NCM-MCI-6.5 Q&As

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

Pass NCM-MCI-6.5 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/ncm-mci-6-5.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

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.

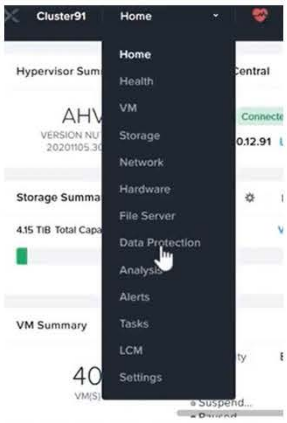
Click Next.

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.

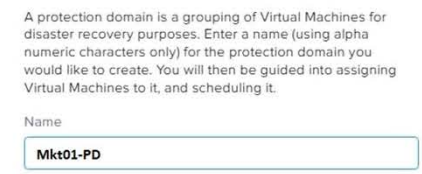
Select Remote Site from the drop-down menu and choose the remote site where you want to replicate the VM. Click Next.

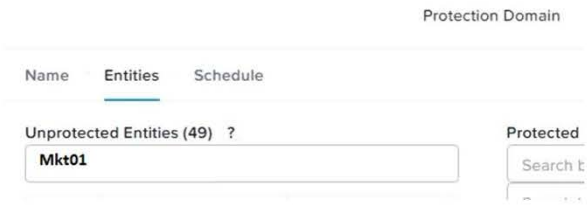
Enter 5 as the number of snapshots to retain on both local and remote sites. Click Next. Review the protection domain details and click Finish. Repeat the same steps for Fin01 and Dev01, using PD_Fin01 and PD_Dev01 as the protection

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


Cluster91
Home
Home
Health
VM
Storage
Network
Hardware
File Server
Data Protection
Alerts
Tasks
LCM
Settings
VM Summary

