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

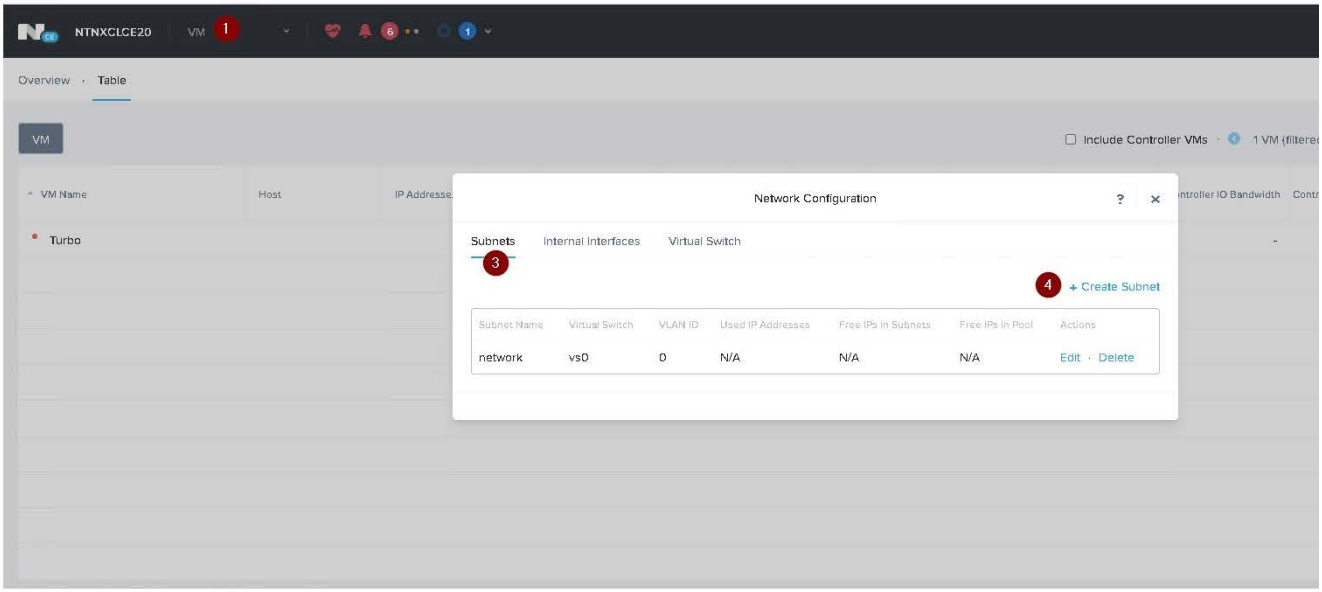
QUESTION 1

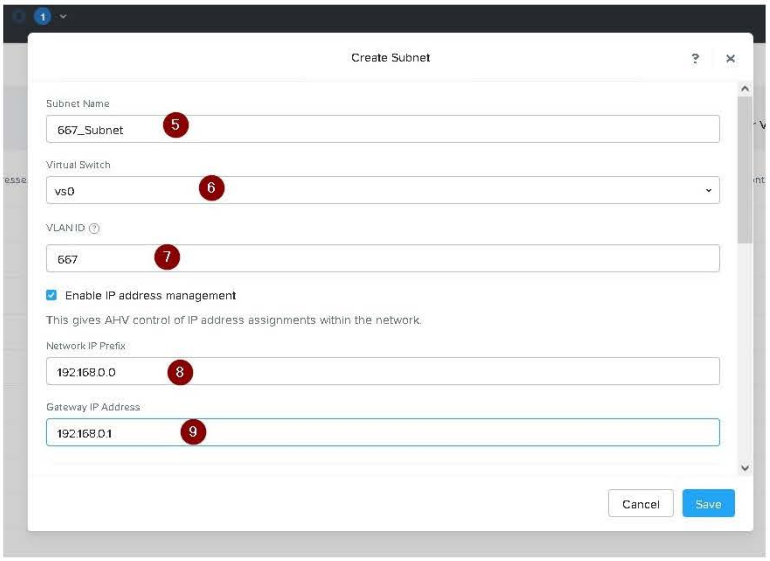
CORRECT TEXT Task 5 An administrator has been informed that a new workload requires a logically segmented network to meet security requirements. Network configuration: VLAN: 667 Network: 192.168.0.0 Subnet Mask: 255.255.255.0 DNS server: 34.82.231.220 Default Gateway: 192.168.0.1 Domain: cyberdyne.net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

