# 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 15

An administrator found a CentOS VM, Cent_Down, on the cluster with a corrupted network stack. To correct the issue, the VM will need to be restored from a previous snapshot to become reachable on the network again.

VM credentials:

Username: root

Password: nutanix/4u

Restore the VM and ensure it is reachable on the network by pinging 172.31.0.1 from the VM.

Power off the VM before proceeding.

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

Correct Answer: A

To restore the VM and ensure it is reachable on the network, you can follow these steps:

Log in to the Web Console of the cluster where the VM is running. Click on Virtual Machines on the left menu and find Cent_Down from the list. Click on the power icon to power off the VM.

Click on the snapshot icon next to the power icon to open the Snapshot Management window.

Select a snapshot from the list that was taken before the network stack was corrupted. You can use the date and time information to choose a suitable snapshot. Click on Restore VM and confirm the action in the dialog box. Wait for the

restore process to complete.

Click on the power icon again to power on the VM. Log in to the VM using SSH or console with the username and password provided. Run the command ping 172.31.0.1 to verify that the VM is reachable on the network. You should see a

reply from the destination IP address.

Go to VMS from the prism central gui

Select the VMand go to More -> Guest Shutdown

Go to Snapshots tab and revert to latest snapshot available power on vm and verify if ping is working

**QUESTION 2**

CORRECT TEXT

Task 8

Depending on the order you perform the exam items, the access information and credentials could change. Please refer to the other item performed on Cluster B if you have problems accessing the cluster.

The infosec team has requested that audit logs for API Requests and replication capabilities be enabled for all clusters for the top 4 severity levels and pushed to their syslog system using highest reliability possible. They have requested no other logs to be included.

Syslog configuration:

Syslog Name: Corp_syslog

Syslop IP: 34.69.43.123

Port: 514

Ensure the cluster is configured to meet these requirements.

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

Correct Answer: A

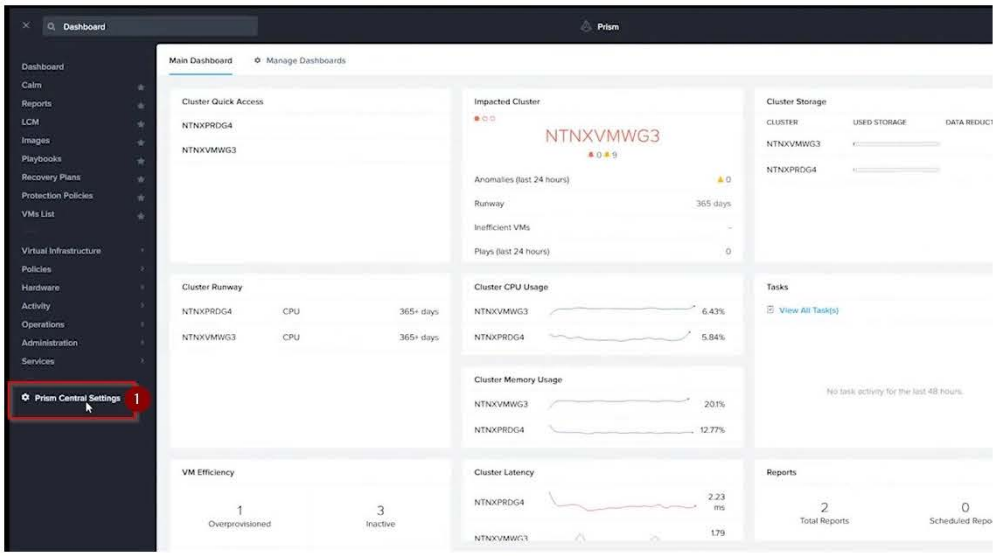
To configure the cluster to meet the requirements of the infosec team, you need to do the following steps:

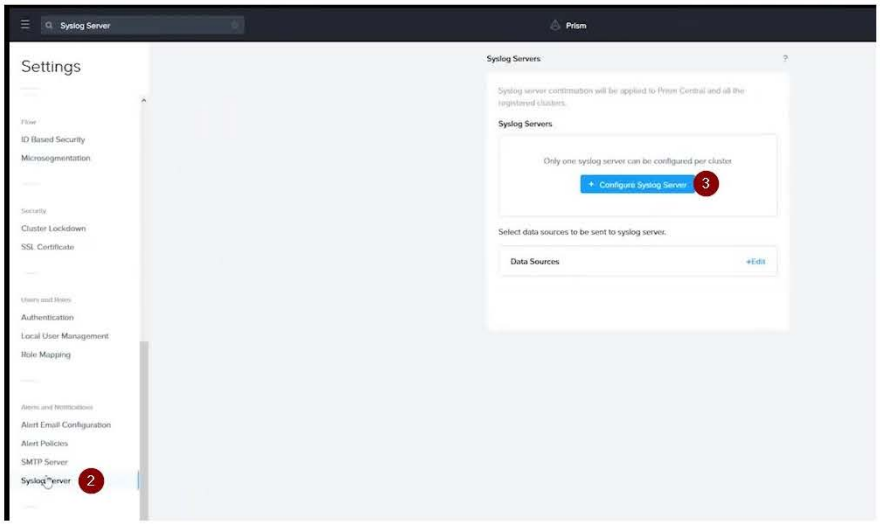
Log in to Prism Central and go to Network > Syslog Servers > Configure Syslog Server. Enter Corp_syslog as the Server Name, 34.69.43.123 as the IP Address, and 514 as the Port. Select TCP as the Transport Protocol and enable RELP

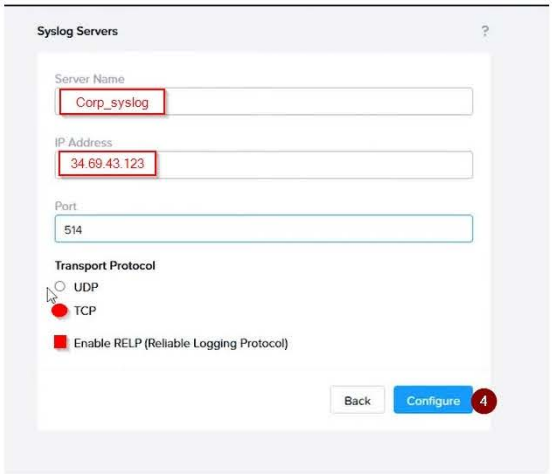
(Reliable Logging Protocol). This will create a syslog server with the highest reliability possible. Click Edit against Data Sources and select Cluster B as the cluster. Select API Requests and Replication as the data sources and set the log level

