NCM-MCI-6.5$^{\text{Q\&As}}$

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

Pass NCM-MCI-6.5 Exam with 100% Guarantee

QUESTION 1

CORRECT TEXT

Task 16

Running NCC on a cluster prior to an upgrade results in the following output

FAIL: CVM System Partition /home usage at 93% (greater than threshold, 90%) Identify the CVM with the issue, remove the fil causing the storage bloat, and check the health again by running the individual disk usage health check only on the problematic CVM do not run NCC health check

Note: Make sure only the individual health check is executed from the affected node

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

Correct Answer: A

To identify the CVM with the issue, remove the file causing the storage bloat, and check the health again, 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 find the NCC health check output file from the list. You can use the date and time information to locate the file. The file name

should be something like ncc-output-YYYY-MM-DD-HH-MM-SS.log. Open the file and look for the line that says FAIL: CVM System Partition /home usage at 93% (greater than threshold, 90%). Note down the IP address of the CVM that has

this issue. It should be something like X.X.X.X.

Log in to the CVM using SSH or console with the username and password provided. Run the command du -sh /home/* to see the disk usage of each file and directory under /home. Identify the file that is taking up most of the space. It could

be a log file, a backup file, or a temporary file. Make sure it is not a system file or a configuration file that is needed by the CVM.

Run the command rm -f /home/ to remove the file causing the storage bloat. Replace with the actual name of the file. Run the command ncc health_checks hardware_checks disk_checks disk_usage_check -cvm_list=X.X.X.X to check the health again by running the individual disk usage health check only on the problematic CVM. Replace X.X.X.X with the IP address of the CVM that you noted down earlier.

Verify that the output shows PASS: CVM System Partition /home usage at XX% (less than threshold, 90%). This means that the issue has been resolved.

```
#access to CVM IP by Putty

allssh df -h #look for the path /dev/sdb3 and select the IP of the CVM ssh CVM_IP

ls

cd software_downloads

ls
```

```
cd nos

ls -l -h

rm files_name

df -h

ncc health_checks hardware_checks disk_checks disk_usage_check
```

QUESTION 2

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.

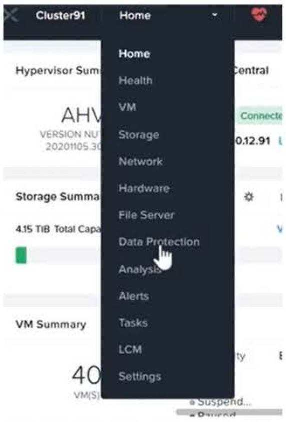
Click Next.

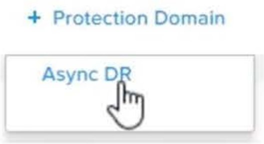
Select Mkt01 from the list of VMs and click Next. Select Schedule Based from the drop-down menu and enter 2 hours as the interval. Click Next.

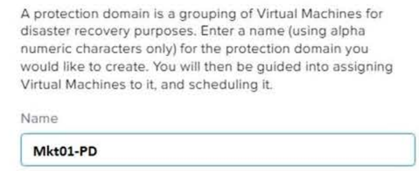
Select Remote Site from the drop-down menu and choose the remote site where you want to replicate the VM. Click Next.

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.

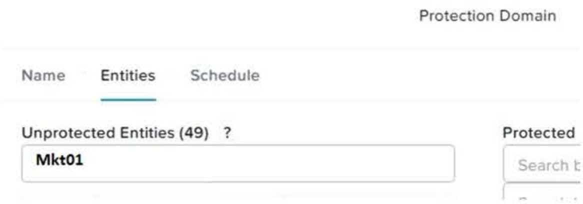





A protection domain is a grouping of Virtual Machines for disaster recovery purposes. Enter a name (using alpha numeric characters only) for the protection domain you would like to create. You will then be guided into assigning Virtual Machines to it, and scheduling it.

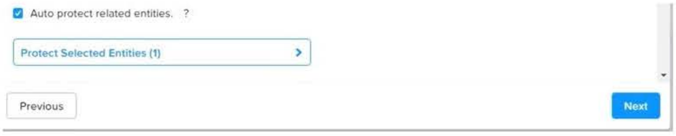
Name

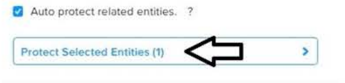
Mkt01-PD

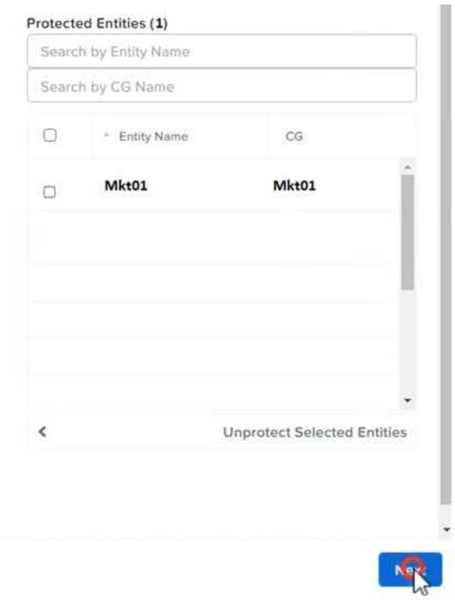


Unprotected Entities (49) ?

Mkt01


☑ Auto protect related entities. ?


☑ Auto protect related entities. ?

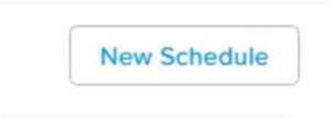


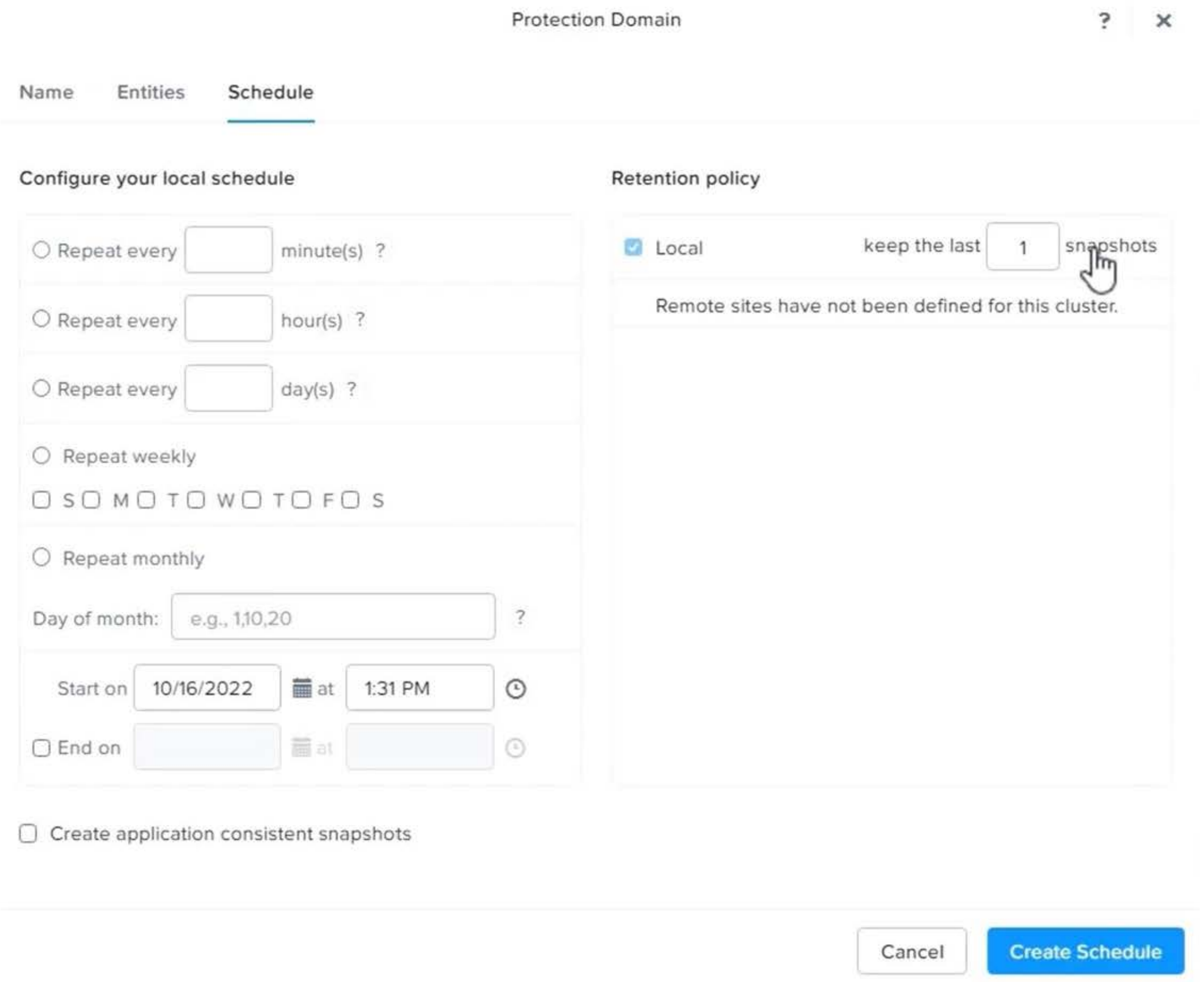
Protected Entities (1)

Search by Entity Name

Search by CG Name

□	Entity Name	CG
□	Mkt01	Mkt01





Protection Domain

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 3

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 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

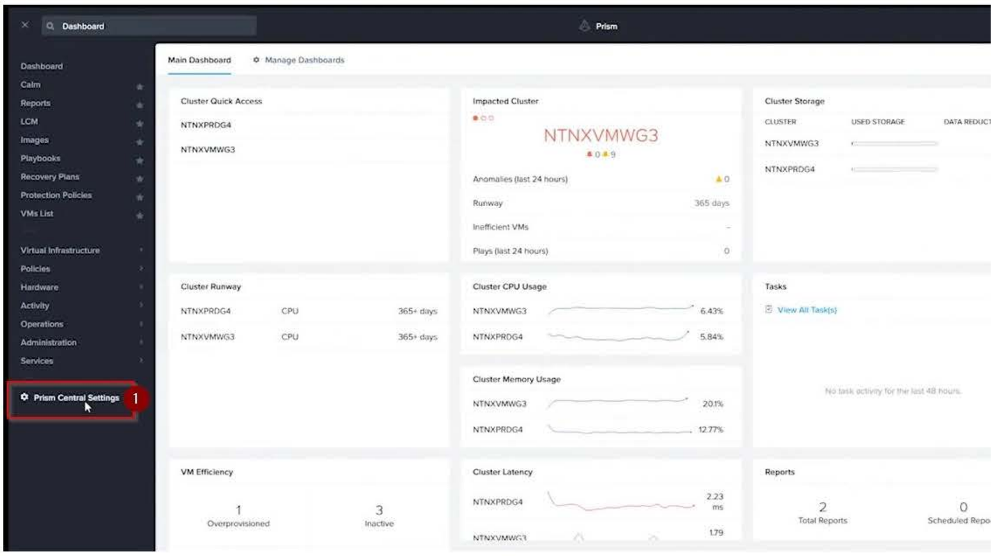
To configure the cluster to meet the requirements of the infosec team, you need to do the following steps:

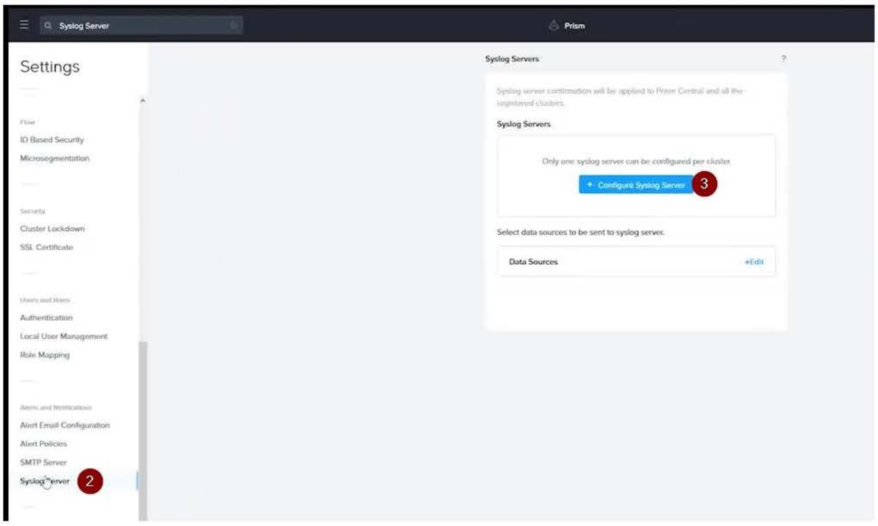
Log in to Prism Central and go to Network > Syslog Servers > Configure Syslog Server. Enter Corp_syslog as the Server Name, 34.69.43.123 as the IP Address, and 514 as the Port. Select TCP as the Transport Protocol and enable RELP

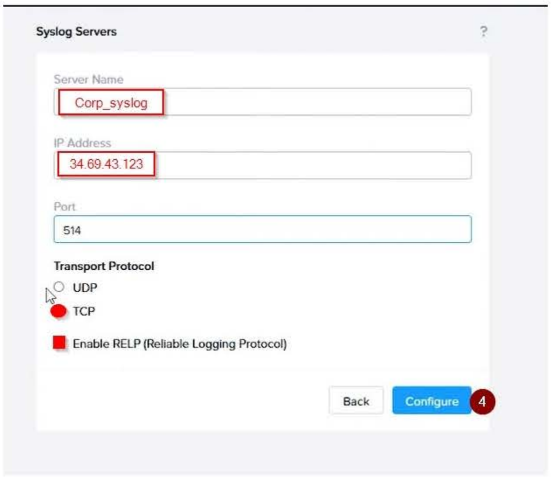
(Reliable Logging Protocol). This will create a syslog server with the highest reliability possible. Click Edit against Data Sources and select Cluster B as the cluster. Select API Requests and Replication as the data sources and set the log level

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

Server Name: Corp_syslog

IP Address: 34.69.43.123

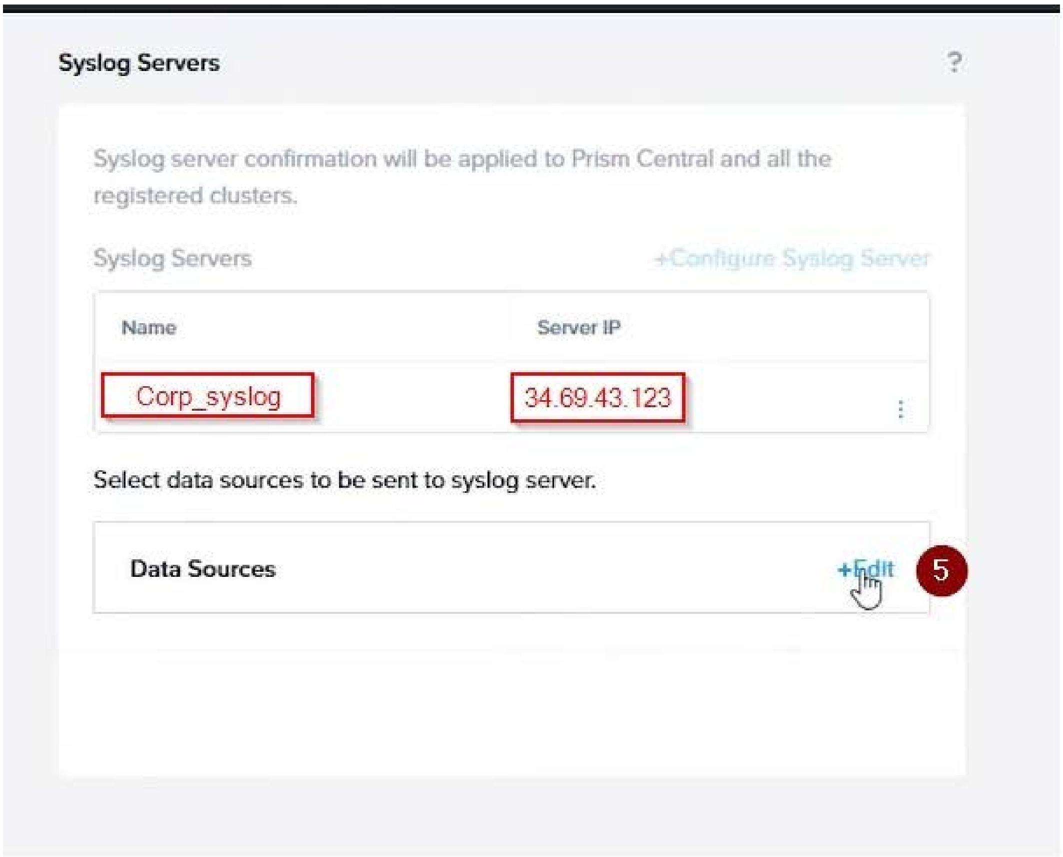
Port: 514

Transport Protocol

○ UDP

● TCP

☒ Enable RELP (Reliable Logging Protocol)