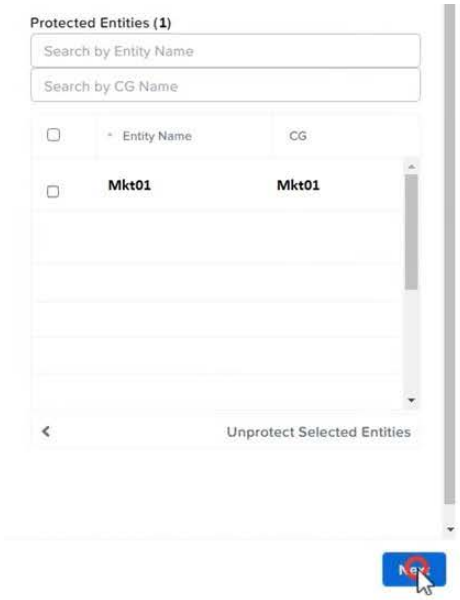

+ Protection Domain
Async DR


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

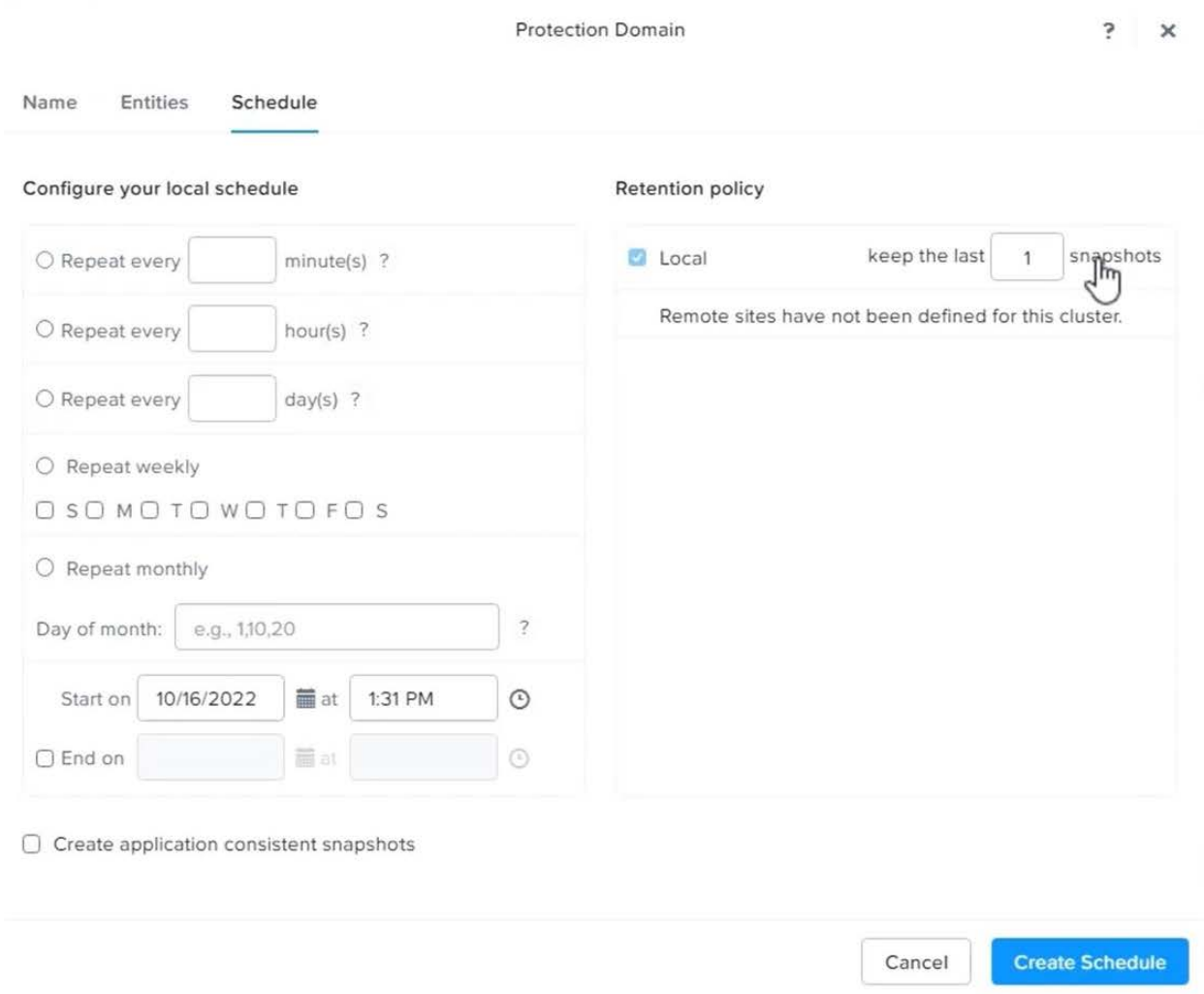

Protection Domain
Name
Entities
Schedule
Unprotected Entities (49) ?
Mkt01
Protected
Search t


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
Unprotect Selected Entities
Next


New Schedule


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
Retention policy
Local keep the last 1 snapshots
Remote sites have not been defined for this cluster.
Create application consistent snapshots
Cancel
Create Schedule

