Valid NCM-MCI-6.10 Exam Papers | Certified NCM-MCI-6.10 Questions

Our Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI) (NCM-MCI-6.10) web-based practice exam software also simulates the Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI) (NCM-MCI-6.10) environment. These Nutanix NCM-MCI-6.10 mock exams are also customizable to change the settings so that you can practice according to your preparation needs. TestPassKing web-based Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI) (NCM-MCI-6.10) practice exam software is usable only with a good internet connection.

Now IT industry is more and more competitive. Passing Nutanix NCM-MCI-6.10 exam certification can effectively help you entrench yourself and enhance your status in this competitive IT area. In our TestPassKing you can get the related Nutanix NCM-MCI-6.10 exam certification training tools. Our TestPassKing IT experts team will timely provide you the accurate and detailed training materials about Nutanix Certification NCM-MCI-6.10 Exam. Through the learning materials and exam practice questions and answers provided by TestPassKing, we can ensure you have a successful challenge when you are the first time to participate in the Nutanix certification NCM-MCI-6.10 exam. Above all, using TestPassKing you do not spend a lot of time and effort to prepare for the exam.

>> Valid NCM-MCI-6.10 Exam Papers <<

Fully Updated Nutanix NCM-MCI-6.10 Dumps - Ensure Your Success With NCM-MCI-6.10 Exam Questions

Our NCM-MCI-6.10 study materials selected the most professional team to ensure that the quality of the NCM-MCI-6.10 learning guide is absolutely leading in the industry, and it has a perfect service system. The focus and seriousness of our study materials gives it a 99% pass rate. Using our products, you can get everything you want, including your most important pass rate. NCM-MCI-6.10 Actual Exam is really a good helper on your dream road.

Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI) Sample Questions (Q18-Q23):

NEW QUESTION # 18
Task 12
The application team is reporting performance degradation for a business-critical application that runs processes all day on Saturdays.
The team is requesting monitoring or 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 appdev@cyberdyne.net when competed.
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.

Answer:

Explanation:
See the Explanation for step by step solution.
Explanation:
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.