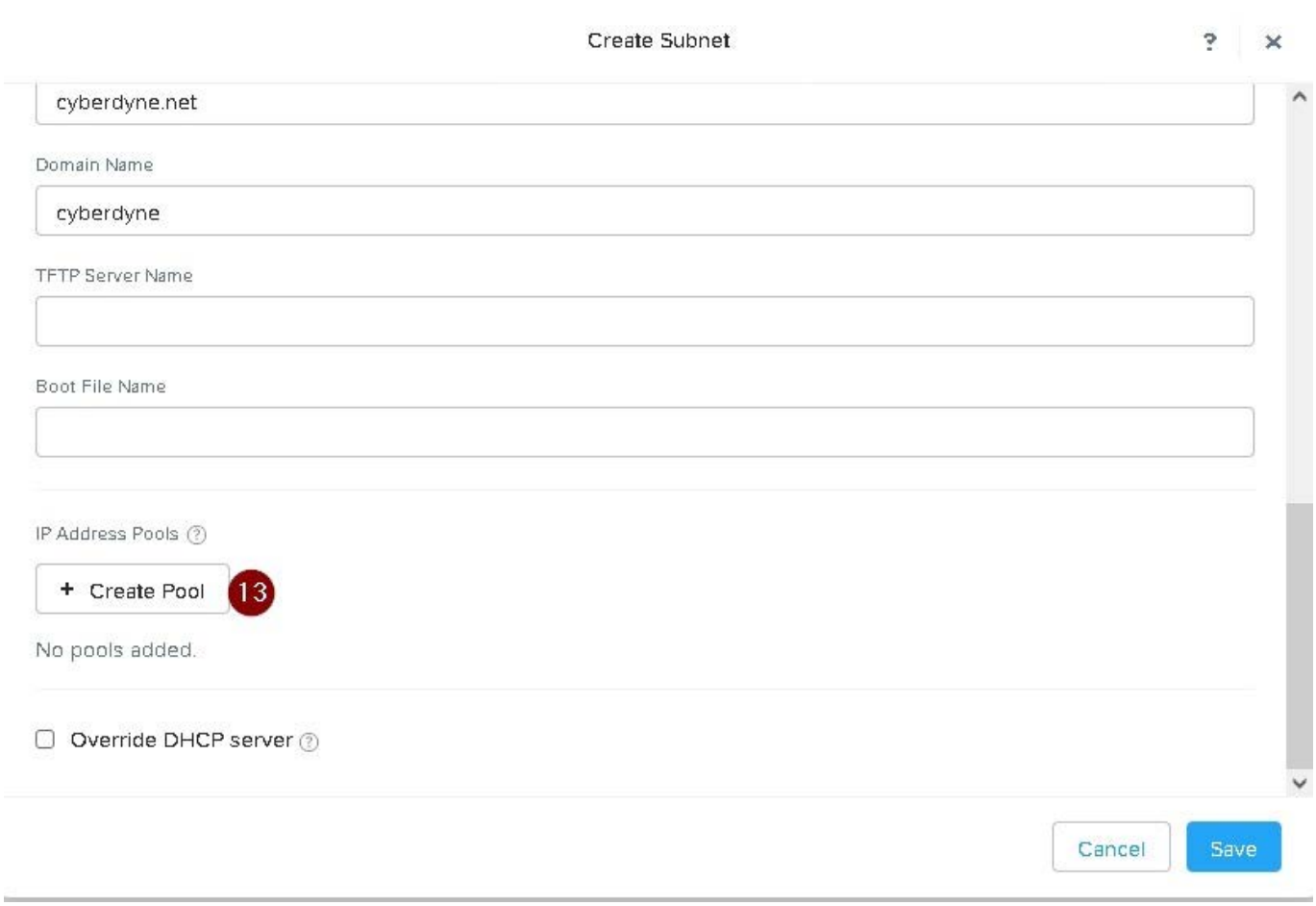
Correct Answer: A

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 2

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

*

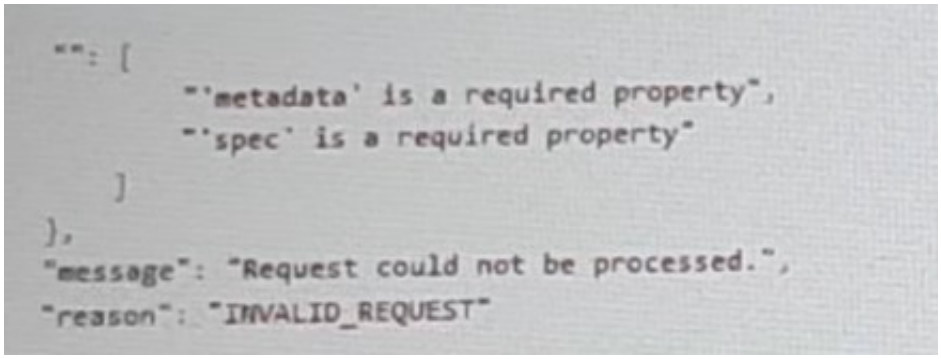
Disk Size: 50Gb

*

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 3

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

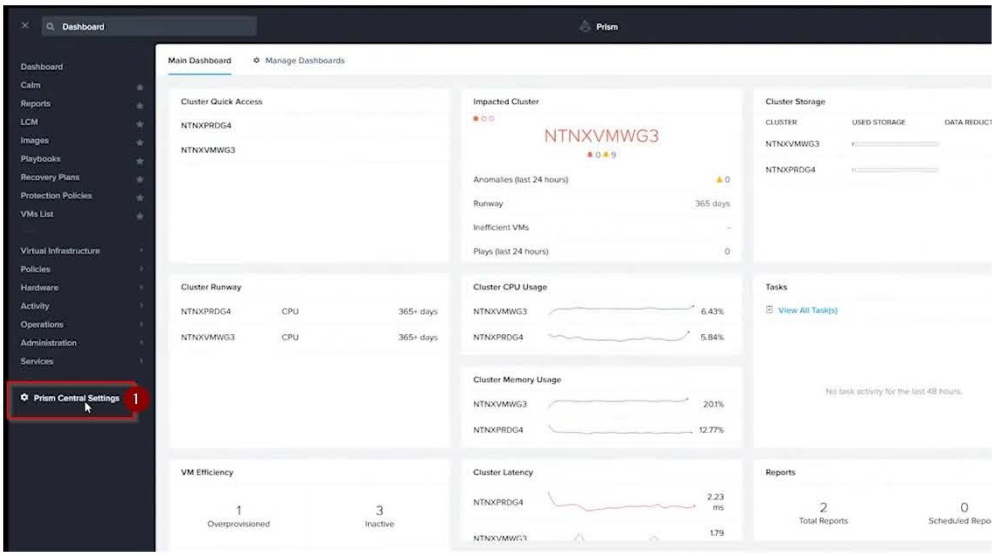
