

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.leads4pass.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 7**

An administrator has environment that will soon be upgraded to 6.5. In the meantime, they need to implement log and apply a security policy named Staging_Production, such that not VM in the Staging Environment can communicate with any

VM in the production Environment,

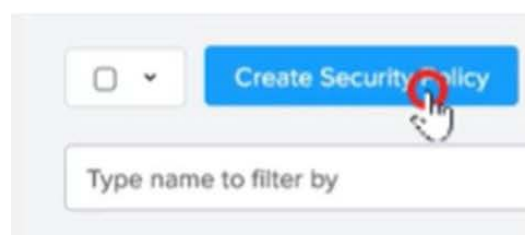
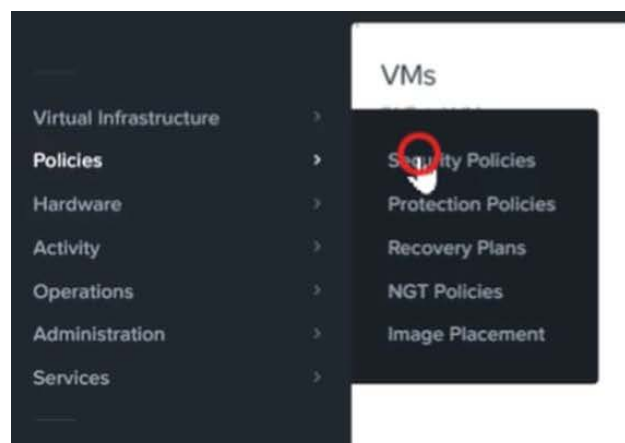
Configure the environment to satisfy this requirement.

Note: All other configurations not indicated must be left at their default values.

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

Correct Answer: A

To configure the environment to satisfy the requirement of implementing a security policy named Staging_Production, such that no VM in the Staging Environment can communicate with any VM in the production Environment, you need to do the following steps: Log in to Prism Central and go to Network > Security Policies > Create Security Policy. Enter Staging_Production as the name of the security policy and select Cluster A as the cluster. In the Scope section, select VMs as the entity type and add the VMs that belong to the Staging Environment and the Production Environment as the entities. You can use tags or categories to filter the VMs based on their environment. In the Rules section, create a new rule with the following settings: Direction: Bidirectional Protocol: Any Source: Staging Environment Destination: Production Environment Action: Deny Save the security policy and apply it to the cluster. This will create a security policy that will block any traffic between the VMs in the Staging Environment and the VMs in the Production Environment. You can verify that the security policy is working by trying to ping or access any VM in the Production Environment from any VM in the Staging Environment, or vice versa. You should not be able to do so.



Name

Purpose

Isolate This Category

From This Category

☐ Apply the isolation only within a subset of the data center

Advanced Configuration
 Policy Hit Logs ☐ Disabled



QUESTION 2

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 from Nutanix Portal. Power on the VM and install the latest Nutanix VirtIO drivers for Windows 10. You can

follow the instructions from Nutanix 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
```

Replace eth0 with the name of your network interface and 8 with the number of multiqueues that you want to enable. You can use `ipconfig /all` to 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"
```

```
}
```

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

remove the old disk

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

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

*

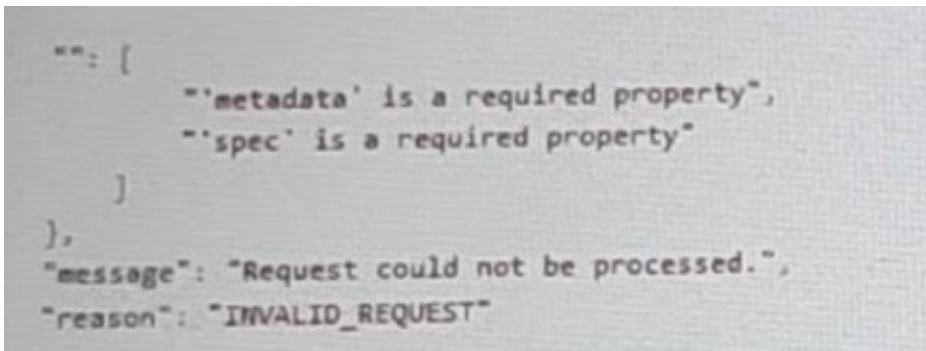
Disk Size: 50Gb

*

Cluster: Cluster A

*

Network: default- net



```
{
  "errors": [
    {
      "code": "INVALID_REQUEST",
      "message": "'metadata' is a required property",
      "reason": "INVALID_REQUEST"
    },
    {
      "code": "INVALID_REQUEST",
      "message": "'spec' is a required property",
      "reason": "INVALID_REQUEST"
    }
  ],
  "message": "Request could not be processed.",
  "reason": "INVALID_REQUEST"
}
```

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 default_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 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

