

IT 认证电子书



质 量 更 高 服 务 更 好

半年免费升级服务

<http://www.itrenzheng.com>

Exam : NCM-MCI-6.5

Title : Nutanix Certified Master -
Multicloud Infrastructure
(NCM-MCI)v6.5

Version : DEMO

1. 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 toggged 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

Task4

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:

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

2.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.

See the Explanation for step by step solution.

Answer:

To configure the cluster to meet the requirements for the new workload, you need to do the following steps:

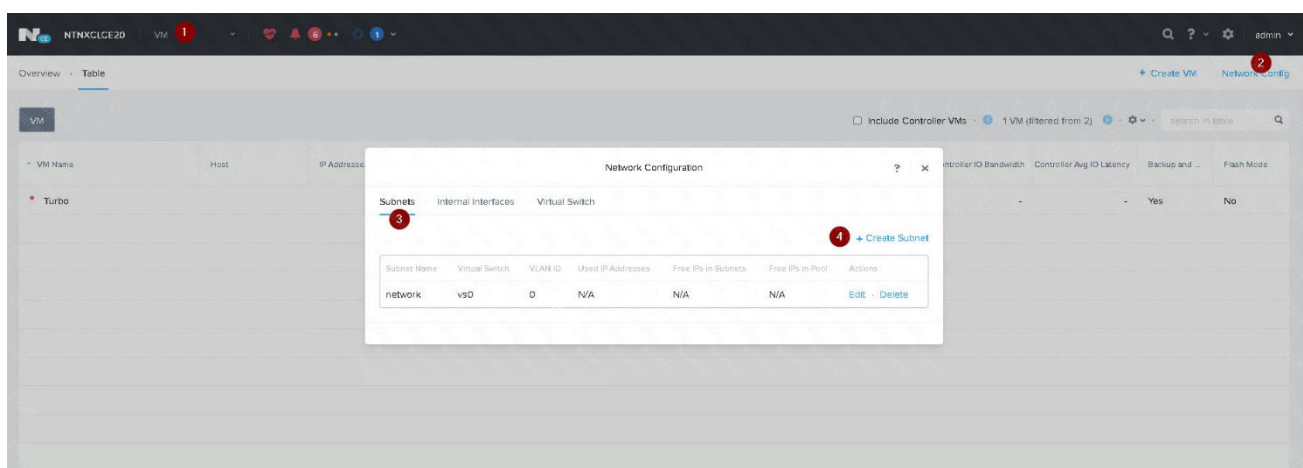
Create a new VLAN with ID 667 on the cluster. You can do this by logging in to Prism Element and going to Network Configuration > VLANs > Create VLAN. Enter 667 as the VLAN ID and a name for the VLAN, such as 667_VLAN.

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.



Create Subnet

Subnet Name: 667_Subnet (5)

Virtual Switch: vs0 (6)

VLAN ID: 667 (7)

Enable IP address management
This gives AHV control of IP address assignments within the network.

Network IP Prefix: 192.168.0.0 (8)

Gateway IP Address: 192.168.0.1 (9)

Buttons: Cancel, Save

Create Subnet

DHCP Settings

Domain Name Servers (Comma Separated): 34.82.231.220 (10)

Domain Search (Comma Separated): cyberdyne.net (11)

Domain Name: cyberdyne (12)

TFTP Server Name: [Empty]

Boot File Name: [Empty]

IP Address Pools: [Empty]

Buttons: Cancel, Save

Create Subnet ? x

cyberdyne.net

Domain Name

cyberdyne

TFTP Server Name

Boot File Name

IP Address Pools ?

+ Create Pool **13**

No pools added.

Override DHCP server ?

Cancel Save

Create Subnet ? x

Boot File Name

IP Address Pools ?

+ Create Pool

Start Address	End Address
192.168.9.100 14	192.168.9.200

Override DHCP server ? **15**

DHCP Server IP Address

192.168.0.2 **16**

Cancel Save **17**

3.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.

See the Explanation for step by step solution.

Answer:

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 data. 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.

4.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.

See the Explanation for step by step solution.

Answer:

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 Drac 2023-06-05T13:22:00I'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>

The screenshot shows a management console interface. On the left is a navigation menu with categories: Network Switch, NTP Servers, SNMP, Security (with 'Cluster Lockdown' selected), Data-at-rest Encryption, Filesystem Whitelists, SSL Certificate, Users and Roles, Authentication, Local User Management, and Role Mapping. The main content area is titled 'Cluster Lockdown' and contains the following information:

