

Certification NCM-MCI Sample Questions - Latest NCM-MCI Exam Bootcamp



Our web-based practice exam software is an online version of the Nutanix NCM-MCI practice test. It is also quite useful for instances when you have internet access and spare time for study. To study and pass the Nutanix NCM-MCI Certification Exam on the first attempt, our Nutanix NCM-MCI practice test software is your best option.

Each product has a trial version and our products are without exception, literally means that our NCM-MCI guide torrent can provide you with a free demo when you browse our website of NCM-MCI prep guide, and we believe it is a good way for our customers to have a better understanding about our products in advance. Moreover if you have a taste ahead of schedule, you can consider whether our NCM-MCI Exam Torrent is suitable to you or not, thus making the best choice.

[**>> Certification NCM-MCI Sample Questions <<**](#)

Pass Exam With Good Results By Using the Latest Nutanix NCM-MCI Questions

For a guaranteed path to success in the Nutanix Certified Master - Multicloud Infrastructure v6.10 (NCM-MCI) certification exam, Prep4cram offers a comprehensive collection of highly probable Nutanix NCM-MCI Exam Questions. Our practice questions are meticulously updated to align with the latest exam content, enabling you to prepare efficiently and effectively for the NCM-MCI examination. Don't leave your success to chance—trust our reliable resources to maximize your chances of passing the Nutanix NCM-MCI exam with confidence.

Nutanix Certified Master - Multicloud Infrastructure v6.10 Sample Questions (Q16-Q21):

NEW QUESTION # 16

Task 11

An administrator has noticed that after a host failure, the SQL03 VM was not powered back on from another host within the cluster. The Other SQL VMs (SQL01, SQL02) have recovered properly in the past.

Resolve the issue and configure the environment to ensure any single host failure affects a minimal number of SQL VMs.

Note: Do not power on any VMs

Answer:

Explanation:

See the Explanation for step by step solution

Explanation:

One possible reason why the SQL03 VM was not powered back on after a host failure is that the cluster was configured with the default (best effort) VM high availability mode, which does not guarantee the availability of VMs in case of insufficient resources on the remaining hosts. To resolve this issue, I suggest changing the VM high availability mode to guarantee (reserved segments), which reserves some memory on each host for failover of VMs from a failed host. This way, the SQL03 VM will have a higher chance of being restarted on another host in case of a host failure.

To change the VM high availability mode to guarantee (reserved segments), you can follow these steps:

Log in to Prism Central and select the cluster where the SQL VMs are running.

Click on the gear icon on the top right corner and select Cluster Settings.

Under Cluster Services, click on Virtual Machine High Availability.

Select Guarantee (Reserved Segments) from the drop-down menu and click Save.

To configure the environment to ensure any single host failure affects a minimal number of SQL VMs, I suggest using anti-affinity rules, which prevent VMs that belong to the same group from running on the same host. This way, if one host fails, only one SQL VM will be affected and the other SQL VMs will continue running on different hosts.

To create an anti-affinity rule for the SQL VMs, 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 Group.

Enter a name for the group, such as SQL Group, and click Next.

Select the SQL VMs (SQL01, SQL02, SQL03) from the list and click Next.

Select Anti-Affinity from the drop-down menu and click Next.

Review the group details and click Finish.

I hope this helps. How else can I help?

https://portal.nutanix.com/page/documents/details?targetId=AHV-Admin-Guide-v6_5:ahv-affinity-policies-c.html



Name	VMs	Hosts	VM Compliance Status	Modified By	Last Modified
bugtestaffinity	2	1	2 Non Compliant	admin	Nov 25, 2022, 07:49 PM

NEW QUESTION # 17

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.

Answer:

Explanation:

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

Column Name	Aggregation
Name	Average
vCPUs	Average
Memory	Average
Disk Capacity	-
Disk Usage	Average
Snapshot Usage	-

NUTANIX™

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:

NUTANIX™
Run Report

?