To configure the cluster to meet the requirements of the infosec team, you need to do the following steps:

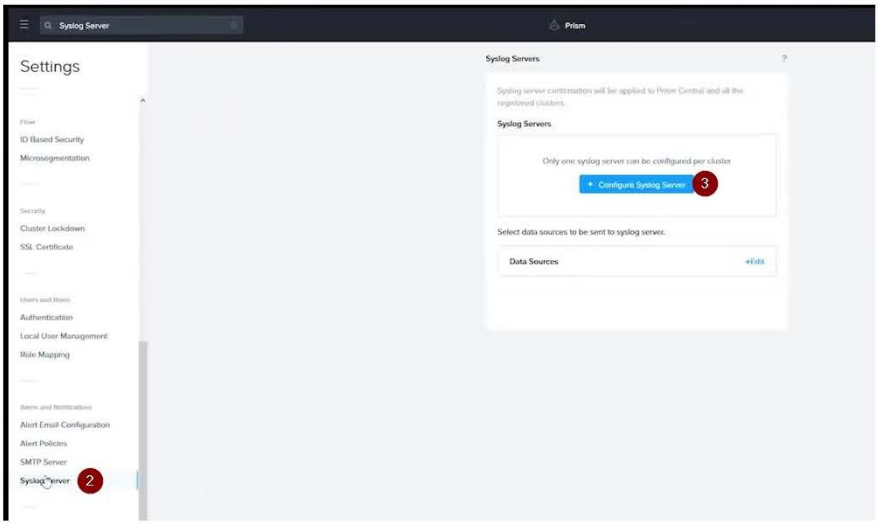
Log in to Prism Central and go to Network > Syslog Servers > Configure Syslog Server. Enter Corp_syslog as the Server Name, 34.69.43.123 as the IP Address, and 514 as the Port. Select TCP as the Transport Protocol and enable RELP