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

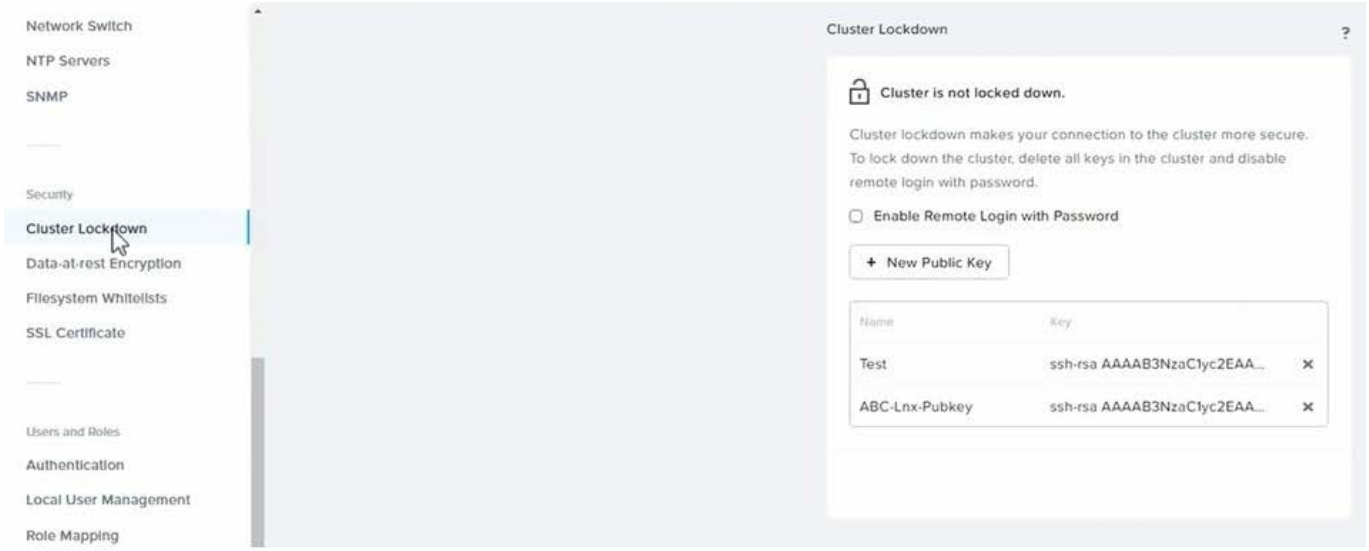
Enable iTLB Multihit M... : false

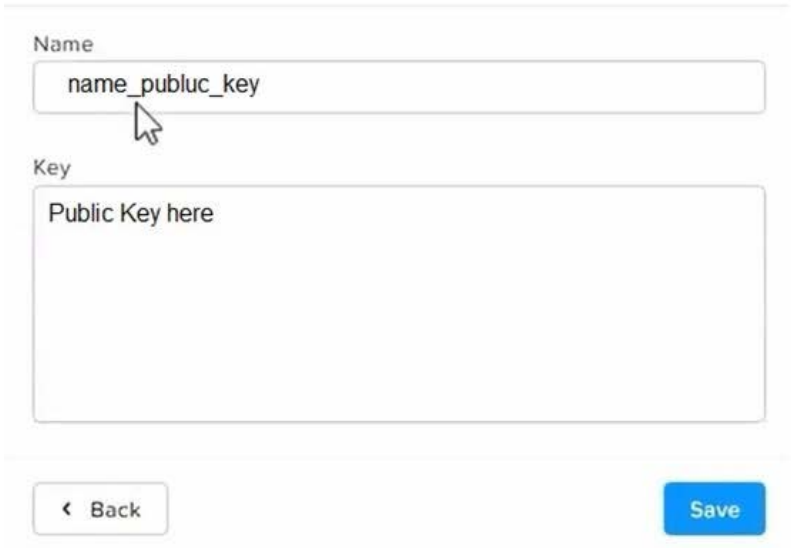
Enable the Advance intrusion Detection Environment (AIDE) to run on a weekly basis for the cluster.