Syslog 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

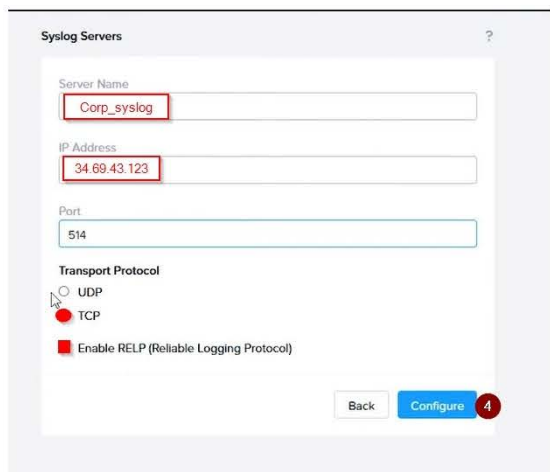
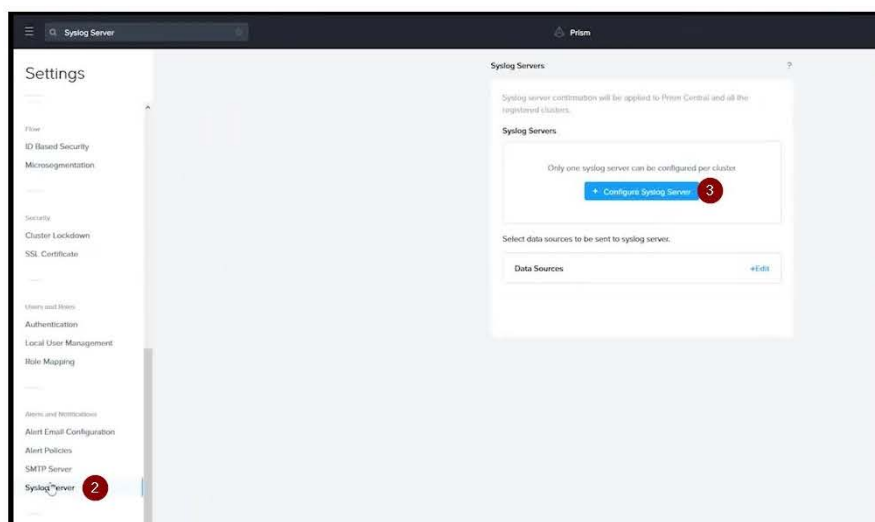
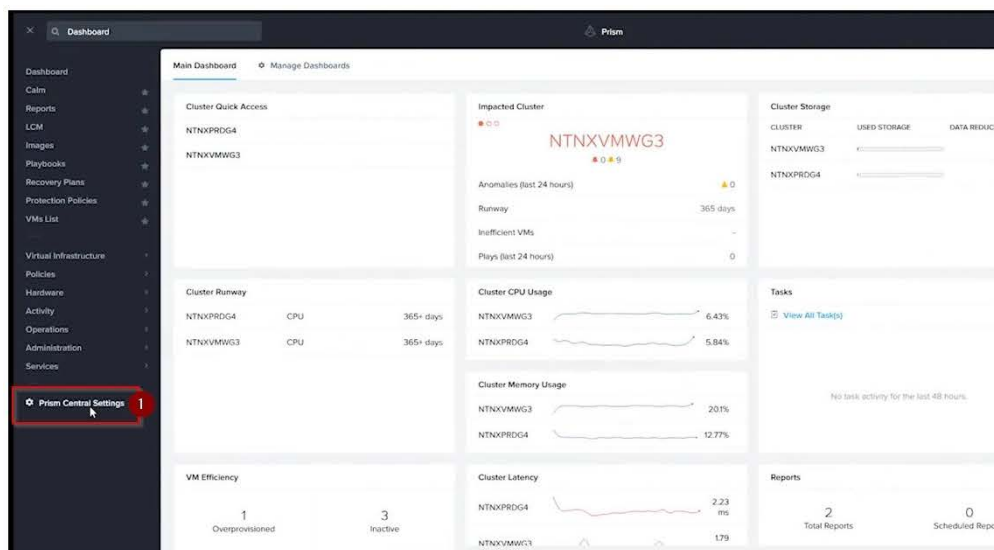
To configure the cluster to meet the requirements of the infosec team, you need to do the following steps:

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.



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

Syslog Servers

Data Sources and Respective Severity Level

<input checked="" type="checkbox"/> Module Name	Severity Level
<input checked="" type="checkbox"/> API Audit	<div>Select Severity Level</div> <div>0 - Emergency: system is unusable</div> <div>1 - Alert: action must be taken immediately</div> <div>2 - Critical: critical conditions</div> <div>3 - Error: error conditions</div> <div>4 - Warning: warning conditions</div> <div>5 - Notice: normal but significant condition</div> <div>6 - Informational: informational messages</div> <div>7 - Debug: debug-level messages</div>

| ☒ Audit | |
| ☒ Flow | |

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.

nccli

```
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 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 of 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 to `toappdev@cyberdyne.net` when completed.

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.

[Latest NCM-MCI-6.5 Dumps](#) [NCM-MCI-6.5 VCE Dumps](#) [NCM-MCI-6.5 Practice Test](#)