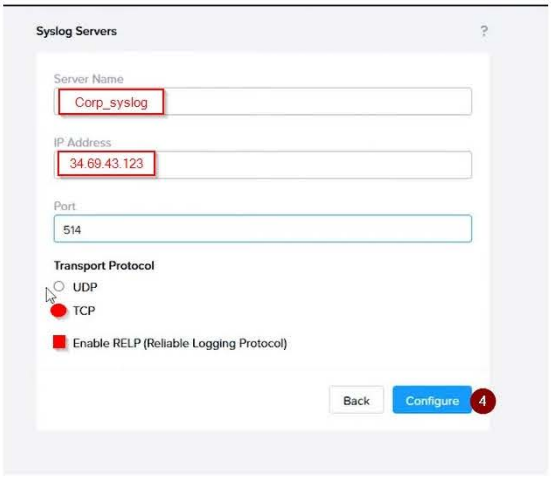
(Reliable Logging Protocol). This will create a syslog server with the highest reliability possible. Click Edit against Data Sources and select Cluster B as the cluster. Select API Requests and Replication as the data sources and set the log level

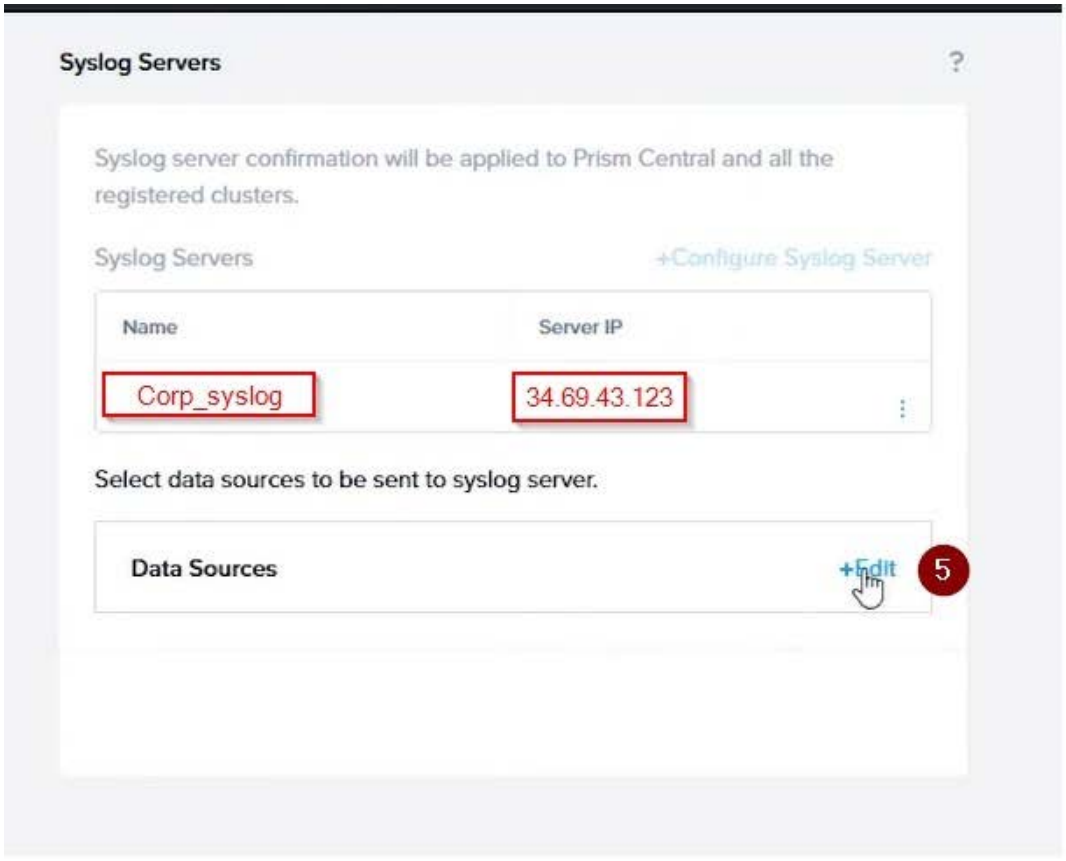
to CRITICAL for both of them. This will enable audit logs for API requests and replication capabilities for the top 4 severity levels (EMERGENCY, ALERT, CRITICAL, and ERROR) and push them to the syslog server. Click Save.

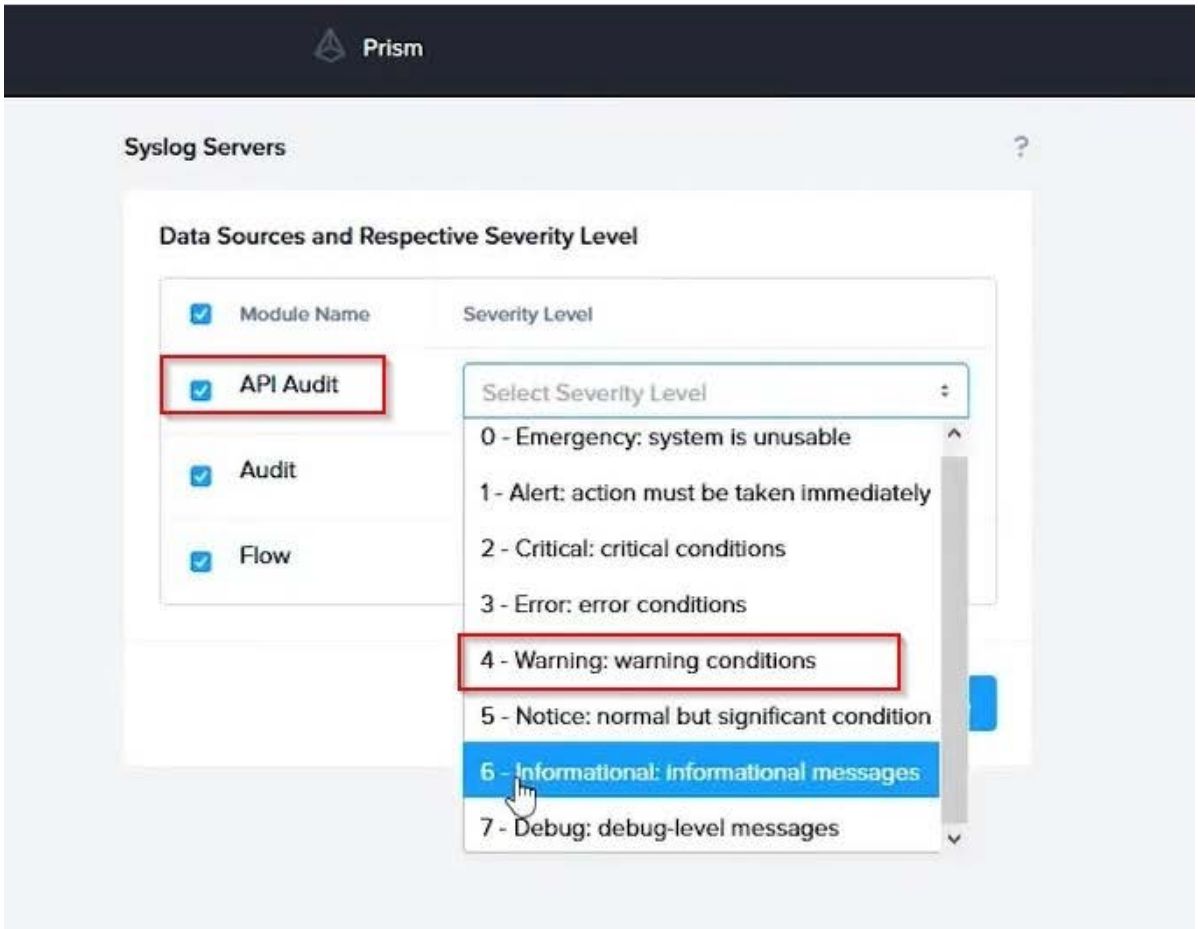
Repeat step 2 for any other clusters that you want to configure with the same requirements.