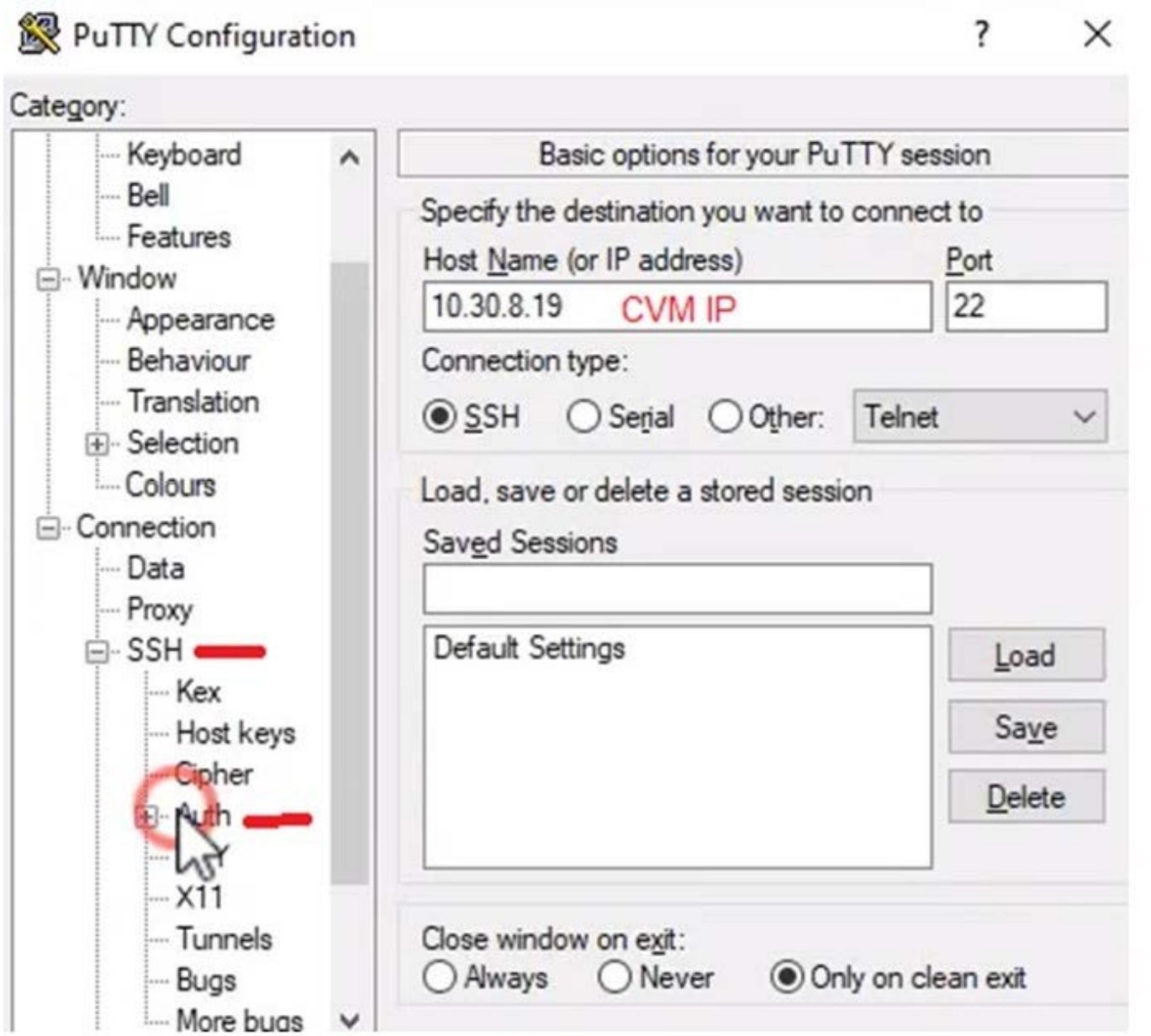
ncli cluster edit-hypervisor-security-params enable-aide=true ncli cluster edit-hypervisor-security-params schedule=weekly

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


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...
ABC-Lnx-Pubkey
ssh-rsa AAAAB3NzaC1yc2EAA...