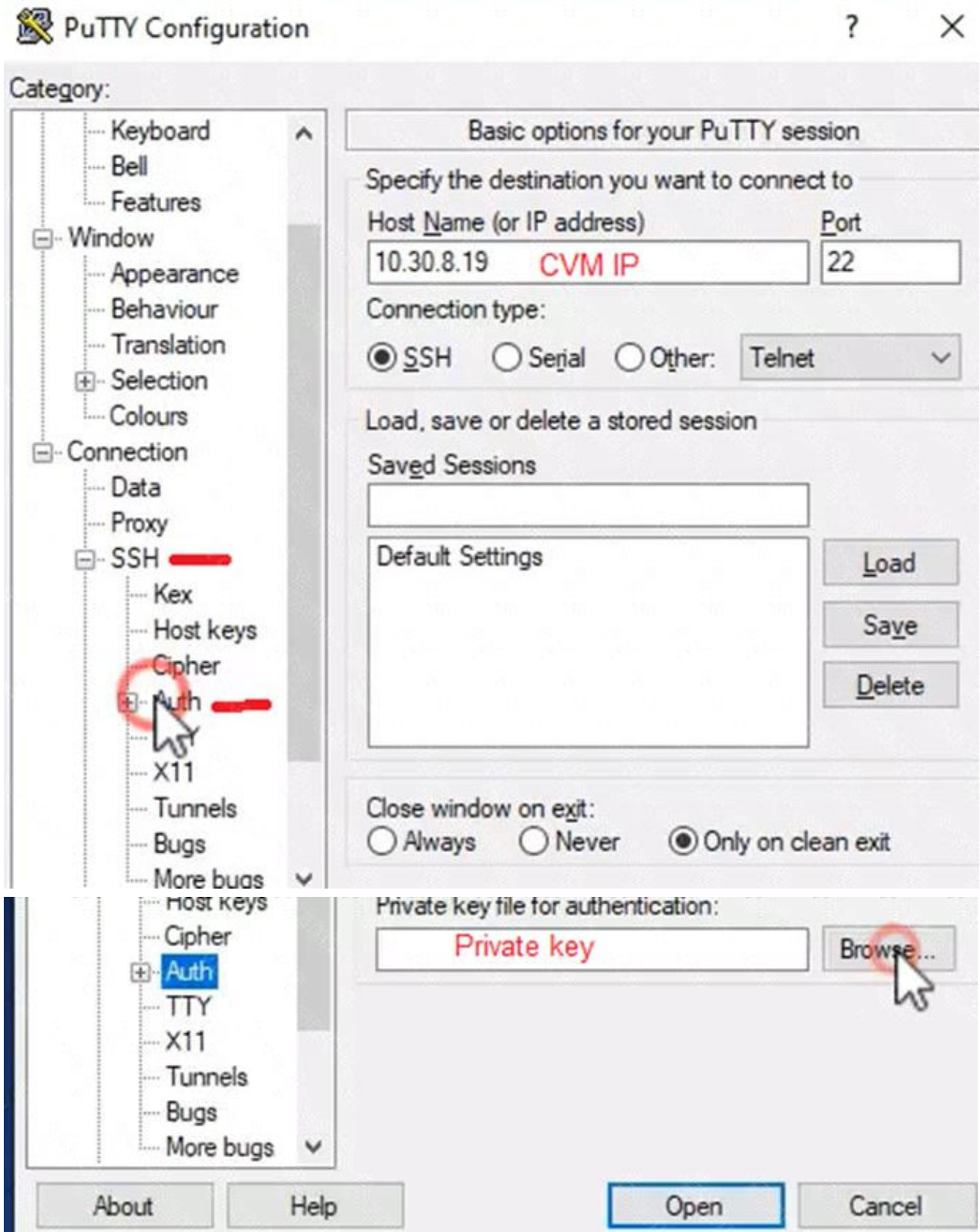
- A lock icon and the text: "Cluster is not locked down."
- Text: "Cluster lockdown makes your connection to the cluster more secure. To lock down the cluster, delete all keys in the cluster and disable remote login with password."
- An unchecked checkbox: "Enable Remote Login with Password"
- A button: "+ New Public Key"
- A table with two columns: "Name" and "Key".

Name	Key
Test	ssh-rsa AAAAB3NzaCtyc2EAA... x
ABC-Lnx-Pubkey	ssh-rsa AAAAB3NzaCtyc2EAA... x

The screenshot shows a form for adding a new public key. It has two main input fields:

- Name:** A text input field containing "name_public_key".
- Key:** A large text area containing the placeholder text "Public Key here".

At the bottom of the form, there are two buttons: a "Back" button with a left-pointing arrow and a blue "Save" button.



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

Answer:

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

Columns

FOCUS

Custom Columns

Custom ⌵

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

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:

Run Report



Report

REPORT INSTANCE NAME

DESCRIPTION

TIME PERIOD FOR REPORT

Last 24 Hours



TIMEZONE

Report Format

PDF

CSV

Email Report

Report will be emailed to the following recipients

-

ADDITIONAL RECIPIENTS

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: