NCM-MCI-6.5 Q&As

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

Pass NCM-MCI-6.5 Exam with 100% Guarantee

QUESTION 1

CORRECT TEXT Task 14 The application team has requested several mission-critical VMs to be configured for disaster recovery. The remote site (when added) will not be managed by Prism Central. As such, this solution should be built using the Web Console.

Disaster Recovery requirements per VM: Mkt01 RPO: 2 hours Retention: 5 snapshots Fin01 RPO: 15 minutes Retention: 7 days Dev01 RPO: 1 day Retention: 2 snapshots Configure a DR solution that meets the stated requirements. Any objects created in this item must start with the name of the VM being protected. Note: the remote site will be added later

A. Answer: See the for step by step solution.

Correct Answer: A

To configure a DR solution that meets the stated requirements, you can follow these steps:

Log in to the Web Console of the source cluster where the VMs are running. Click on Protection Domains on the left menu and click on Create Protection Domain. Enter a name for the protection domain, such as PD_Mkt01, and a description

if required.

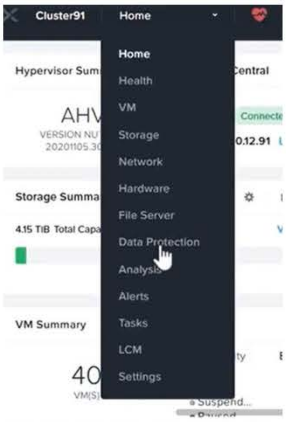
Click Next.

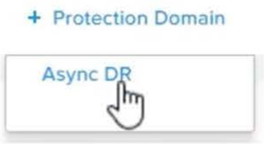
Select Mkt01 from the list of VMs and click Next. Select Schedule Based from the drop-down menu and enter 2 hours as the interval. Click Next.

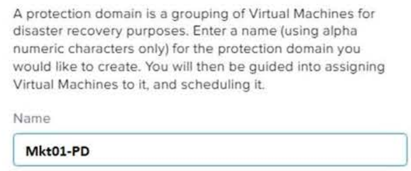
Select Remote Site from the drop-down menu and choose the remote site where you want to replicate the VM. Click Next.

Enter 5 as the number of snapshots to retain on both local and remote sites. Click Next. Review the protection domain details and click Finish. Repeat the same steps for Fin01 and Dev01, using PD_Fin01 and PD_Dev01 as the protection

domain names, and adjusting the interval and retention values according to the requirements.



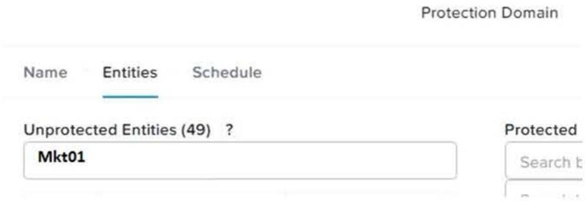




A protection domain is a grouping of Virtual Machines for disaster recovery purposes. Enter a name (using alpha numeric characters only) for the protection domain you would like to create. You will then be guided into assigning Virtual Machines to it, and scheduling it.

Name

Mkt01-PD



Protection Domain

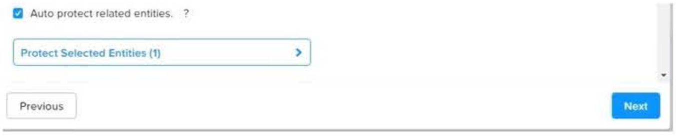
Name Entities Schedule

Unprotected Entities (49) ?

Mkt01

Protected

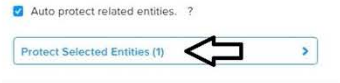
Search b



☑ Auto protect related entities. ?

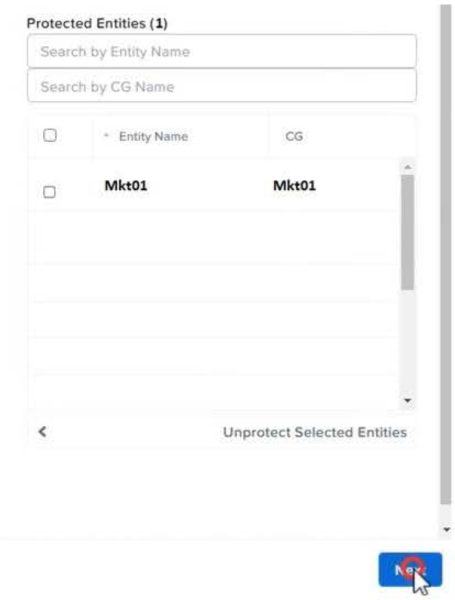
Protect Selected Entities (1) >

Previous Next



☑ Auto protect related entities. ?

Protect Selected Entities (1) >

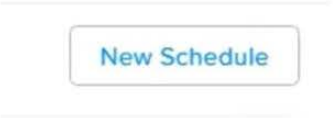


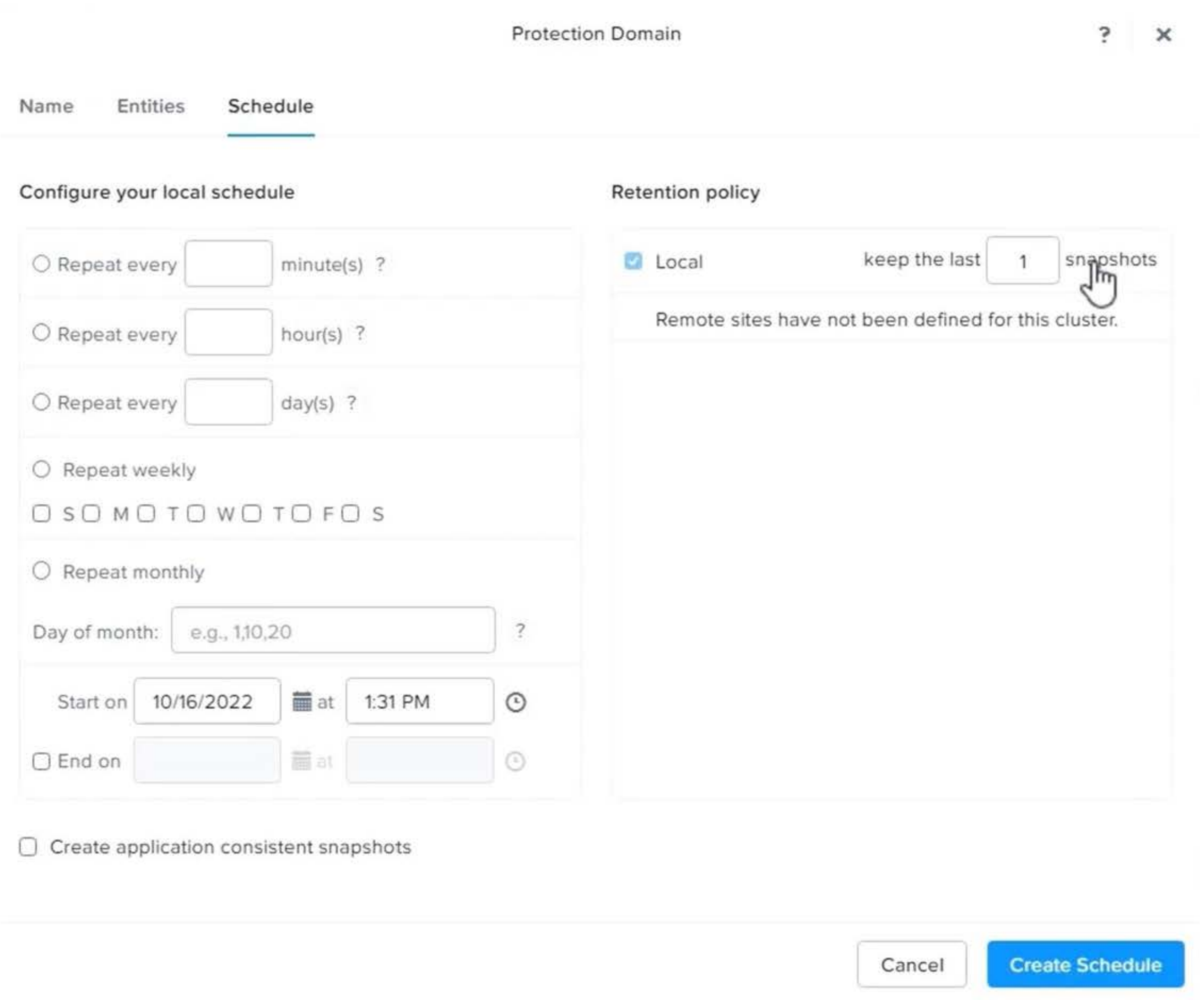
Protected Entities (1)

Search by Entity Name

Search by CG Name

□	Entity Name	CG
□	Mkt01	Mkt01





Protection Domain ? ×

Name | Entities | Schedule

Configure your local schedule

○ Repeat every [ ] minute(s) ?

○ Repeat every [ ] hour(s) ?

○ Repeat every [ ] day(s) ?

○ Repeat weekly

□ S □ M □ T □ W □ T □ F □ S

○ Repeat monthly

Day of month: e.g., 1,10,20 ?

Start on 10/16/2022 at 1:31 PM

□ End on at

Retention policy

☑ Local keep the last 1 snapshots

Remote sites have not been defined for this cluster.

□ Create application consistent snapshots

QUESTION 2

CORRECT TEXT

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 thedefaultpassword.

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.

A. Answer: See the for step by step solution.

Correct Answer: A

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= enable-maintenance-mode=false
```

You can determine the host ID by usingncli host ls. See the troubleshooting topics related to failed cluster services in the Advanced Administration Guide available from the Nutanix Portal\\'sSoftware Documentationpage. (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 Drac2023-06-05T13:22:00I\\'ll update this one with a smaller, if possible, command Update the default password for the rootuser 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:

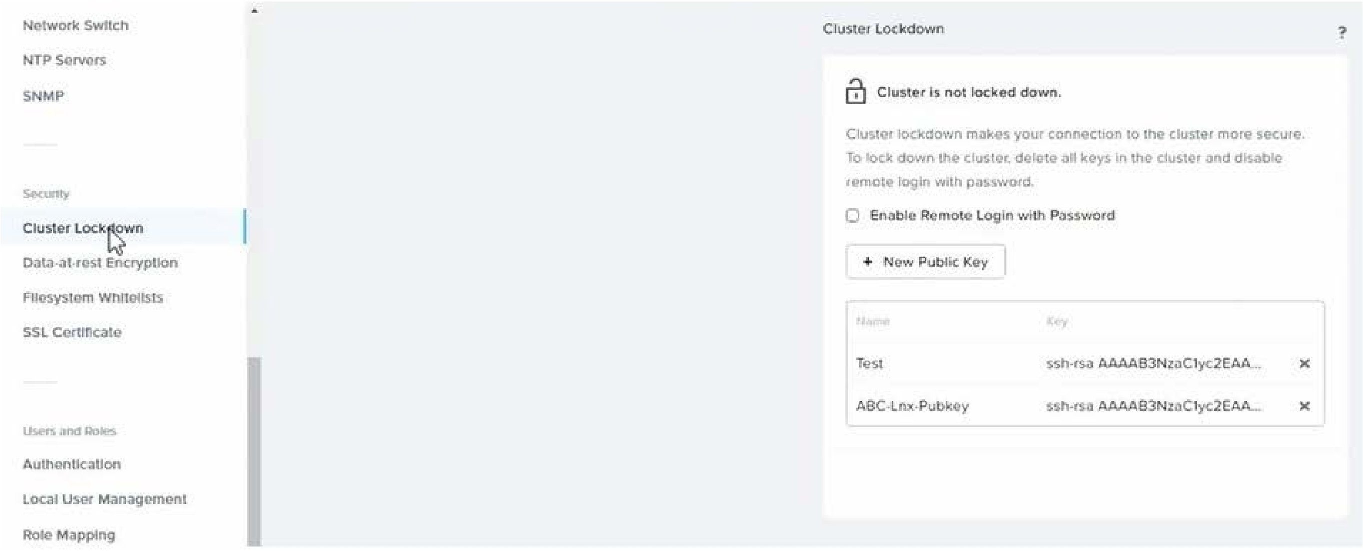
```
nutanix@NTNX-372a19a3-A-CVM:10.35.150.184:~$ ncli cluster get-hypervisor-security- config

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



Cluster Lockdown

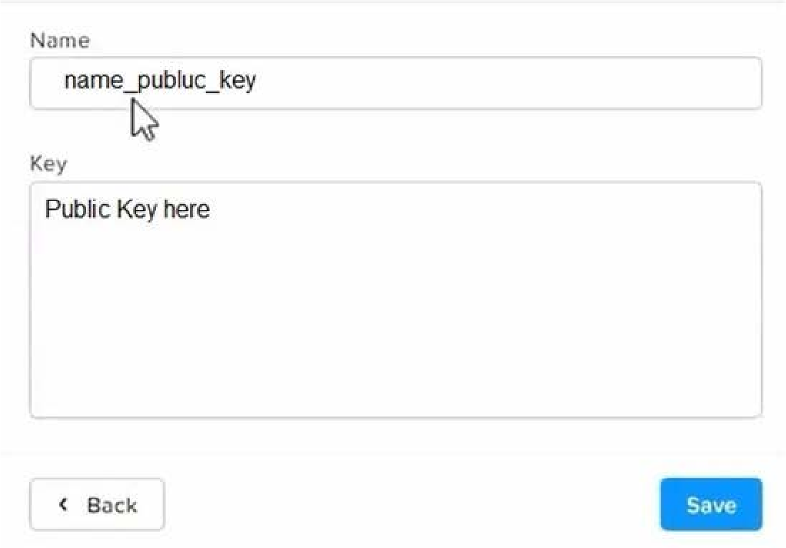
Cluster is not locked down.

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

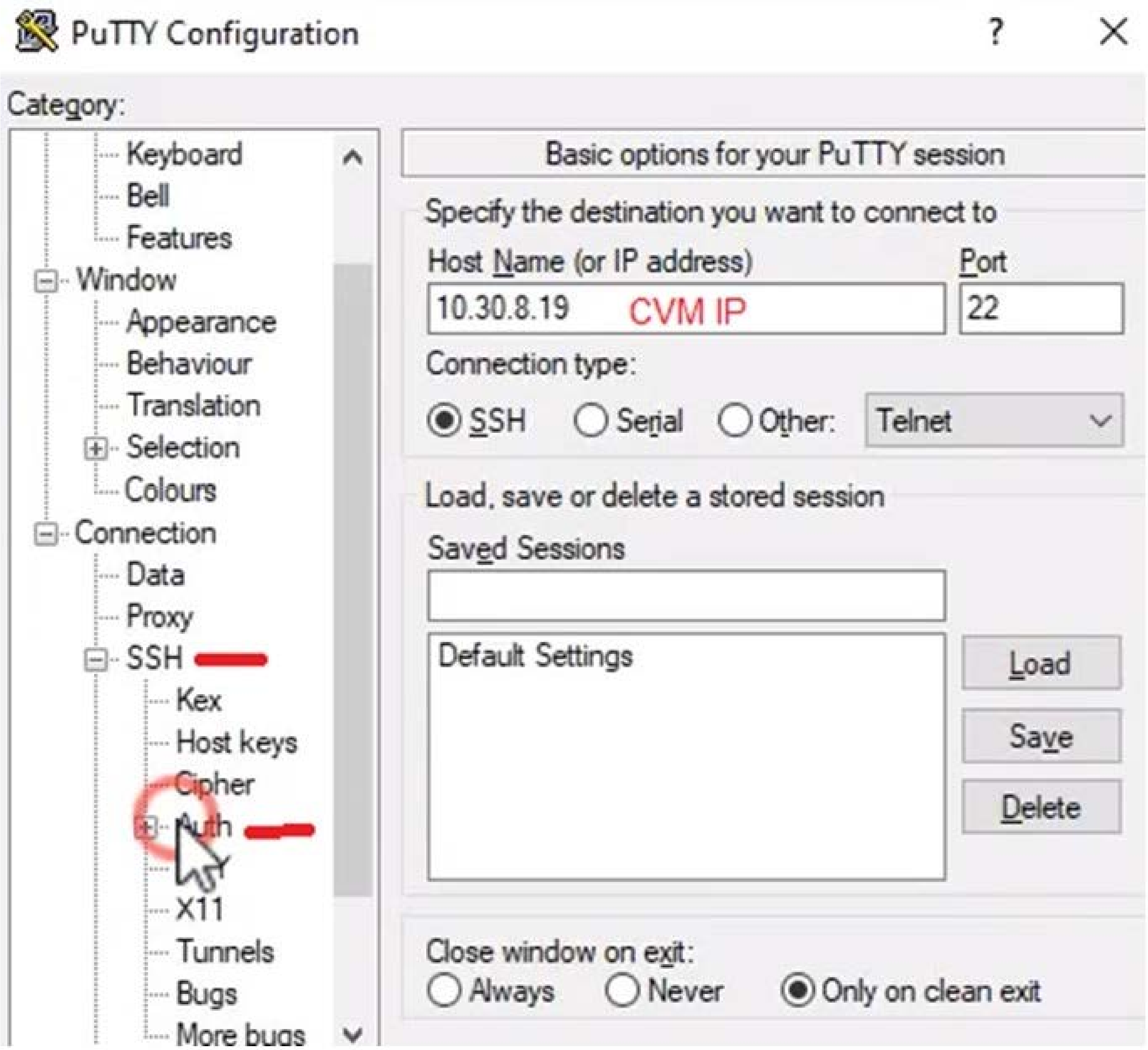
+ New Public Key

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



Name: name_publuc_key

Key: Public Key here



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 10.30.8.19 CVM IP

Port: 22

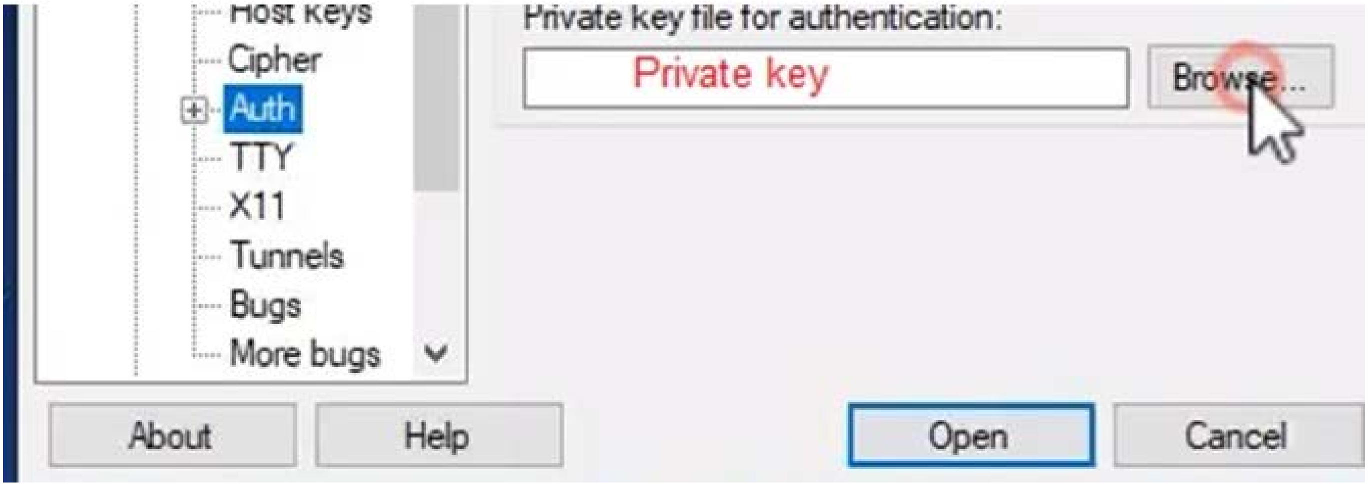
Connection type: ● SSH ○ Serial ○ Other: Telnet

Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit



Private key file for authentication: Private key

QUESTION 3

CORRECT TEXT

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 toadmin@syberdyne.netwhen 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.

A. Answer: See the for step by step solution.

Correct Answer: A

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

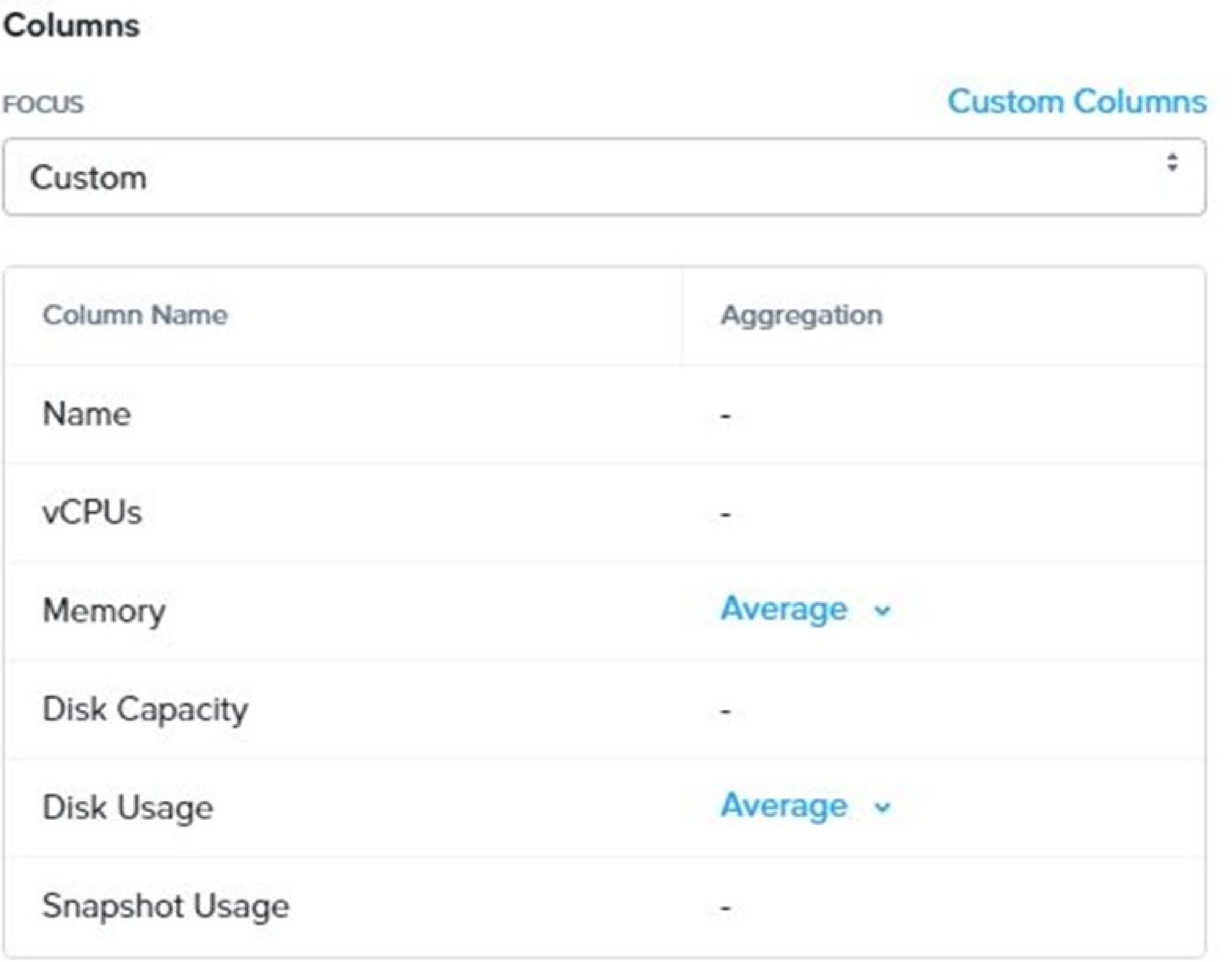
6.This report can include all as well as a selection of the VMs 7.Click on the Custom Columns option and add the below variables:

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

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:

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:

QUESTION 4

CORRECT TEXT

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
```

A. Answer: See the for step by step solution.

Correct Answer: A

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

QUESTION 5

CORRECT TEXT

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 os SQL VMs.

Note: Do not power on any VMs

A. Answer: See the for step by step solution.

Correct Answer: A

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:

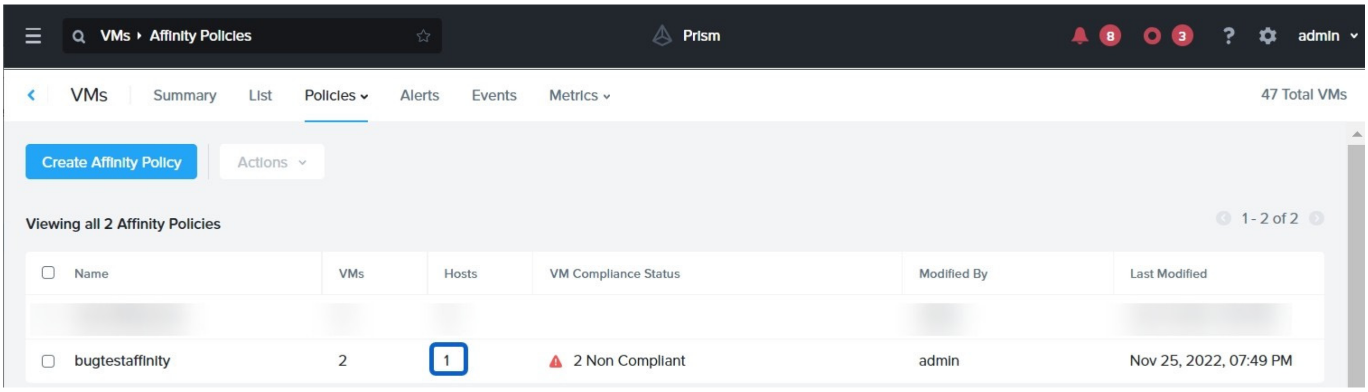
Log in to Prism Central and click on Entities on the left menu. Select Virtual Machines from the drop-down menu and click on Create Group. Enter a name for the group, such as SQL Group, and click Next. Select the SQL VMs (SQL01,

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
[redacted]	[redacted]	[redacted]		[redacted]	[redacted]
□ bugtestaffinity	2	1	▲ 2 Non Compliant	admin	Nov 25, 2022, 07:49 PM

A screenshot of a computer

Description automatically generated with medium confidence

NCM-MCI-6.5 Study Guide NCM-MCI-6.5 Exam Questions NCM-MCI-6.5 Braindumps