

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

Two VDI pools will be created

Non-persistent pool named 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.

正解:

解説:

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>

質問 # 14

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.

正解:

解説:

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
```

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

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

.....

NCM-MCI日本語対策問題集: <https://www.mogixam.com/NCM-MCI-exam.html>

- 無料でクラウドストレージから最新のMogiExamNCM-MCI PDFダンプをダウンロードする：<https://drive.google.com/open?id=1eX3QAmGut3DSKhcH9RNVDeDAU8oX-92>