Name
name_publuc_key
Key
Public Key here
Back
Save


PuTTY Configuration
Category:
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Kex
Host keys
Cipher
Auth
TTY
X11
Tunnels
Bugs
More bugs
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
10.30.8.19
CVM IP
22
Connection type:
SSH
Serial
Other:
Telnet
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit


Host Keys
Cipher
Auth
TTY
X11
Tunnels
Bugs
More bugs
Private key file for authentication:
Private key
Browse...
About
Help
Open
Cancel

QUESTION 3

CORRECT TEXT

Task 10

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

*

VM specifications:

*

vCPUs: 2

*

Memory: BGb

*

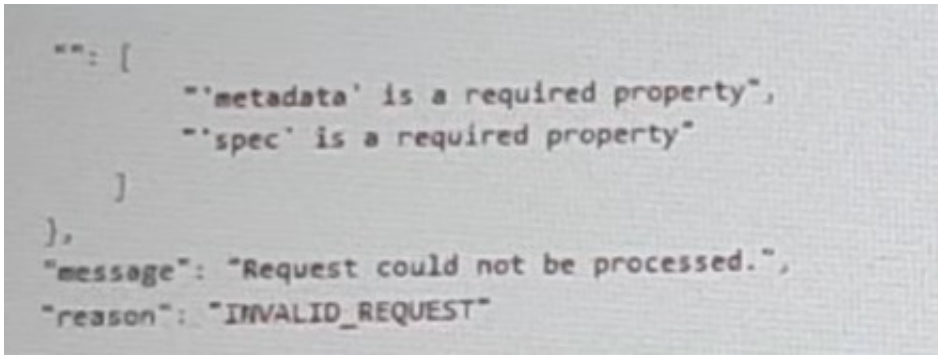
Disk Size: 50Gb

*

Cluster: Cluster A

*

Network: default- net



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

The body is saved in Desktop/ Files/API_Create_VM,text

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

Deploy the vm through the API

Note: Do not power on the VM.

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

Correct Answer: A

https://portal.nutanix.com/page/documents/kbs/details?targetId=kA00e000000LLEzCAO
https://jsonformatter.curiousconcept.com/#

acli net.list(uuid network defult_net)

ncli cluster info(uuid cluster)

Put Call: https://Prism Central IP address : 9440/api/nutanix/v3vms Edit these lines to fix the API call, do not add new lines or copy lines. You can test using the Prism Element API explorer or PostMan Body:

{

{

"spec": {

"name": "Test_Deploy",

"resources": {

"power_state":"OFF",

"num_vcpus_per_socket": ,

"num_sockets": 1,

"memory_size_mib": 8192,

"disk_list": [

{

"disk_size_mib": 51200,

"device_properties": {

"device_type":"DISK"

}

},

{

"device_properties": {

"device_type":"CDROM"

}

}

],

"nic_list":[

{

"nic_type": "NORMAL_NIC",

"is_connected": true,

"ip_endpoint_list": [

{

"ip_type": "DHCP"

}

],

"subnet_reference": {

"kind": "subnet",

"name": "default_net",

"uuid": "00000000-0000-0000-0000-000000000000"

}

}

],

},

"cluster_reference": {

"kind": "cluster",

"name": "NTNXDemo",

"uuid": "00000000-0000-0000-0000-000000000000"

}

},

"api_version": "3.1.0",

"metadata": {

"kind": "vm"