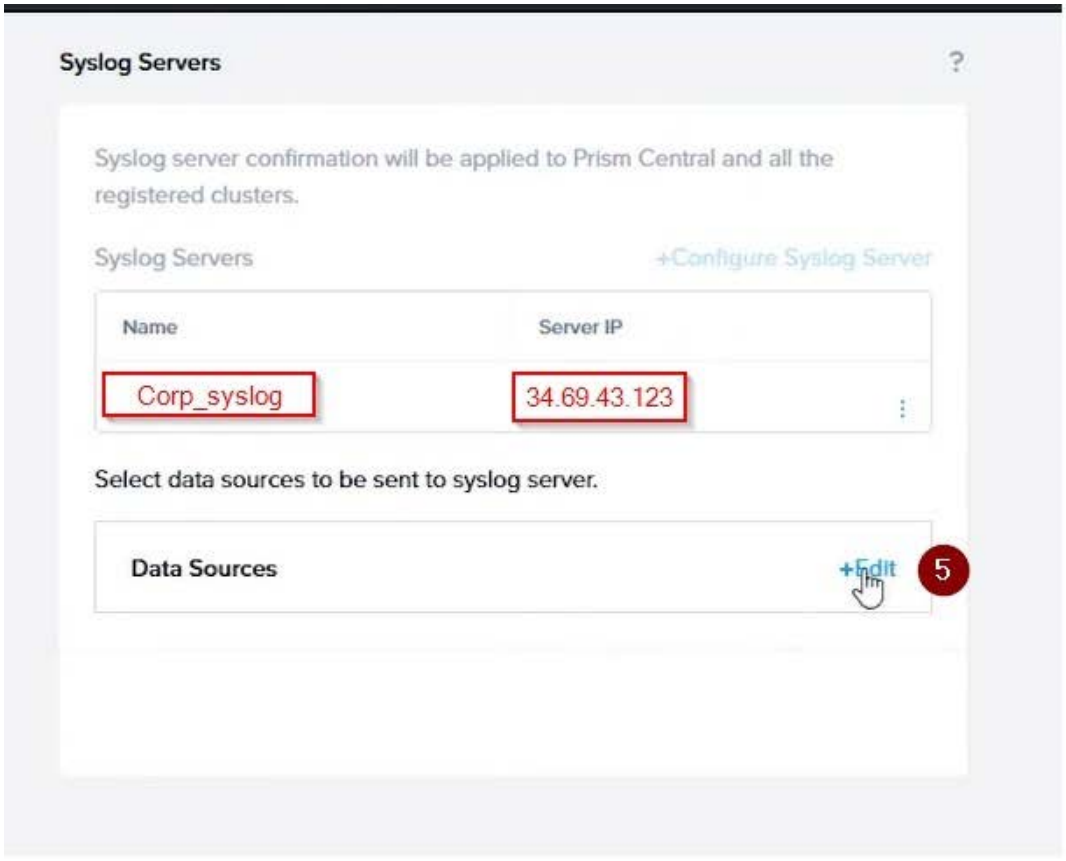
to CRITICAL for both of them. This will enable audit logs for API requests and replication capabilities for the top 4 severity levels (EMERGENCY, ALERT, CRITICAL, and ERROR) and push them to the syslog server. Click Save.

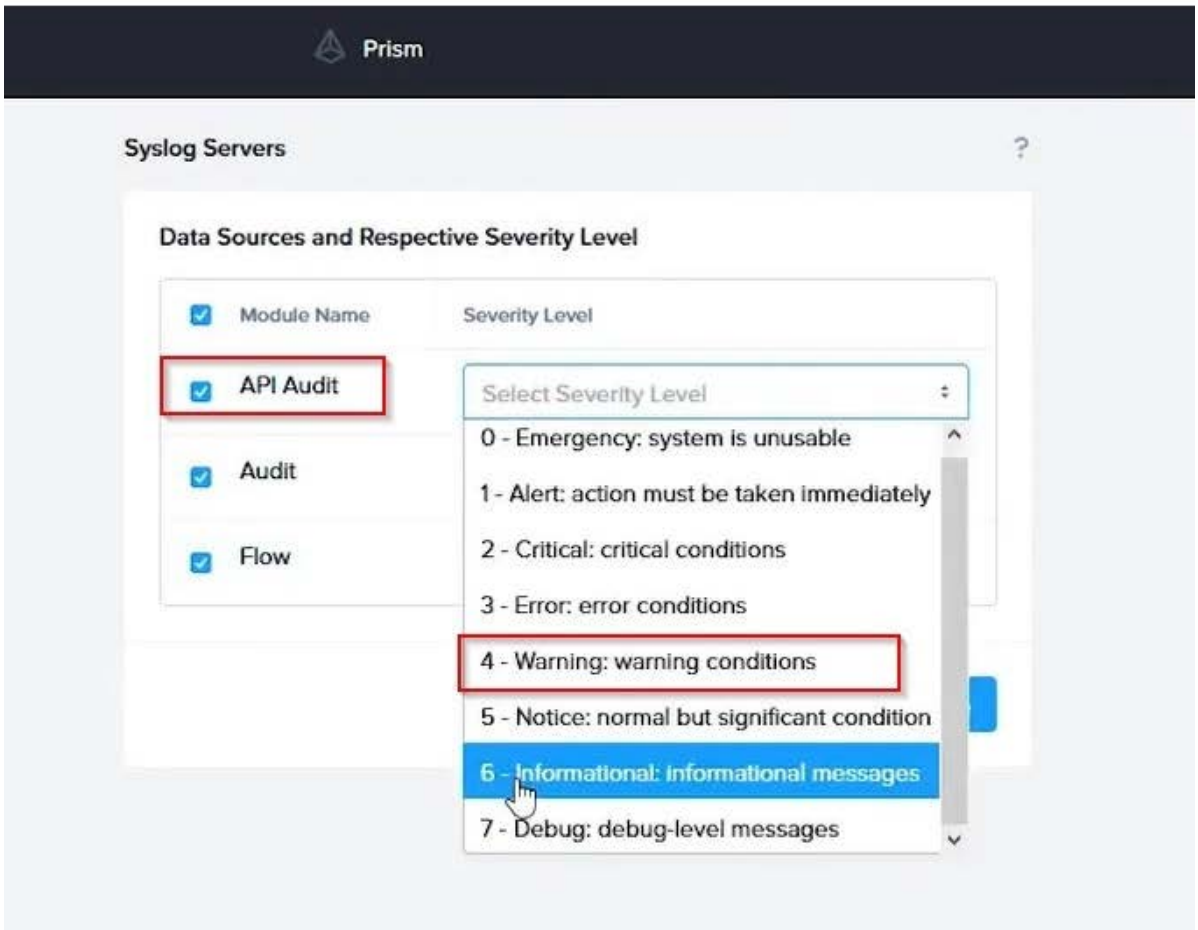
Repeat step 2 for any other clusters that you want to configure with the same requirements.