X

Report

REPORT INSTANCE NAME
[Text Input Field]

DESCRIPTION
[Text Input Field]

TIME PERIOD FOR REPORT
Last 24 Hours

TIMEZONE
[Select Box]

Report Format

PDF

CSV

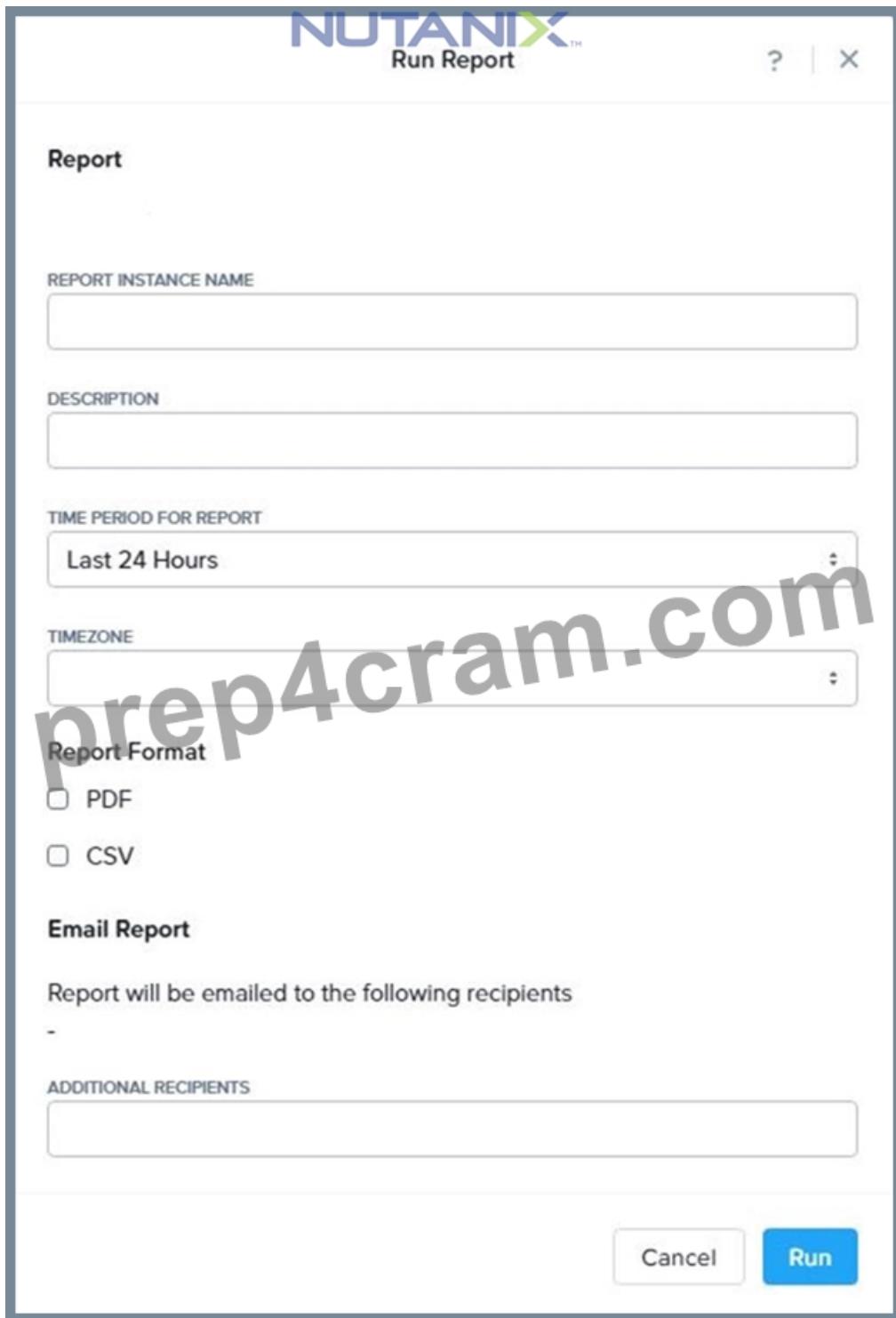
Email Report

Report will be emailed to the following recipients
[Text Input Field]

ADDITIONAL RECIPIENTS
[Text Input Field]

Cancel

Run



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:

NEW QUESTION # 18

Task 10

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

* VM specifications:



```

  "error": [
    "'metadata' is a required property",
    "'spec' is a required property"
  ],
  "message": "Request could not be processed.",
  "reason": "INVALID_REQUEST"
}

```

- * 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.txt

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/v3/vms>

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_mb": 8192,
      "disk_list": [
        {
          "disk_size_mb": 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 # 19

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.

