

# What are reliable sources for Nutanix NCM-MCI-6.10 certification exam preparation?



You can also set the number of Nutanix NCM-MCI-6.10 dumps questions to attempt in the practice test and time as well. The web-based Nutanix NCM-MCI-6.10 practice test software needs an active internet connection and can be accessed through all major browsers like Chrome, Edge, Firefox, Opera, and Safari. Our Desktop-based Nutanix NCM-MCI-6.10 Practice Exam Software is very suitable for those who don't have an internet connection. You can download and install it within a few minutes on Windows-based PCs only and start preparing for the Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI) exam.

If your budget is limited, but you need complete exam material. Then you can try the ExamCost's Nutanix NCM-MCI-6.10 Exam Training materials. ExamCost can escort you to pass the IT exam. Training materials of ExamCost are currently the most popular materials on the internet. NCM-MCI-6.10 Exam is a milestone in your career. In this competitive world, it is more important than ever. We guarantee that you can pass the exam easily. This certification exam can also help you tap into many new avenues and opportunities. This is really worth the price, the value it creates is far greater than the price.

>> NCM-MCI-6.10 Exam Dumps Provider <<

## Pass Guaranteed 2026 Nutanix Valid NCM-MCI-6.10: Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI) Exam Dumps Provider

It never needs an internet connection. ExamCost's Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI) practice exam software has several mock exams, designed just like the real exam. Nutanix NCM-MCI-6.10 practice exam software contains all the important questions which have a greater chance of appearing in the final exam. ExamCost always tries to ensure that you are provided with the most updated Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI) (NCM-MCI-6.10) Exam Questions to pass the exam on the first attempt.

## Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI) Sample Questions (Q16-Q21):

### NEW QUESTION # 16

Task 2

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.

**Answer:**

Explanation:

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.

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 $i "ls -ltr /home/nutanix/data/logs/*.FATAL"; done
NCC Health Check: cluster_services_down_check (nutanix.com)
Part2 Vlad Drac2023-06-05T13:22:00.86I'll update this one with a smaller, if possible, command
Update the default password for the root user on the node to match the admin user password
echo -e "CHANGING ALL AHV HOST ROOT PASSWORDS.\nPlease input new password: "; read -rs password1; echo "Confirm new password: "; read -rs password2; if [ "$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>