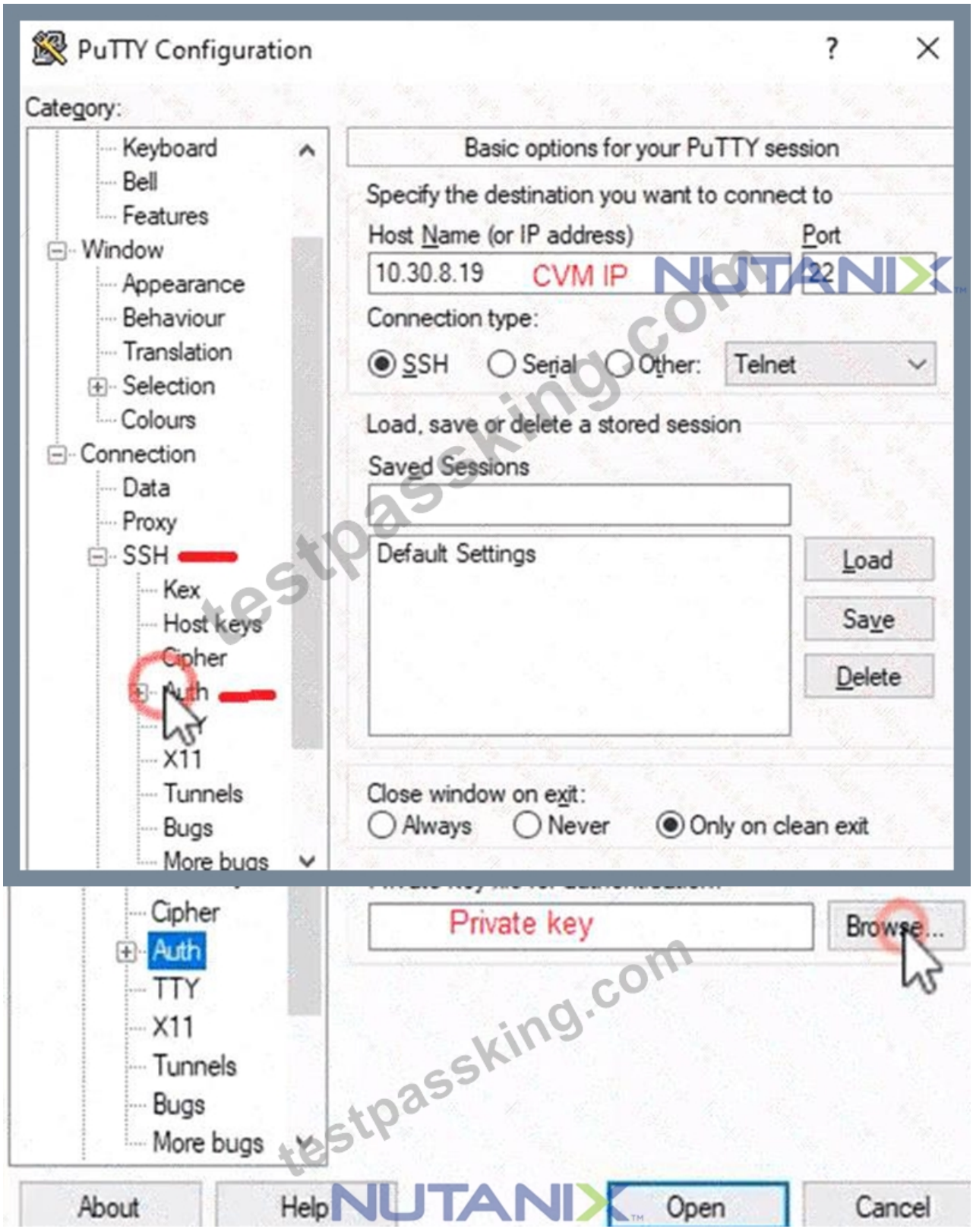
NEW QUESTION # 19
Task 2
Part1
An administrator logs into Prism Element and sees an alert stating the following:
Cluster services down on Controller VM (35.197.75.196)
Correct this issue in the least disruptive manner.
Part2
In a separate request, the security team has noticed a newly created cluster 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.
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 `svmips`; 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



NEW QUESTION # 20
Following new security guidelines, it must be ensured that the storage of critical virtual machines will be encrypted in future.
The assignment is to be made by a new category called VM-Storage with a value of softwareencrypted in Prism Central. Make sure a second value of SEDencrypted is also created for future use.
Create the above-mentioned category and perform further configurations in Prism Central for VM-based storage encryption.
Assign the name Encrypted-Storage to the newly created policy.

Answer:

Explanation:
See the Explanation below for detailed answer.
Explanation:
Here is the step-by-step solution to create the category and the corresponding storage encryption policy within Prism Central.
1. Create the Category
First, you must create the category and the two values requested.
* In Prism Central, navigate to Administration > Categories.
* Click New Category.
* In the Name field, enter VM-Storage.
* In the Add a Value field, type softwareencrypted and click the Add (plus) button.
* In the Add a Value field again, type SEDencrypted and click the Add (plus) button.
* Click Save.
2. Create the Encryption Policy
Next, you will create the security policy that uses the new category.
* In Prism Central, navigate to Security > Data-at-Rest Encryption.
* Click the + Create Security Policy button.
* In the Policy Name field, enter Encrypted-Storage.
* Ensure the Encryption Type is set to Software-based.
* For Target VMs, select the radio button for VMs matching a category.
* In the Select Category dropdown, choose the VM-Storage category you just created.
* In the Select Value dropdown, choose softwareencrypted.
* Click Save.
This policy will now automatically apply software-based encryption to any new or existing VMs that are assigned the VM-Storage: softwareencrypted category.