}

}

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

Reference

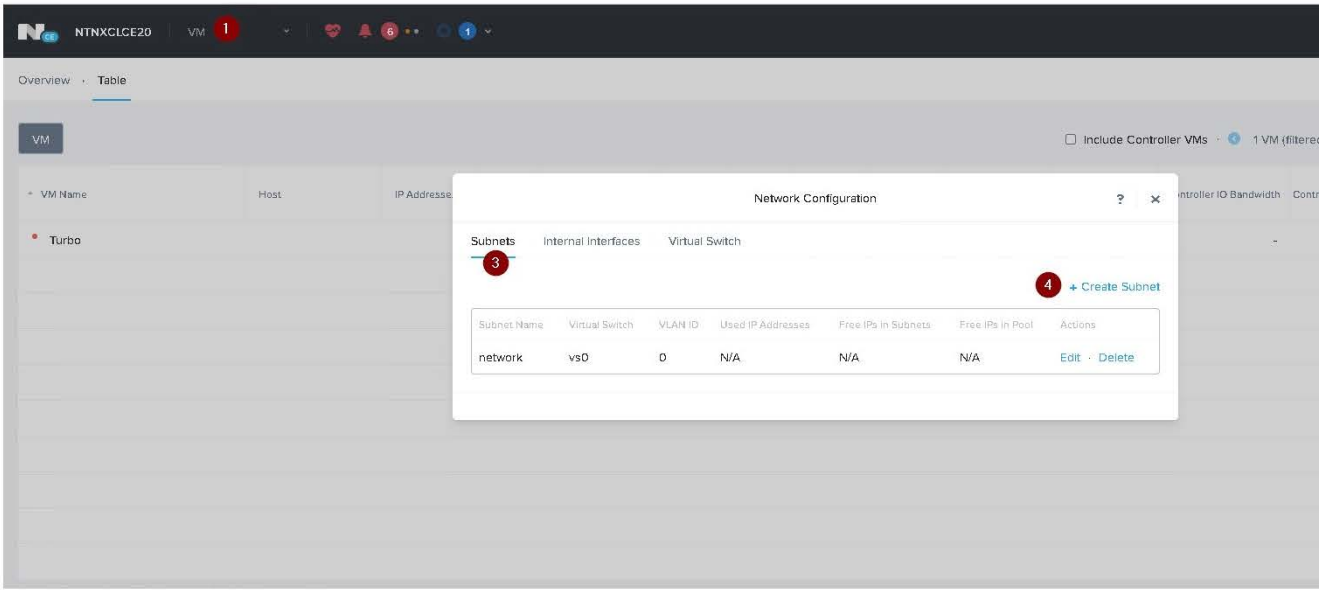
QUESTION 4

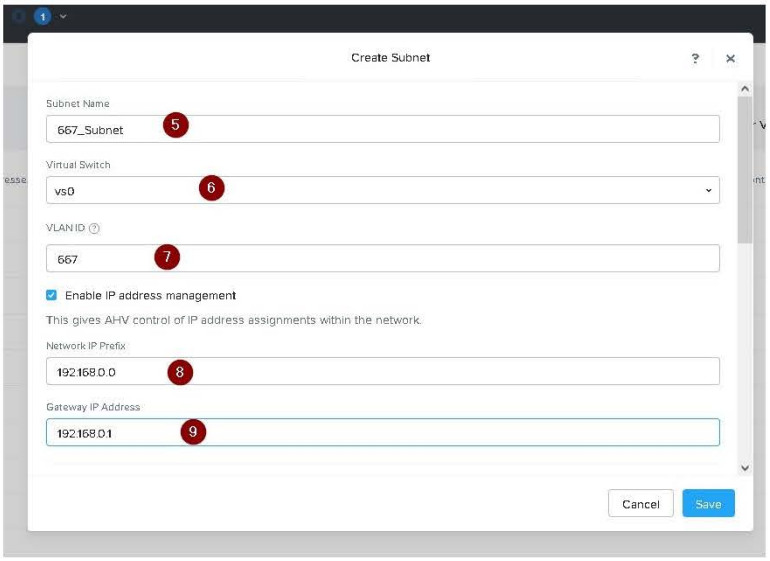
CORRECT TEXT Task 5 An administrator has been informed that a new workload requires a logically segmented network to meet security requirements. Network configuration: VLAN: 667 Network: 192.168.0.0 Subnet Mask: 255.255.255.0 DNS server: 34.82.231.220 Default Gateway: 192.168.0.1 Domain: cyberdyne.net 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.