Name

name\_public\_key

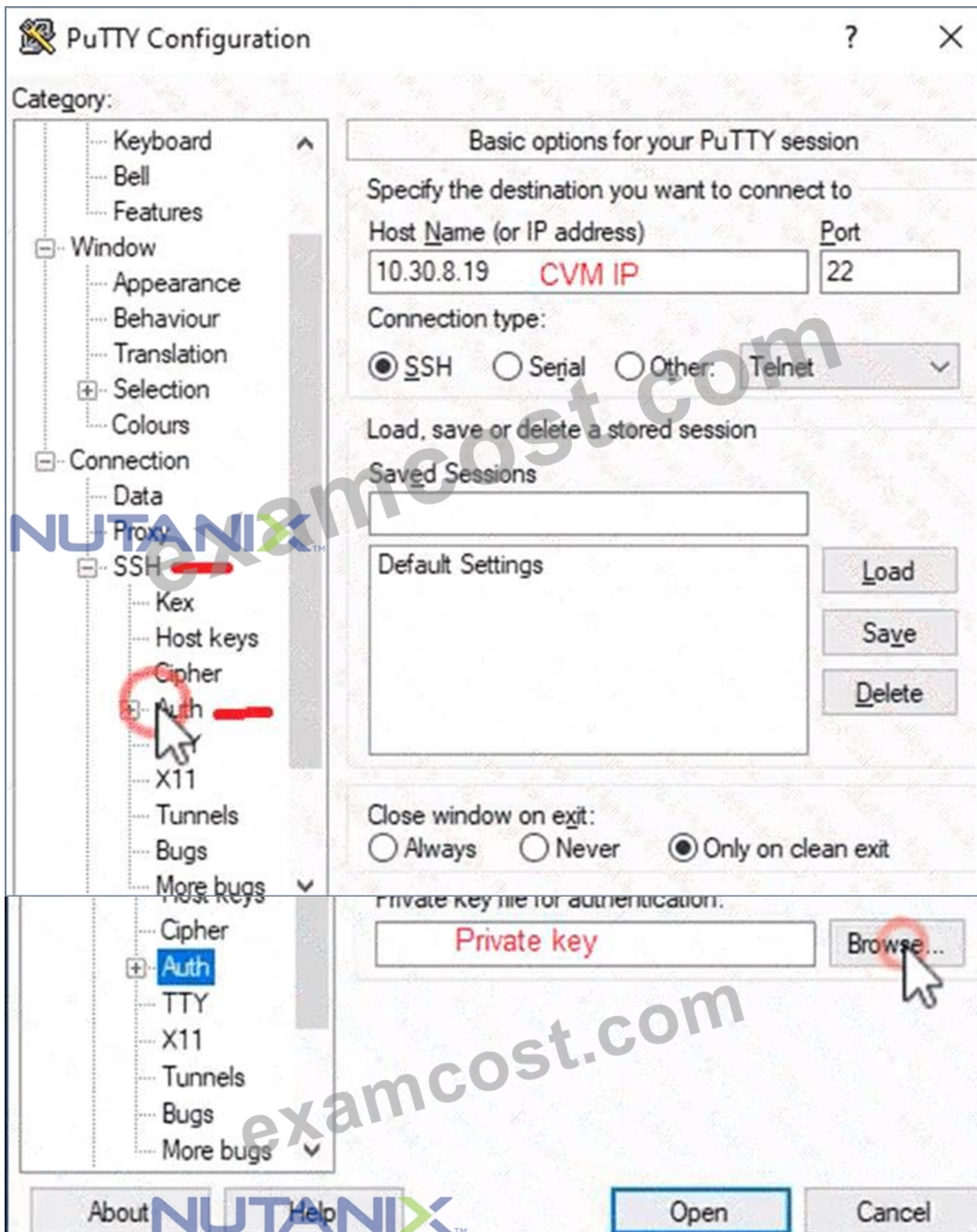
Key

Public Key here

examcost.com

NUTANIX

Back Save

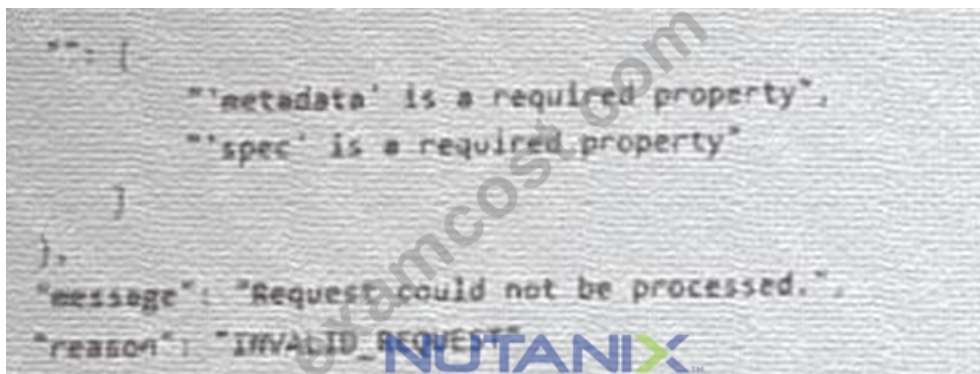


#### NEW QUESTION # 17

Task 16

An administrator is working to create a VM using Nutanix V3 API calls with the following specifications.

\* VM specifications:



- \* vCPUs: 2
- \* Memory: 8Gb
- \* Disk Size: 50Gb
- \* Cluster: Cluster A
- \* Network: default- net

The API call is failing, indicating an issue with the payload:

The body is saved in Desktop/ Files/API\_Create\_VM,text

Correct any issues in the text file that would prevent from creating the VM. Also ensure the VM will be created as speeded and make sure it is saved for re-use using that filename.

Deploy the vm through the API

Note: Do not power on the VM.

### Answer:

Explanation:

See the Explanation for step by step solution.

Explanation:

<https://portal.nutanix.com/page/documents/kbs/details?targetId=kA00e000000LLEzCAO>

<https://jsonformatter.curiousconcept.com/#>

acli net.list (uuid network default\_net)

ncli cluster info (uuid cluster)

Put Call: <https://Prism Central IP address : 9440/api/nutanix/v3vms>

Edit these lines to fix the API call, do not add new lines or copy lines.

You can test using the Prism Element API explorer or PostMan

Body:

```
{
{
"spec": {
"name": "Test_Deploy",
"resources": {
"power_state": "OFF",
"num_vcpus_per_socket":,
"num_sockets": 1,
"memory_size_mib": 8192,
"disk_list": [
{
"disk_size_mib": 51200,
"device_properties": {
"device_type": "DISK"
}
},
{
"device_properties": {
"device_type": "CDROM"
}
}
],
"nic_list": [
{
"nic_type": "NORMAL_NIC",
```

```

"is_connected": true,
"ip_endpoint_list": [
{
"ip_type": "DHCP"
}
],
"subnet_reference": {
"kind": "subnet",
"name": "default_net",
"uuid": "00000000-0000-0000-0000-000000000000"
}
},
"cluster_reference": {
"kind": "cluster",
"name": "NTNXDemo",
"uuid": "00000000-0000-0000-0000-000000000000"
}
},
"api_version": "3.1.0",
"metadata": {
"kind": "vm"
}
}

```

<https://www.nutanix.dev/2019/08/26/post-a-package-building-your-first-nutanix-rest-api-post-request/> Reference

### NEW QUESTION # 18

The Database team is reporting performance degradation for a business-critical application on Saturdays.