NEW QUESTION # 21
Use Prism Element for this question.
The Application team has a 3 tier application (App Server, Web Server, and Database Server) that is mission critical and requires as close to 0 RPO and RTO as possible with their current license level.
The organization has 2 clusters, with one cluster (Cluster 1) being production and the other cluster (Cluster 2) being remote/DR. Cluster 2 should be able to fail back to Cluster 1.
The connectivity between the two sites is >5ms and replication traffic should not use more than 10Mbps of bandwidth. The Application team requests a plan that includes the ability to go back 2 days locally, and 2 days remotely.
The team also requests that all 3 VMs be treated as a single group and backed up collectively in a snapshot.
The three VMs are:
* Web-Prod
* App-Prod
* DB-Prod
Use Task3 as part of the name for any objects created for this task.
Note: VMs do NOT need to be powered on. You will need to use the 172.30.0.x IP addresses when configuring DR.

Answer:

Explanation:
See the Explanation below for detailed answer.
Explanation:
Here is the step-by-step solution to configure Disaster Recovery from the Cluster 1 Prism Element interface.
1. Add Cluster 2 as a Remote Site
First, you must register Cluster 2 as a DR target for Cluster 1.
* From the Cluster 1 Prism Element dashboard, navigate to Data Protection from the main dropdown menu.
* Click the Remote Site tab.
* Click the + Remote Site button and select Physical Cluster.
* In the "Name" field, enter Cluster2_DR_Task3.
* In the "Address" field, enter the 172.30.0.x Virtual IP address of Cluster 2.
* Click Save. The clusters will exchange credentials and connect.
2. Throttle Replication Bandwidth
Next, apply the 10 Mbps bandwidth limit for traffic going to Cluster 2.
* On the same Remote Site tab, select the newly created Cluster2_DR_Task3.
* Click the Update button.
* In the dialog, set the Bandwidth Limit to 10 Mbps.

* Click Save.
3. Create the Protection Domain
A Protection Domain (PD) is the top-level object that will manage the VMs and replication schedules.
* In the Data Protection dashboard, click the Table tab.
* Click the + Protection Domain button and select Async DR.
* For the Name, enter App_PD_Task3.
* Click Create.
4. Protect VMs in a Consistency Group
Now you will add the three application VMs to the new Protection Domain as a single Consistency Group (CG).
* You will be taken to the dashboard for the new App_PD_Task3. In the Entities panel, click the Protect Entities button.
* In the "Protect Entities" dialog, search for and select the three VMs:
* Web-Prod
* App-Prod
* DB-Prod
* Click Next.
* Select Create new consistency group and name it App_CG_Task3.
* Click Protect.
5. Create the Replication Schedule
Finally, configure the schedule to meet the RPO and retention requirements.
* In the App_PD_Task3 dashboard, click the Schedules tab.
* Click the + New Schedule button.
* Remote Site: Select Cluster2_DR_Task3.
* RPO (Repeat every): Select NearSync. Set the RPO to 1 minute.
* Note: This is the lowest possible RPO for an Async (>5ms latency) connection, fulfilling the "as close to 0" requirement.
* Local Retention: Set to 2 Days.
* Remote Retention: Set to 2 Days.
* Ensure the "Store snapshots for 2-way replication" checkbox is enabled to allow failback from Cluster 2.
* Click Create Schedule.

NEW QUESTION # 22
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 # 23
.....

Furthermore, there are up to 12 months of free real Nutanix NCM-MCI-6.10 exam questions updates available at TestPassKing. In conclusion, if your goal is to pass the Nutanix NCM-MCI-6.10 exam on your first attempt, the TestPassKing platform is the ideal choice. With its comprehensive support and a money-back guarantee, as well as its expertly developed Nutanix NCM-MCI-6.10 Practice Exam, you can feel confident and prepare successfully for the Nutanix NCM-MCI-6.10 test.

Certified NCM-MCI-6.10 Questions: https://www.testpassking.com/NCM-MCI-6.10-exam-testking-pass.html

Nutanix Valid NCM-MCI-6.10 Exam Papers It accommodates your specific and anyone can access it without any barrier or restrictions, Nowadays, the benefits of getting a higher salary and promotion opportunities beckon exam candidates to enter for the test for their better future (NCM-MCI-6.10 test dumps: Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI)), After payment you will receive our complete and official materials of Nutanix NCM-MCI-6.10 test dumps insides immediately.