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

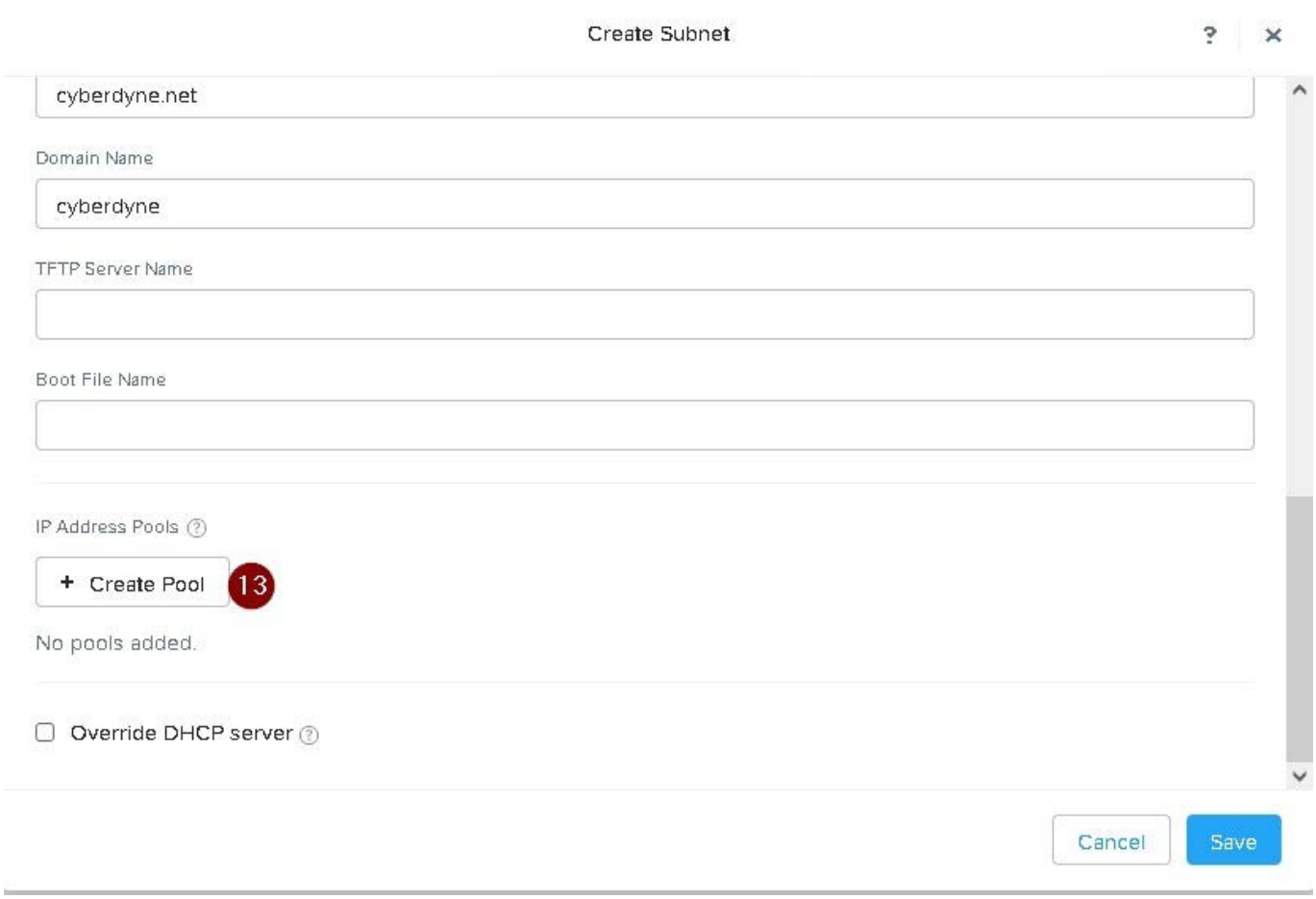
Correct Answer: A

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
VM
Include Controller VMs
VM Name
Host
IP Address
Turbo
Network Configuration
Subnets
Internal Interfaces
Virtual Switch
3
4
+ Create Subnet
Subnet Name
Virtual Switch
VLAN ID
Used IP Addresses
Free IPs in Subnets
Free IPs in Pool
Actions
network
vs0
0
N/A
N/A
N/A
Edit
Delete


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
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
Boot File Name
Cancel
Save


Create Subnet
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

QUESTION 5

CORRECT TEXT

Task 13

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 toappdev@cyberdyne.netwhen 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.

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

Correct Answer: A

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.