NCM-MCI日本語練習問題 & NCM-MCI学習資料

2026年Topexam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=14uTWR8fX1GROn7tV8_zF9b4jr8Vryk5C

私たちは、このキャリアの中で、10年以上にわたりプロとしてNCM-MCI練習資料を作りました。NCM-MCI練習資料が最も全面的な参考書です。 そして、私たちは十分な耐久力を持って、ずっとNCM-MCI練習資料の研究に取り組んでいます。私たちのNCM-MCI練習資料を利用したら、NCM-MCI試験に合格した人がかなり多いです。だから、弊社のNCM-MCI練習資料を早く購入しましょう！

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	• Business Continuity: The topic of business continuity measures knowledge about analyzing BCDR plans for compliance and evaluating BCDR plans for specific workloads.
トピック 2	• Advanced Configuration and Troubleshooting: This topic covers sub-topics of executing API calls, configuring third-party integrations, analyzing AOS security posture, and translate business needs into technical solutions. Lastly, it discusses troubleshooting Nutanix services as well.
トピック 3	• Analyze and Optimize Storage Performance: It covers storage settings, workload requirements, and storage internals.

トピック 4	• Analyze and Optimize VM Performance: Manipulation of VM configuration for resource utilization is discussed in this topic. It also explains interpreting VM, node, and cluster metrics.
トピック 5	• Analyze and Optimize Network Performance: Focal points of this topic are overlay networking, physical networks, virtual networks, network configurations, and flow policies. Moreover, questions about configurations also appear.

>> NCM-MCI日本語練習問題 <<

信頼的NCM-MCI｜ハイパスレートのNCM-MCI日本語練習問題試験｜試験の準備方法Nutanix Certified Master - Multicloud Infrastructure v6.10学習資料

すべての働く人は、NCM-MCIがこの分野で支配的な人物であり、また彼らのキャリアに役立つことを知っています。 NCM-MCI信頼性の高い試験ブートキャンプが試験に合格し、資格証明書を取得するのに役立つ場合、より良いキャリア、より良い人生を得ることができます。 私たちの研究NCM-MCIガイド資料は、最新のNCM-MCIテストの質問と回答のほとんどを網羅しています。 確かにこの分野で何か違うことをしようと決心しているなら、役に立つ認定はあなたのキャリアの足がかりになるでしょう。

Nutanix Certified Master - Multicloud Infrastructure v6.10 認定 NCM-MCI 試験問題 (Q11-Q16):

質問 # 11
Topic 1, Performance Based Questions
Environment
You have been provisioned a dedicated environment for your assessment which includes the following:
Workstation
* windows Server 2019
* All software/tools/etc to perform the required tasks
* Nutanix Documentation and whitepapers can be found in desktop\files\Documentation
* Note that the workstation is the system you are currently togged into Nutanix Cluster
* There are three clusters provided. The connection information for the relevant cluster will be displayed to the high of the question Please make sure you are working on the correct cluster for each item Please ignore any licensing violations
* Cluster A is a 3-node cluster with Prism Central 2022.6 where most questions will be performed
* Cluster B is a one-node cluster and has one syslog item and one security item to perform
* Cluster D is a one-node duster with Prism Central 5.17 and has a security policy item to perform Important Notes
* If the text is too small and hard to read, or you cannot see an of the GUI. you can increase/decrease the zoom of the browser with CTRL + ,and CTRL + (the plus and minus keys) You will be given 3 hours to complete the scenarios for Nutanix NCMMCI Once you click the start button below, you will be provided with:
- A Windows desktop A browser page with the scenarios and credentials (Desktop\instructions) Notes for this exam delivery:
The browser can be scaled lo Improve visibility and fit all the content on the screen.
- Copy and paste hot-keys will not work Use your mouse for copy and paste.
- The Notes and Feedback tabs for each scenario are to leave notes for yourself or feedback for
- Make sure you are performing tasks on the correct components.
- Changing security or network settings on the wrong component may result in a falling grade.
- Do not change credentials on an component unless you are instructed to.
- All necessary documentation is contained in the Desktop\Files\Documentation directory Task 1 An administrator has been asked to configure a storage for a distributed application which uses large data sets across multiple worker VMs.
The worker VMs must run on every node. Data resilience is provided at the application level and low cost per GB is a Key Requirement.
Configure the storage on the cluster to meet these requirements. Any new object created should include the phrase Distributed_App in the name.

正解：

解説：

See the Explanation for step by step solution
Explanation:
To configure the storage on the cluster for the distributed application, you can follow these steps:
Log in to Prism Element of cluster A 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 Distributed_App_Storage_Pool, and select the disks to include in the pool. You can choose any combination of SSDs and HDDs, but for low cost per GB, you may prefer to use more HDDs than SSDs.
Click Save to create the storage pool.
Go to Storage > Containers and click on Create Container.
Enter a name for the new container, such as Distributed_App_Container, and select the storage pool that you just created, Distributed_App_Storage_Pool, as the source.
Under Advanced Settings, enable Erasure Coding and Compression to reduce the storage footprint of the dat a. You can also disable Replication Factor since data resilience is provided at the application level. These settings will help you achieve low cost per GB for the container.
Click Save to create the container.
Go to Storage > Datastores and click on Create Datastore.
Enter a name for the new datastore, such as Distributed_App_Datastore, and select NFS as the datastore type. Select the container that you just created, Distributed_App_Container, as the source.
Click Save to create the datastore.
The datastore will be automatically mounted on all nodes in the cluster. You can verify this by going to Storage > Datastores and clicking on Distributed_App_Datastore. You should see all nodes listed under Hosts.
You can now create or migrate your worker VMs to this datastore and run them on any node in the cluster. The datastore will provide low cost per GB and high performance for your distributed application.

質問 # 12
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 # 13
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 fil 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 # 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
Syslop 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

質問 # 15
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.

正解：

解説：
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 ncli 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.

質問 # 16
.....

NCM-MCI試験のAPPテストエンジンのような多くの受験者は、非常に強力に思えるので。 このバージョンに興味がある場合は、購入できます。 このバージョンでは、NCM-MCI試験問題集の質問と回答だけでなく、実践と習得が容易な機能も提供します。 携帯電話、iPadなどのブラウザを開くことができる場合にのみ、あらゆる電子製品で使用できます。 常に実際のテストに不安がある場合、またはテストの終了時間を制御できない場合、Nutanix NCM-MCI試験ブレーンダンプのAPPテストエンジンは、時間指定テストを設定し、実際のテストシーンをシミュレートできます。

excelmanindia.com, carrabreconservatoryofmusic.com, main.temploifamosun.com, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

2026年Topexam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=14uTWR8fX1GROn7tV8_zF9b4jr8Vryk5C