The team is requesting monitoring of processor, memory and storage utilization for the cluster for the application: SQL01, SQL02.

The report should contain views for the following:

- \* At the cluster level, only for the Cluster 1: The maximum percentage of CPU used
- \* At the VM level, including any future VM with the prefix SQL: The maximum time taken, maximum percentage of time a VM waits to use the physical CPU, out of the total CPU The report should run on Sundays at 12:00 AM for the previous 7 days. The report should show when completed.

Create a report named SQL\_Batch\_Saturday that meets these requirements.

Generate an instance of the report named SQL\_Batch\_Saturday as a CSV and save the file.

Note: You must name the report SQL\_Batch\_Saturday to receive any credit. Any other name will not be accepted. SMTP is not configured.

### Answer:

Explanation:

See the Explanation below for detailed answer.

Explanation:

Here is the step-by-step solution to create and run the report, performed entirely within Prism Central.

1. Create the Analysis Session

First, we will build the charts and entities for the report using the Analysis tool.

- \* From the Prism Central main menu, navigate to Operations > Analysis.
- \* Click the + New Session button.
- \* Add the required entities:
  - \* In the "Entities" search box, type Cluster 1 and select Cluster: Cluster 1.
  - \* In the "Entities" search box, type SQL01 and select VM: SQL01.
  - \* In the "Entities" search box, type SQL02 and select VM: SQL02.
- \* Click Add Charts > New Chart to add the Cluster CPU chart:
  - \* Title: Cluster 1 Max CPU Usage
  - \* Entity Type: Cluster
  - \* Metric: Cluster CPU Usage %
  - \* Aggregation: Select Maximum
- \* Click Add.



- \* Click Add Charts > New Chart to add the VM CPU Ready Time chart:
  - \* Title: VM Max CPU Ready Time
  - \* Entity Type: VM
  - \* Metric: CPU Ready Time %
  - \* Aggregation: Select Maximum
  - \* Click Add.
2. Save and Configure the Report
- Now, save the session as a report and configure it to dynamically include all VMs with the SQL prefix.
- \* Click the Save as Report icon (the bookmark icon in the upper right).
  - \* Name the report SQL\_Batch\_Saturday and click Save.
  - \* Navigate to Operations > Reports.
  - \* Find the SQL\_Batch\_Saturday report you just created and click its name to open the report editor.
  - \* In the Entities tile, click the Edit (pencil) icon.
  - \* By default, it will list "Cluster 1", "SQL01", and "SQL02".
  - \* Change the VM selection:
  - \* Select the radio button for All VMs prefixed with.
  - \* In the text box, enter SQL.
  - \* Ensure "Cluster 1" is still listed under "Clusters".
  - \* Click Save.
3. Schedule the Report
- \* While still in the report editor for SQL\_Batch\_Saturday, click the Schedule button.
  - \* Configure the schedule:
  - \* Recurrence: Weekly
  - \* Repeat on: Sunday
  - \* Start Time: 12:00 AM
  - \* Time Range: Previous 7 Days
  - \* Configure the notification (as SMTP is not available):
  - \* Expand the Notification Settings section.
  - \* Check the box for Notify when ready (this enables the bell icon notification).
  - \* Ensure "Email Report" is not checked.
  - \* Click Save.
4. Generate and Save the CSV Instance
- Finally, run the report now and download the CSV as requested.
- \* Navigate back to the main Operations > Reports list.
  - \* Select the checkbox next to SQL\_Batch\_Saturday.
  - \* Click the Actions dropdown and select Run Now.
  - \* In the dialog, confirm the time range (e.g., "Last 7 Days") and click Run.
  - \* Click the Report Instances tab.
  - \* Wait for the report instance "SQL\_Batch\_Saturday" to finish running (the status will change from "Running" to Succeeded).
  - \* Once it has succeeded, click the Download (arrow) icon for that instance.
  - \* Select the CSV format.
  - \* Save the file to the desktop.

## NEW QUESTION # 19

### Task 10

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:

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 # 20

Create a VM template on Cluster 1 named Small Template that matches the small VM Configuration in NVD-2031 (see the Files\Documentation 6.10 folder) however, you will use default storage container.

Configure SMTP Alerting and NCC reports per NVD-2031 for Cluster 1.

Settings:

- \* SMTP: Use Cluster 2 IP address
- \* Cluster email: cluster1@ACME.org
- \* Alert emails: primaryalerts@ACME.org, secondaryalerts@ACME.org

#### Answer:

##### Explanation:

See the Explanation below for detailed answer.