Syslog Servers

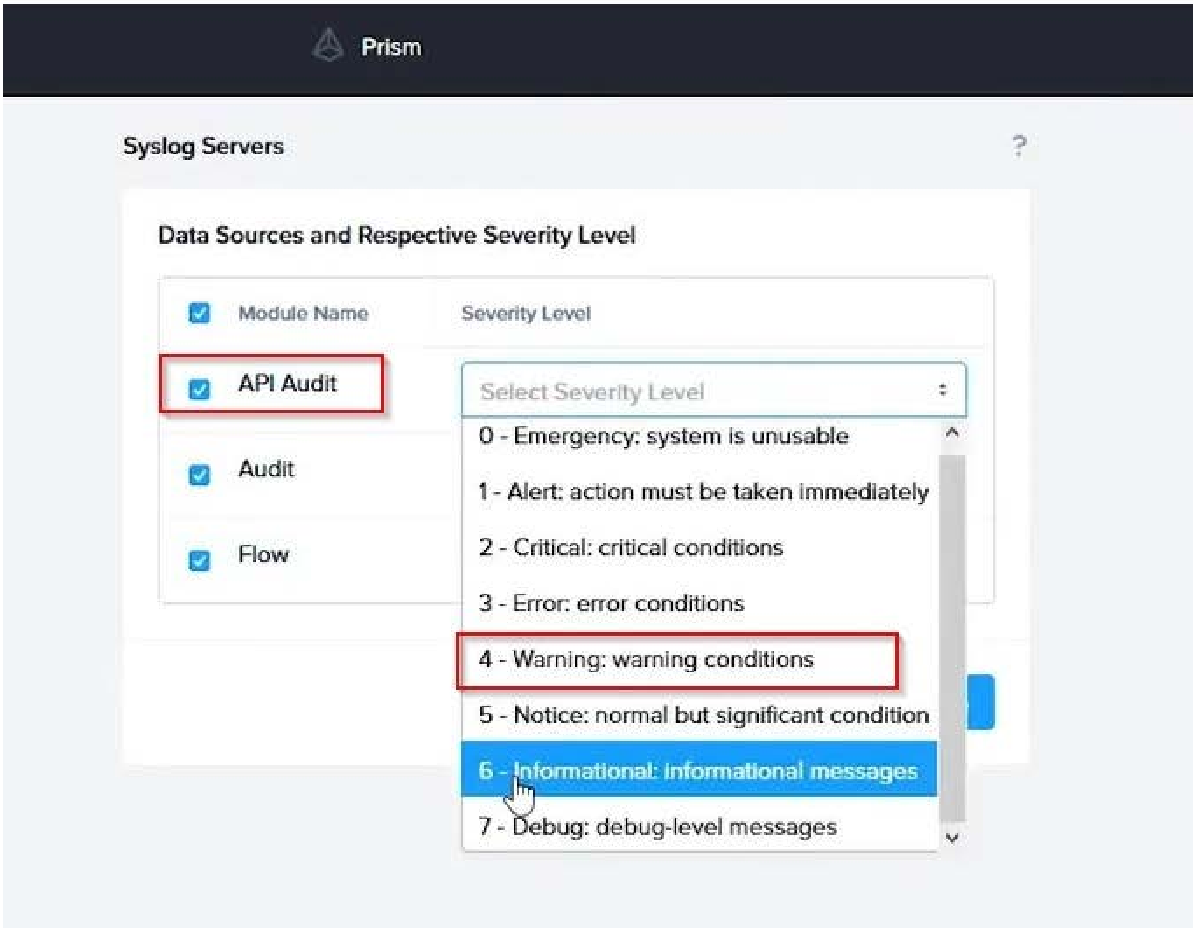
Syslog server confirmation will be applied to Prism Central and all the registered clusters.