Dashboard
Prism
Main Dashboard
Manage Dashboards
Prism Central Settings
1
Cluster Quick Access
Impacted Cluster
NTNXVMWG3
Cluster Storage
Cluster Runway
Cluster CPU Usage
Cluster Memory Usage
Tasks
VM Efficiency
Cluster Latency
Reports


Syslog Server
Prism
Settings
Syslog Servers
Syslog Servers
Configure Syslog Server
3
Data Sources
Syslog Server
2


Syslog Servers
Server Name
Corp_syslog
IP Address
34.69.43.123
Port
514
Transport Protocol
UDP
TCP
Enable RELP (Reliable Logging Protocol)
Back
Configure
4


Syslog Servers
Syslog server confirmation will be applied to Prism Central and all the registered clusters.
Syslog Servers
+Configure Syslog Server
Name
Server IP
Corp_syslog
34.69.43.123
Select data sources to be sent to syslog server.
Data Sources
+Edit
5


Prism
Syslog Servers
Data Sources and Respective Severity Level
Module Name
Severity Level
API Audit
Audit
Flow
Select Severity Level
0 - Emergency: system is unusable
1 - Alert: action must be taken immediately
2 - Critical: critical conditions
3 - Error: error conditions
4 - Warning: warning conditions
5 - Notice: normal but significant condition
6 - Informational: informational messages
7 - Debug: debug-level messages

To configure the Nutanix clusters to enable audit logs for API Requests and replication capabilities, and push them to the syslog system with the highest reliability possible, you can follow these steps:

Log in to the Nutanix Prism web console using your administrator credentials. Navigate to the "Settings" section or the configuration settings interface within Prism. Locate the "Syslog Configuration" or "Logging" option and click on it.

Configure the syslog settings as follows:

Syslog Name: Enter "Corp_syslog" as the name for the syslog configuration. Syslog IP: Set the IP address to "34.69.43.123", which is the IP address of the syslog system.

Port: Set the port to "514", which is the default port for syslog. Enable the option for highest reliability or persistent logging, if available. This ensures that logs are sent reliably and not lost in case of network interruptions.

Save the syslog configuration.

Enable Audit Logs for API Requests:

In the Nutanix Prism web console, navigate to the "Cluster" section or the cluster management interface.

Select the desired cluster where you want to enable audit logs. Locate the "Audit Configuration" or "Security Configuration" option and click on it. Look for the settings related to audit logs and API requests. Enable the audit logging feature and

select the top 4 severity levels to be logged.

Save the audit configuration.

Enable Audit Logs for Replication Capabilities:

In the Nutanix Prism web console, navigate to the "Cluster" section or the cluster management interface.

Select the desired cluster where you want to enable audit logs. Locate the "Audit Configuration" or "Security Configuration" option and click on it. Look for the settings related to audit logs and replication capabilities. Enable the audit logging

feature and select the top 4 severity levels to be logged.