Dashboard
Prism
Main Dashboard
Manage Dashboards
Prism Central Settings
1
Cluster Quick Access
NTNXPRDG4
NTNXVMWG3
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
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
Select Severity Level
Audit
Flow
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 4

CORRECT TEXT Task 3 An administrator needs to assess performance gains provided by AHV Turbo at the guest level. To perform the test the administrator created a Windows 10 VM named Turbo with the following configuration. 1 vCPU 8 GB RAM SATA Controller

40 GB vDisk

The stress test application is multi-threaded capable, but the performance is not as expected with AHV Turbo enabled. Configure the VM to better leverage AHV Turbo.

Note: Do not power on the VM. Configure or prepare the VM for configuration as best you can without powering it on.

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

Correct Answer: A

To configure the VM to better leverage AHV Turbo, you can follow these steps:

Log in to Prism Element of cluster A using the credentials provided.

Go to VM > Table and select the VM named Turbo.

Click on Update and go to Hardware tab.

Increase the number of vCPUs to match the number of multiqueues that you want to enable. For example, if you want to enable 8 multiqueues, set the vCPUs to 8. This will improve the performance of multi-threaded workloads by allowing

them to use multiple processors.

Change the SCSI Controller type from SATA to VirtIO. This will enable the use of VirtIO drivers, which are required for AHV Turbo.

Click Save to apply the changes.

Power off the VM if it is running and mount the Nutanix VirtIO ISO image as a CD-ROM device. You can download the ISO image fromNutanix Portal. Power on the VM and install the latest Nutanix VirtIO drivers for Windows 10. You can

follow the instructions fromNutanix Support Portal. After installing the drivers, power off the VM and unmount the Nutanix VirtIO ISO image.

Power on the VM and log in to Windows 10.

Open a command prompt as administrator and run the following command to enable multiqueue for the VirtIO NIC:

ethtool -L eth0 combined 8

Replaceeth0with the name of your network interface and8with the number of multiqueues that you want to enable. You can useipconfig /allto find out your network interface name.

Restart the VM for the changes to take effect.

You have now configured the VM to better leverage AHV Turbo. You can run your stress test application again and observe the performance gains.

https://portal.nutanix.com/page/documents/kbs/details?targetId=kA00e000000LKPdCAO change vCPU to 2/4 ?

Change SATA Controller to SCSI:

acli vm.get Turbo

Output Example:

Turbo {

config {

agent_vm: False

allow_live_migrate: True

boot {

boot_device_order: "kCdrom"

boot_device_order: "kDisk"

boot_device_order: "kNetwork"

uefi_boot: False

}

cpu_passthrough: False

disable_branding: False

disk_list {

addr {

bus: "ide"

index: 0

}

cdrom: True

device_uuid: "994b7840-dc7b-463e-a9bb-1950d7138671" empty: True

}

disk_list {

addr {

bus: "sata"

index: 0

}

container_id: 4

container_uuid: "49b3e1a4-4201-4a3a-8abc-447c663a2a3e" device_uuid: "622550e4-fb91-49dd-8fc7-9e90e89a7b0e" naa_id: "naa.6506b8dcda1de6e9ce911de7d3a22111"

storage_vdisk_uuid: "7e98a626-4cb3-47df-a1e2-8627cf90eae6" vmdisk_size: 10737418240

vmdisk_uuid: "17e0413b-9326-4572-942f-68101f2bc716" }

flash_mode: False

hwclock_timezone: "UTC"

machine_type: "pc"

memory_mb: 2048

name: "Turbo"

nic_list {

connected: True

mac_addr: "50:6b:8d:b2:a5:e4"

network_name: "network"

network_type: "kNativeNetwork"

network_uuid: "86a0d7ca-acfd-48db-b15c-5d654ff39096" type: "kNormalNic"

uuid: "b9e3e127-966c-43f3-b33c-13608154c8bf"

vlan_mode: "kAccess"

}

num_cores_per_vcpu: 2

num_threads_per_core: 1

num_vcpus: 2

num_vnuma_nodes: 0

vga_console: True

vm_type: "kGuestVM"

}

is_rf1_vm: False

logical_timestamp: 2

state: "Off"

uuid: "9670901f-8c5b-4586-a699-41f0c9ab26c3"

}

acli vm.disk_create Turbo clone_from_vmdisk=17e0413b-9326-4572-942f-68101f2bc716 bus=scsi

remove the old disk

acli vm.disk_delete 17e0413b-9326-4572-942f-68101f2bc716 disk_addr=sata.0

QUESTION 5

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