##### Explanation:

Here is the step-by-step solution to complete both tasks on Cluster 1.

This solution requires you to first find the IP of Cluster 2 (for the SMTP server) and then perform all configurations within the Prism Element interface for Cluster 1.

Prerequisite: Find Cluster 2 IP

- \* In Prism Central, navigate to Hardware > Clusters.
- \* Find Cluster 2 in the list and note its IP Address. You will use this in the steps below.

Task 1: Create the VM Template

- \* Log in to the Prism Element (PE) interface for Cluster 1. (From PC, go to Hardware > Clusters > click the name "Cluster 1").
- \* Navigate to the VM view from the main dashboard.
- \* Click the + Create VM button.
- \* Fill in the VM details based on the NVD-2031 "Small VM" configuration (e.g., 2 vCPUs, 1 Core per vCPU, 4 GB RAM).

\* Name: Small Template

\* Compute Details:

\* vCPUs: 2

\* Number of Cores per vCPU: 1



- \* Memory: 4 GB
- \* Scroll down to Storage and click + Add New Disk.
- \* Operation: Select Clone from Image Service.
- \* Image: Select any available guest OS image (e.g., a Windows or CentOS image).
- \* Storage Container: Ensure the default container is selected (as required by the task).
- \* Click Add.
- \* Scroll down to Network Adapters (NIC) and click + Add NIC.
- \* Select any available VLAN/Subnet (e.g., Primary).
- \* Click Add.
- \* Click Save. The VM will be created (and remain powered off).
- \* Find the new Small Template VM in the list. Select its checkbox.
- \* Click the Actions dropdown and select Convert to Template.
- \* Confirm the action by clicking OK.

#### Task 2: Configure SMTP and NCC Reports

- \* While still in the Cluster 1 Prism Element interface, click the gear icon (Settings) in the top-right corner.
- \* Select SMTP Server from the left-hand menu.
- \* Click the Configure button.
- \* In the "Server Settings" tab, fill in the following:
  - \* Server Address: Enter the Cluster 2 IP Address (which you found in the prerequisite step).
  - \* Port: 25 (leave as default).
  - \* From Email Address: cluster1@ACME.org
- \* Click Next.
- \* In the "Email Recipients" tab, click + Add Email Recipient.
  - \* Address: primaryalerts@ACME.org
  - \* Ensure all severities (Critical, Warning, Info) are checked.
  - \* Click Save.
  - \* Click + Add Email Recipient again.
  - \* Address: secondaryalerts@ACME.org
  - \* Ensure all severities are checked.
  - \* Click Save.
  - \* Click Done. A test email will be sent.
- \* In the main Settings menu, select Alerts and Notifications.
- \* Scroll to the NCC Health Checks section.
- \* Check the box labeled Email Nutanix Cluster Check reports to recipients. (This will use the SMTP settings and recipients you just configured).
- \* Click Save.

#### NEW QUESTION # 21

.....

We provide three versions to let the clients choose the most suitable equipment on their hands to learn the NCM-MCI-6.10 study materials such as the smart phones, the laptops and the tablet computers. We provide the professional staff to reply your problems about our study materials online in the whole day and the timely and periodical update to the clients. So you will definitely feel it is your fortune to buy our NCM-MCI-6.10 Study Materials.

**Dump NCM-MCI-6.10 Torrent:** <https://www.examcost.com/NCM-MCI-6.10-practice-exam.html>

If you are finding it difficult to choose the best quality NCM-MCI-6.10 exam dumps, then you should consider trying out our demo, (NCM-MCI-6.10 pass review - Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI)) We assure you 100% pass for sure, We are equipped with professionals having vast experience in the NCM-MCI-6.10 practice test; they are a committed team of individuals that make sure that the customers get the latest NCM-MCI-6.10 test questions and NCM-MCI-6.10 test answers, Nutanix NCM-MCI-6.10 Exam Dumps Provider Such an international certification is recognition of your IT skills.

What if you wanted to perform multiple actions and/or dynamically NCM-MCI-6.10 add or subtract a number of actions, Whatever your Linux workplace looks like, it probably sees a fair amount of coming and going.

**Pass Guaranteed High Hit-Rate Nutanix - NCM-MCI-6.10 - Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI) Exam Dumps Provider**

If you are finding it difficult to choose the best quality NCM-MCI-6.10 Exam Dumps, then you should consider trying out our demo, (NCM-MCI-6.10 pass review - Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI)) We assure you 100% pass for sure.

We are equipped with professionals having vast experience in the NCM-MCI-6.10 practice test; they are a committed team of individuals that make sure that the customers get the latest NCM-MCI-6.10 test questions and NCM-MCI-6.10 test answers.

Such an international certification Dump NCM-MCI-6.10 Torrent is recognition of your IT skills, You can pass the exam just one time.

- [illegible]