Save the audit configuration.

After completing these steps, the Nutanix clusters will be configured to enable audit logs for API Requests and replication capabilities. The logs will be sent to the specified syslog system with the highest reliability possible.

ncli

rsyslog-config set-status enable=false

rsyslog-config add-server name=Corp_Syslog ip-address=34.69.43.123 port=514 network-protocol=tdp relp-enabled=false

rsyslog-config add-module server-name= Corp_Syslog module-name=APLOS level=INFO

rsyslog-config add-module server-name= Corp_Syslog module-name=CEREBRO level=INFO

rsyslog-config set-status enable=true

https://portal.nutanix.com/page/documents/kbs/details?targetId=kA00e0000009CEECA2

**QUESTION 3**

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

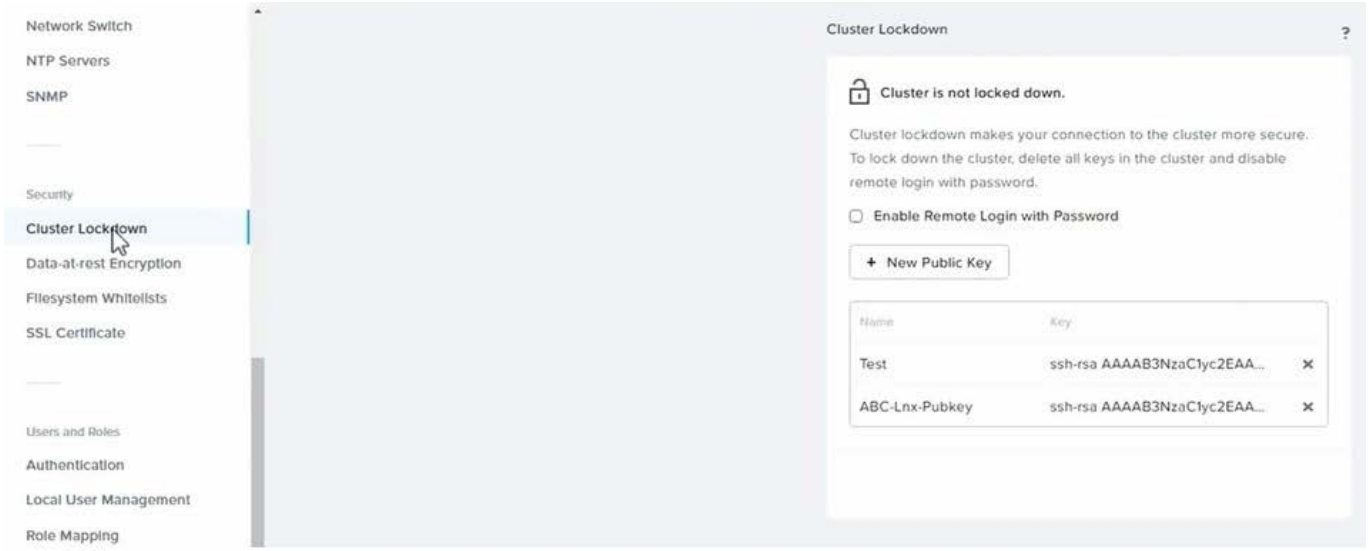
Enable iTLB Multihit M... : false

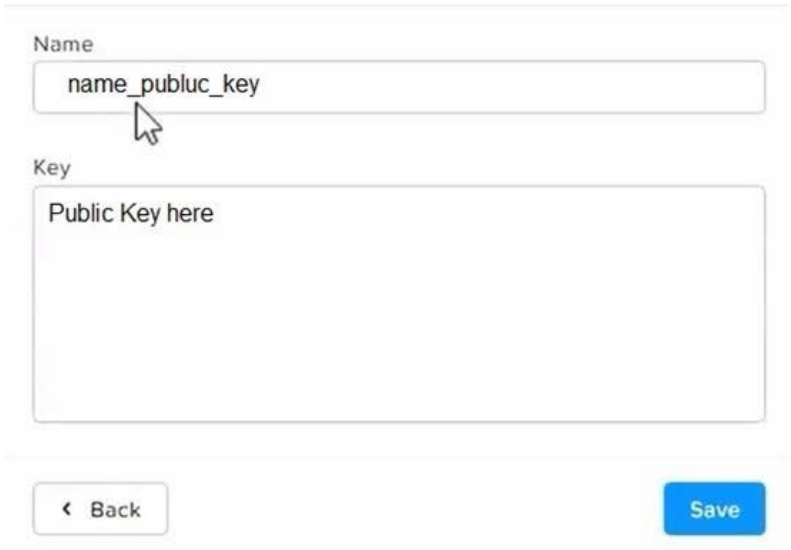
Enable the Advance intrusion Detection Environment (AIDE) to run on a weekly basis for the cluster.

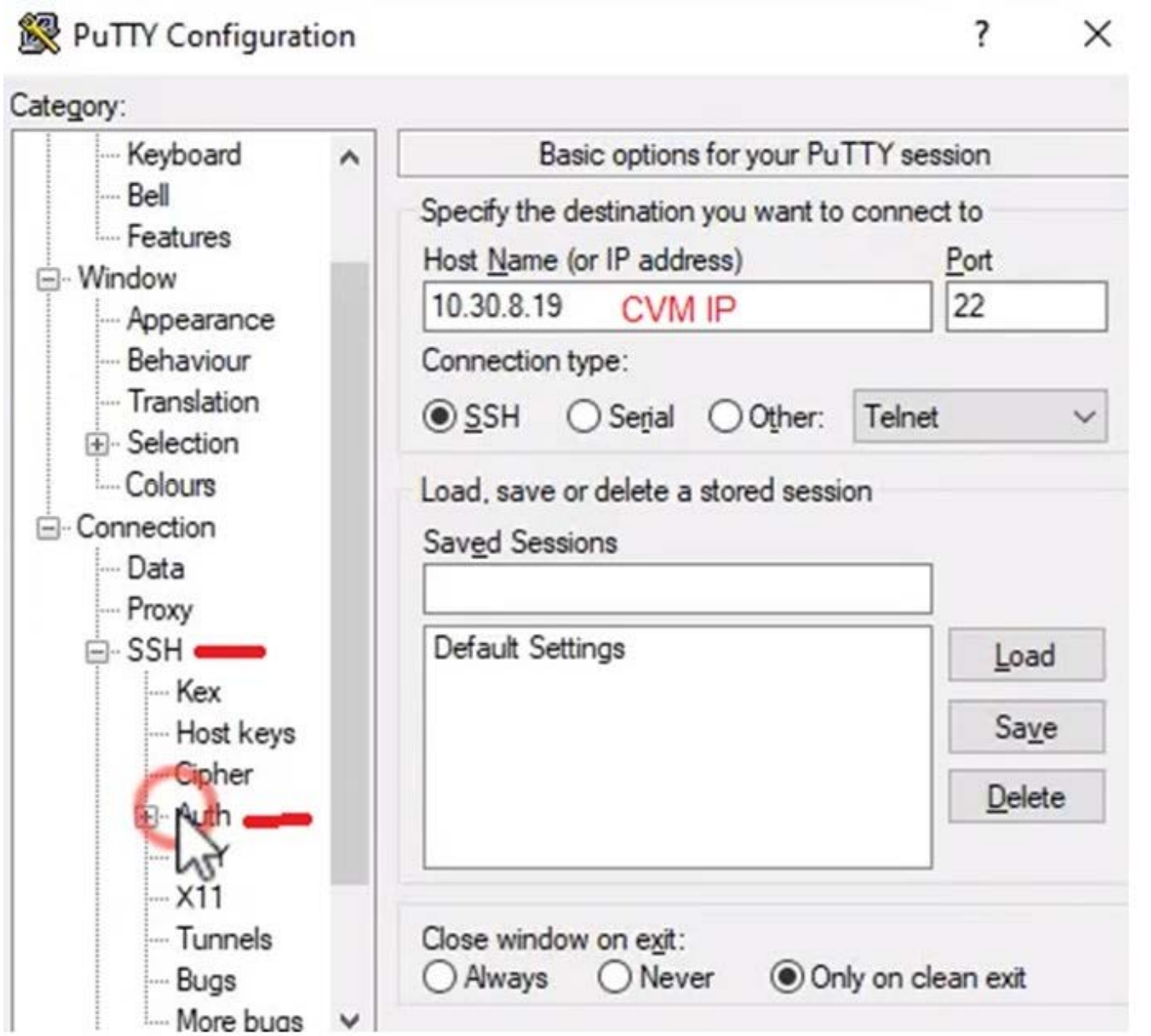
ncli cluster edit-hypervisor-security-params enable-aide=true ncli cluster edit-hypervisor-security-params schedule=weekly