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



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 5

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,

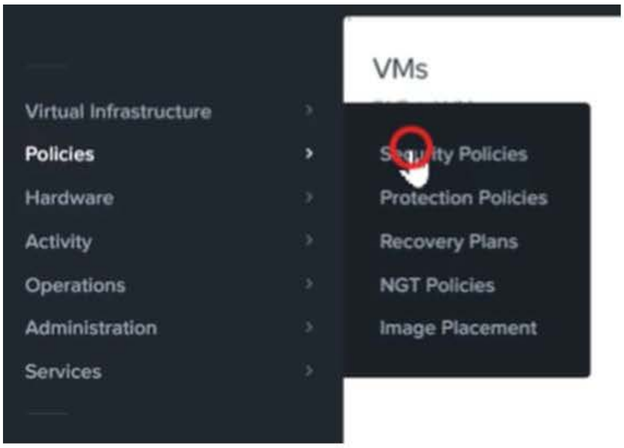
Configure the environment to satisfy this requirement.

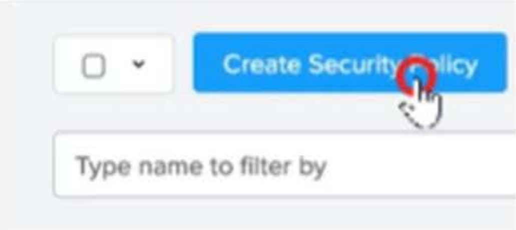
Note: All other configurations not indicated must be left at their default values.

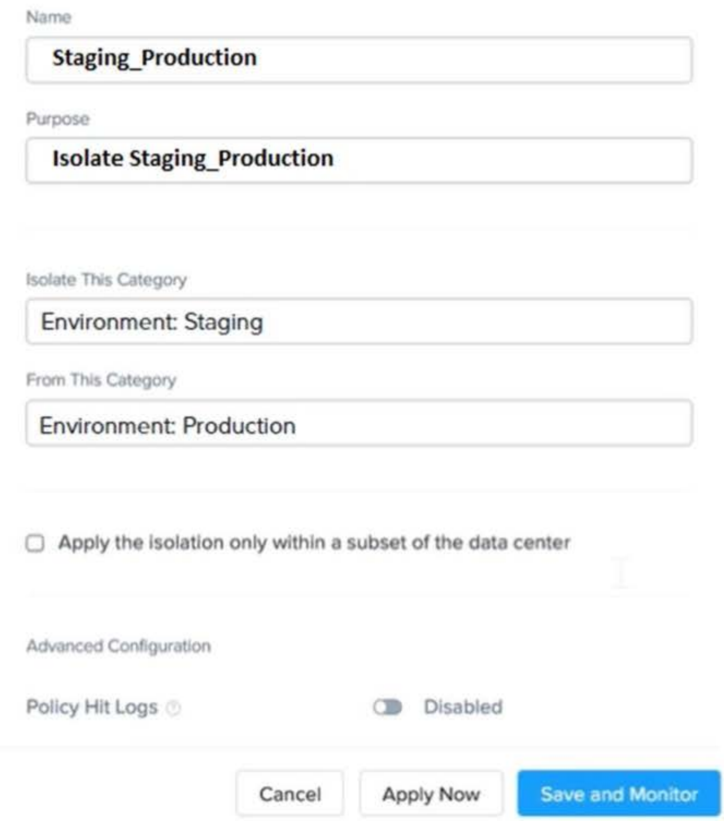
A. Answer: See the for step by step solution.

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
Staging_Production

Purpose
Isolate Staging_Production

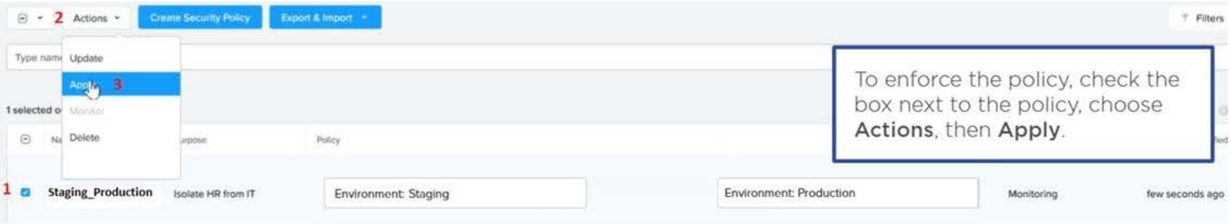
Isolate This Category
Environment: Staging

From This Category
Environment: Production

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

Advanced Configuration

Policy Hit Logs Disabled



☑ Staging_Production | Isolate HR from IT | Environment: Staging | Environment: Production | Monitoring | few seconds ago

To enforce the policy, check the box next to the policy, choose **Actions**, then **Apply**.