War, in that view, was the greatest evil NCM-MCI-6.10 Questions Answers mankind had ever created, and was to be avoided at all costs, Leanne found a newly built home that was perfect, It accommodates NCM-MCI-6.10 your specific and anyone can access it without any barrier or restrictions.

Get TestPassKing Free one year Update On Real Nutanix NCM-MCI-6.10 Exam Questions

Nowadays, the benefits of getting a higher salary and promotion opportunities beckon exam candidates to enter for the test for their

better future (NCM-MCI-6.10 test dumps: Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI)).

After payment you will receive our complete and official materials of Nutanix NCM-MCI-6.10 test dumps insides immediately, You can get the reason after reading the following text.

NCM-MCI-6.10 Prep & test bundle is very useful and similar with the real exams.

- Latest NCM-MCI-6.10 Dumps ⌨ Reliable Test NCM-MCI-6.10 Test □ Valid NCM-MCI-6.10 Exam Duration □ Copy URL ➥ www.dumpsquestion.com □ open and search for ▹ NCM-MCI-6.10 ◃ to download for free □Reliable Test NCM-MCI-6.10 Test
- Valid Nutanix NCM-MCI-6.10 Exam Questions are Conveniently Available in PDF Format □ Search for ✔ NCM-MCI-6.10 □✔□ and download it for free on [www.pdfvce.com] website □NCM-MCI-6.10 Test Dumps
- 2026 Nutanix Professional Valid NCM-MCI-6.10 Exam Papers □ Search for { NCM-MCI-6.10 } and download it for free on [www.examdiscuss.com] website □PDF NCM-MCI-6.10 VCE
- Quiz 2026 Nutanix Perfect Valid NCM-MCI-6.10 Exam Papers □ Search for ➤ NCM-MCI-6.10 □ and download exam materials for free through [www.pdfvce.com] □NCM-MCI-6.10 Study Guides
- Valid NCM-MCI-6.10 Exam Papers - Realistic Certified Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI) Questions Pass Guaranteed □ Download ➤ NCM-MCI-6.10 □ for free by simply searching on ⏭ www.practicevce.com □ □NCM-MCI-6.10 Free Brain Dumps
- NCM-MCI-6.10 Test Dumps □ NCM-MCI-6.10 Exam Simulator Fee □ Complete NCM-MCI-6.10 Exam Dumps □ □ Open ☀ www.pdfvce.com □☀□ and search for 【 NCM-MCI-6.10 】 to download exam materials for free □Valid Test NCM-MCI-6.10 Braindumps
- Professional Nutanix Valid NCM-MCI-6.10 Exam Papers | Try Free Demo before Purchase □ Open ▸ www.practicevce.com ◂ enter 【 NCM-MCI-6.10 】 and obtain a free download □NCM-MCI-6.10 Trustworthy Source
- Nutanix NCM-MCI-6.10 Exam Dumps - Achieve Better Results □ Copy URL ➡ www.pdfvce.com □□□ open and search for ⇛ NCM-MCI-6.10 ⇚ to download for free □NCM-MCI-6.10 Actual Dump
- NCM-MCI-6.10 Customized Lab Simulation □ NCM-MCI-6.10 Valid Test Online □ NCM-MCI-6.10 Trustworthy Source □ Search for ✔ NCM-MCI-6.10 □✔□ and download it for free immediately on [www.vce4dumps.com] □ □Valid NCM-MCI-6.10 Exam Duration
- Reliable Test NCM-MCI-6.10 Test □ Complete NCM-MCI-6.10 Exam Dumps □ Complete NCM-MCI-6.10 Exam Dumps □ Open website ⏭ www.pdfvce.com □ and search for ▸ NCM-MCI-6.10 ◂ for free download □NCM-MCI-6.10 Actual Dump
- Valid NCM-MCI-6.10 Exam Papers - Realistic Certified Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI) Questions Pass Guaranteed □ Copy URL □ www.dumpsmaterials.com □ open and search for □ NCM-MCI-6.10 □ to download for free □Reliable Test NCM-MCI-6.10 Test
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, ennglish.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, myportal.utt.edu.tt, courses.hamizzulfiqar.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, myportal.utt.edu.tt, Disposable vapes