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
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 4**

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

*

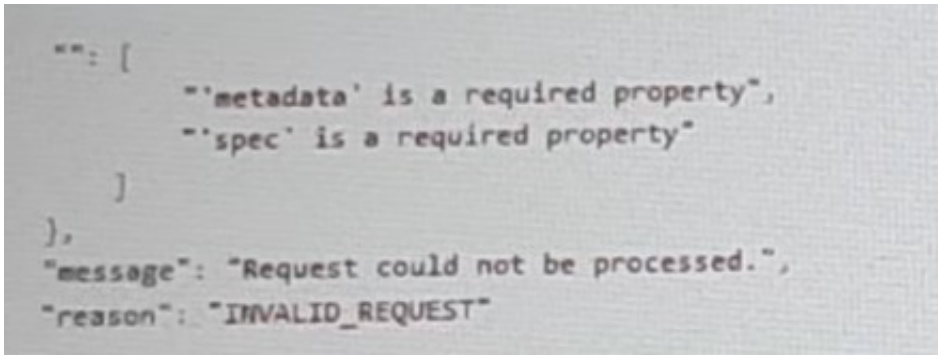
Disk Size: 50Gb

*

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 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:

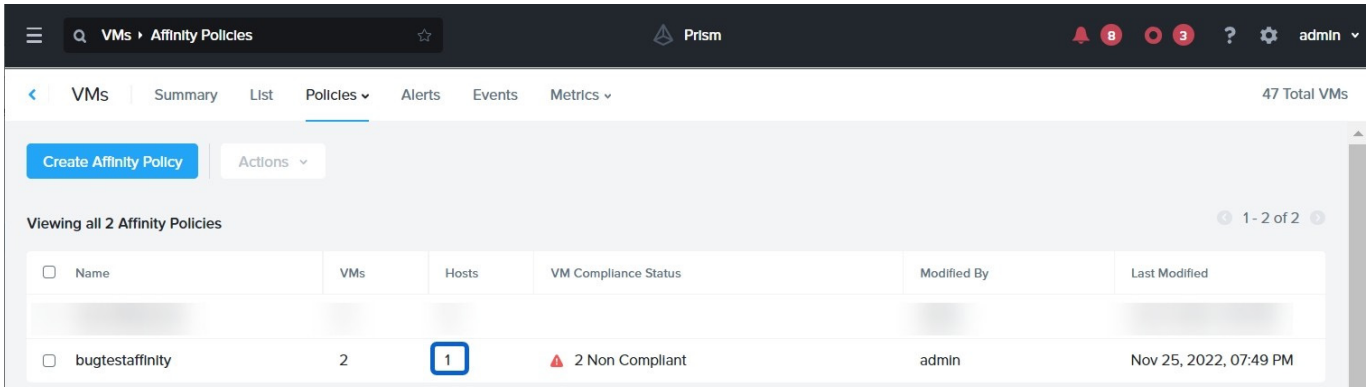
Log in to Prism Central and click on Entities on the left menu. Select Virtual Machines from the drop-down menu and click on Create Group. Enter a name for the group, such as SQL Group, and click Next. Select the SQL VMs (SQL01,

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




A screenshot of a computer

Description automatically generated with medium confidence

Latest NCM-MCI-6.5 Dumps NCM-MCI-6.5 Practice Test NCM-MCI-6.5 Exam Questions