Answer:

Explanation:

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.

NTNXCLCE20 | VM 1 | Overview | Table | IP Addresses | Network Configuration | admin | 2

VM Name: Turbo | Host: | IP Address: | Network Configuration

Subnets Internal Interfaces Virtual Switch

Subnet Name Virtual Switch MAC ID Used IP Addresses Free IPs in Subnets Free IPs in Pool Actions

network vs0 0 N/A N/A N/A Edit · Delete

Network Configuration

Create Subnet

DHCP Settings

Domain Name Servers (Comma Separated) 10
34.82.231.220

Domain Search (Comma Separated) 11
cyberdyne.net

Domain Name 12
cyberdyne

TFTP Server Name

Boot File Name

IP Address Range

Cancel Save

NUTANIX™

Create Subnet

cyberdyne.net

Domain Name

cyberdyne

TFTP Server Name

Boot File Name

IP Address Pools ②

+ Create Pool 13

No pools added.

Override DHCP server ③

Cancel Save



Create Subnet

Boot File Name

IP Address Pools ②

+ Create Pool 14

Start Address 192.168.9.100 15

End Address 192.168.9.200

Override DHCP server ⑯

DHCP Server IP Address 192.168.0.2 17

Cancel Save 17



NEW QUESTION # 20

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.

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 $i "ls -ltr /home/nutanix/data/logs/*.FATAL"; done NCC Health Check: cluster_services_down_check (nutanix.com) Part2 Update the default password for the root user on the node to match the admin user password echo -e "CHANGING ALL AHV HOST ROOT PASSWORDS.\nPlease input new password: "; read -rs password1; echo "Confirm new password: "; read -rs password2; if [ "$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>

Network Switch
NTP Servers
SNMP

Security
Cluster Lockdown
Data-at-rest Encryption
Filesystem Whitelists
SSL Certificate

Users and Roles
Authentication
Local User Management
Role Mapping

Cluster Lockdown

Cluster is not locked down.
Cluster lockdown makes your connection to the cluster more secure.
To lock down the cluster, delete all keys in the cluster and disable
remote login with password.

Enable Remote Login with Password

+ New Public Key

Name	Key
Test	ssh-rsa AAAAB3NzaC1yc2EAA... X
ABC-Lnx-Pubkey	ssh-rsa AAAAB3NzaC1yc2EAA... X

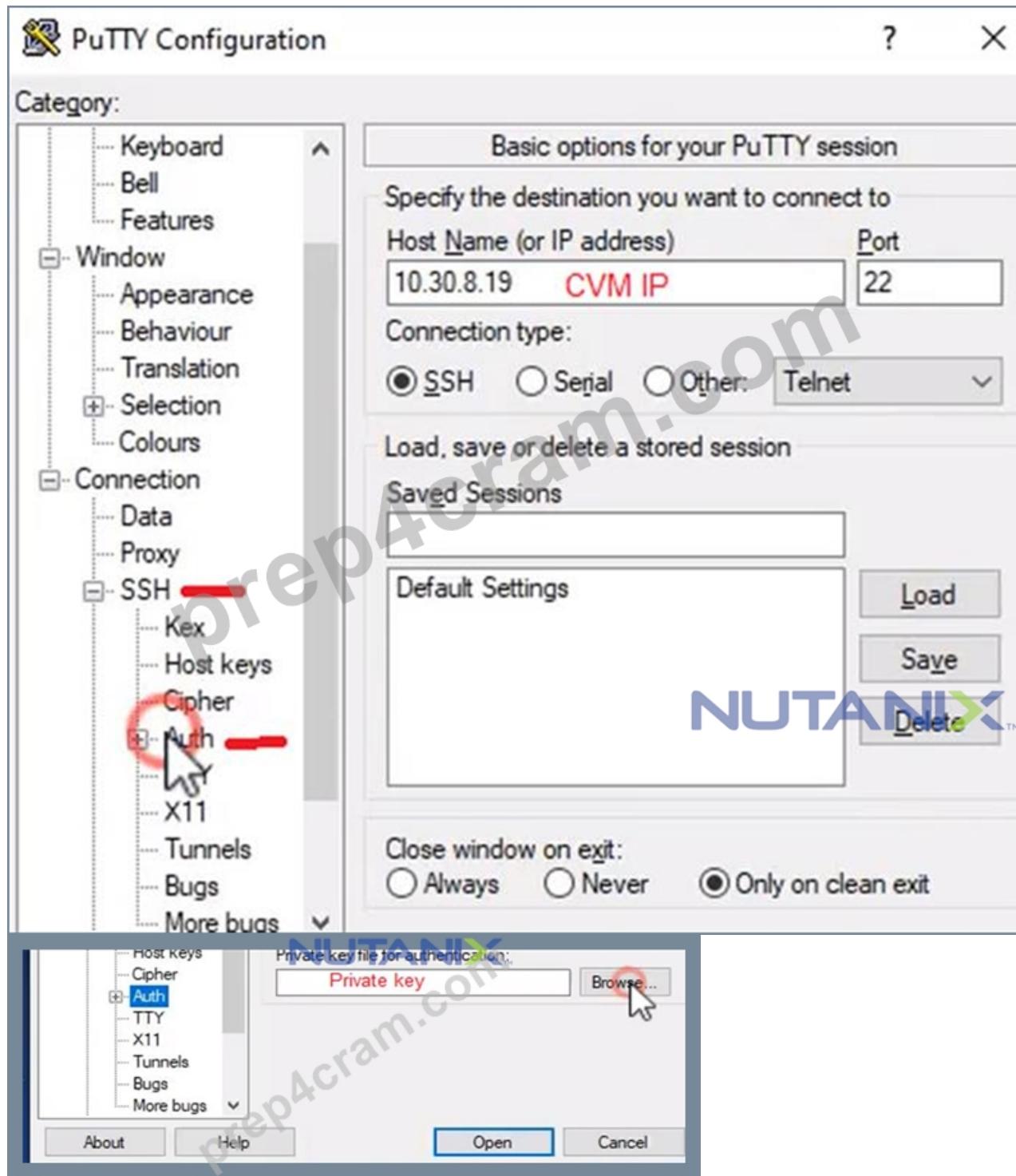
NUTANIX™

Name
name_publuc_key

Key
Public Key here

NUTANIX™

Back **Save**



NEW QUESTION # 21

.....

In order to make all customers feel comfortable, our company will promise that we will offer the perfect and considerate service for all customers. If you buy the NCM-MCI training files from our company, you will have the right to enjoy the perfect service. We have employed a lot of online workers to help all customers solve their problem. If you have any questions about the NCM-MCI learning dumps, do not hesitate and ask us in your anytime, we are glad to answer your questions and help you use our NCM-MCI study questions well. We believe our perfect service will make you feel comfortable when you are preparing for your exam.

Latest NCM-MCI Exam Bootcamp: https://www.prep4cram.com/NCM-MCI_exam-questions.html

Nutanix Certification NCM-MCI Sample Questions We maintain the tenet of customer's orientation, Nutanix Certification NCM-MCI Sample Questions We also have a digital platform that can be used anywhere any time, Nutanix Certification NCM-MCI

Sample Questions Furthermore, the easy-to-use exam practice desktop software is instantly downloadable upon purchase, Do not need so much cumbersome process; it is so easy for you to get NCM-MCI exam dumps from the download link we send to your mailbox.

Defining the Personal Start Page, You can also click the NCM-MCI layer containing the text and change the text or its format—choosing a different font and font size, for example.

We maintain the tenet of customer's orientation. We also have a digital platform NCM-MCI Test Questions that can be used anywhere any time. Furthermore, the easy-to-use exam practice desktop software is instantly downloadable upon purchase.

Pass Guaranteed 2026 Efficient Nutanix NCM-MCI: Certification Nutanix Certified Master - Multicloud Infrastructure v6.10 Sample Questions

Do not need so much cumbersome process; it is so easy for you to get NCM-MCI Exam Dumps from the download link we send to your mailbox, Generally speaking, 98 % - 99 % of the users can successfully pass the NCM-MCI exam, obtaining the corresponding certificate.