Number: NCM-MCI-6.5
Passing Score: 800
Time Limit: 120
File Version: 2.0

Exam Code: NCM-MCI-6.5

Exam Name: Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI) V6.5

Exam A

QUESTION 1

Task 6

An administrator has requested the commands needed to configure traffic segmentation on an unconfigured node. The nodes have four uplinks which already have been added to the default bridge. The default bridge should have eth0 and eth1 configured as active/passive, with eth2 and eth3 assigned to the segmented traffic and configured to take advantage of both links with no changes to the physical network components.

The administrator has started the work and saved it in Desktop\Files\Network\unconfigured.txt

Replacle any x in the file with the appropriate character or string Do not delete existing lines or add new lines.

Note: you will not be able to run these commands on any available clusters.

Unconfigured.txt

```
manage_ovs --bond_name brX-up --bond_mode xxxxxxxxxxx --interfaces ethX,ethX update_uplinks
manage_ovs --bridge_name brX-up --interfaces ethX,ethX --bond_name bond1 --bond_mode xxxxxxxxxxx update_uplinks
```

A. See the Explanation for step by step solution

Correct Answer: A

Section:

Explanation:

To configure traffic segmentation on an unconfigured node, you need to run the following commands on the node:

```
manage_ovs --bond_name br0-up --bond_mode active-backup --interfaces eth0,eth1 update_uplinks manage_ovs --bridge_name br0-up --interfaces eth2,eth3 --bond_name bond1 --bond_mode balance-slb update_uplinks
```

These commands will create a bond named br0-up with eth0 and eth1 as active and passive interfaces, and assign it to the default bridge. Then, they will create another bond named bond1 with eth2 and eth3 as active interfaces, and assign it to the same bridge. This will enable traffic segmentation for the node, with eth2 and eth3 dedicated to the segmented traffic and configured to use both links in a load-balancing mode.

I have replaced the x in the file Desktop\Files\Network\unconfigured.txt with the appropriate character or string for you. You can find the updated file in Desktop\Files\Network\configured.txt.

```
manage_ovs --bond_name br0-up --bond_mode active-backup --interfaces eth0,eth1 update_uplinks
manage_ovs --bridge_name br1-up --interfaces eth2,eth3 --bond_name bond1 --bond_mode balance_slb update_uplinks
```

https://portal.nutanix.com/page/documents/solutions/details?targetId=BP-2071-AHV-Networking:ovs-command-line-configuration.html

QUESTION 2

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. See the Explanation for step by step solution

Correct Answer: A

Section:

Explanation:

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.

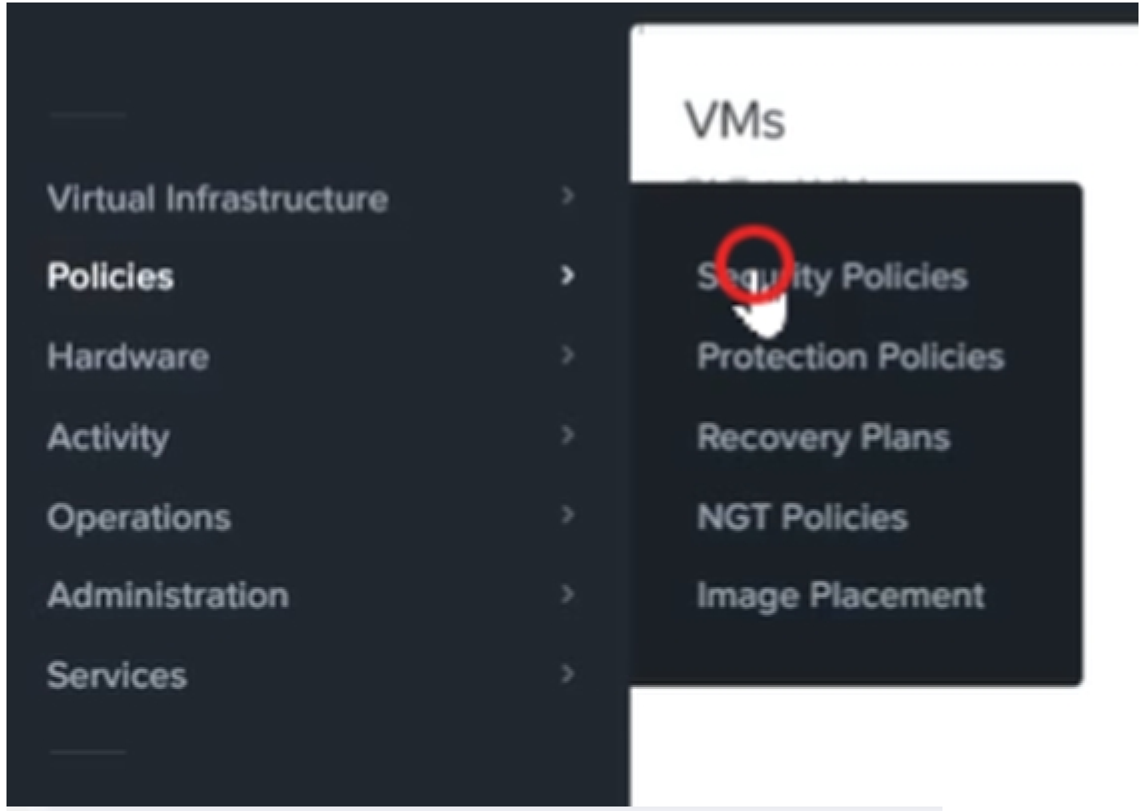
In the Rules section, create a new rule with the following settings:

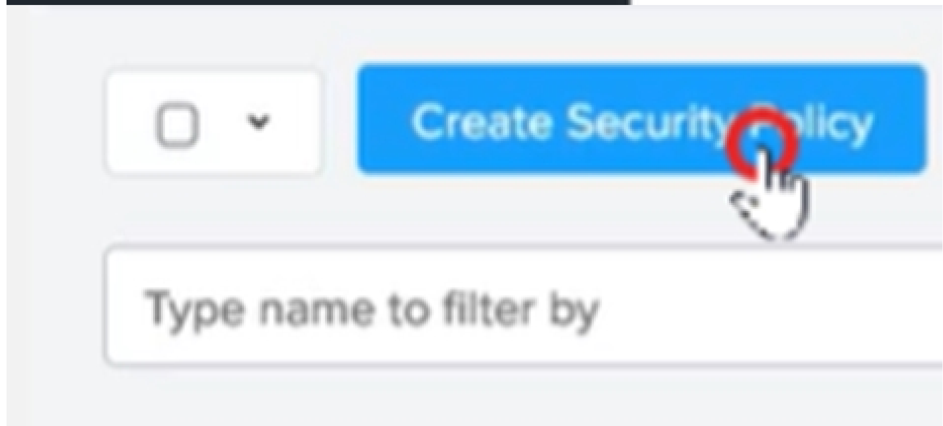
Direction: Bidirectional

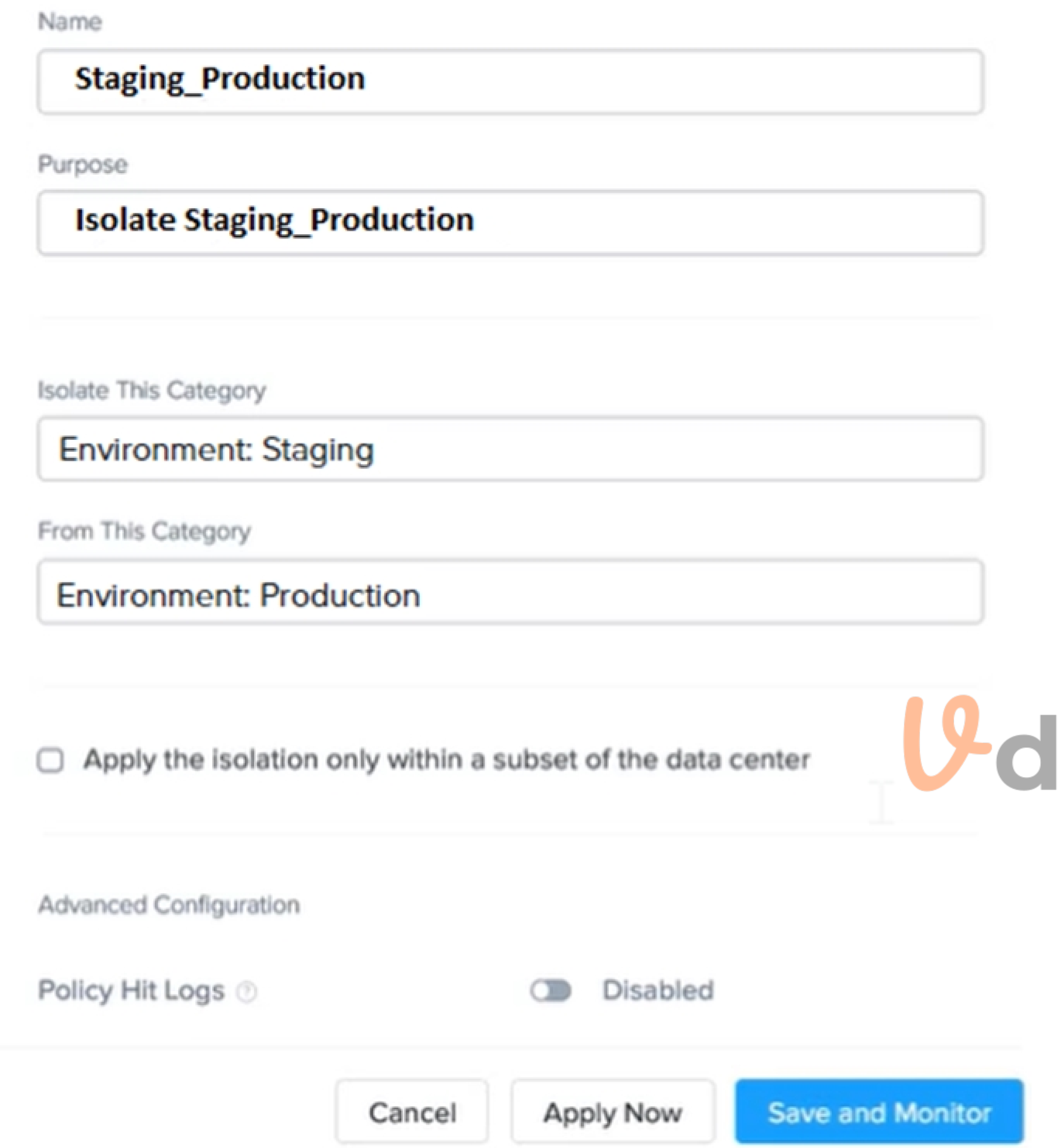
Protocol: Any

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

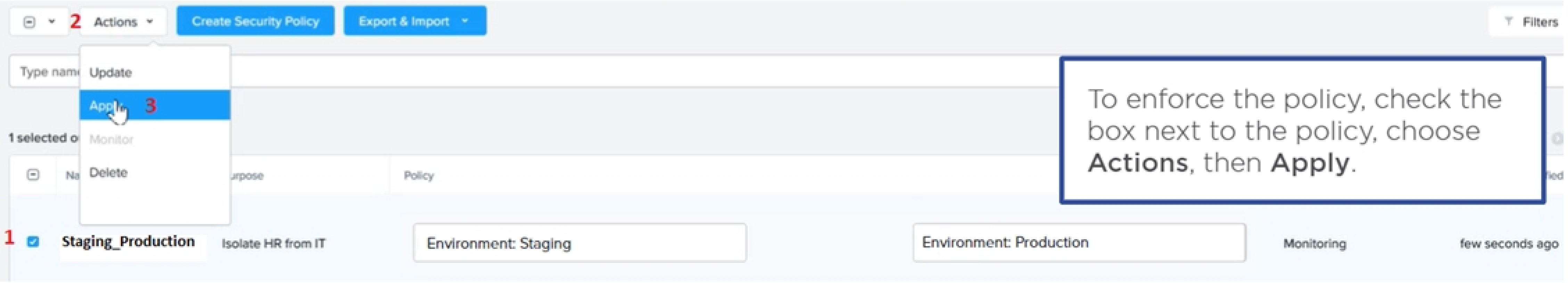
From This Category

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**.

QUESTION 3

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. See the Explanation for step by step solution

Correct Answer: A

Section:

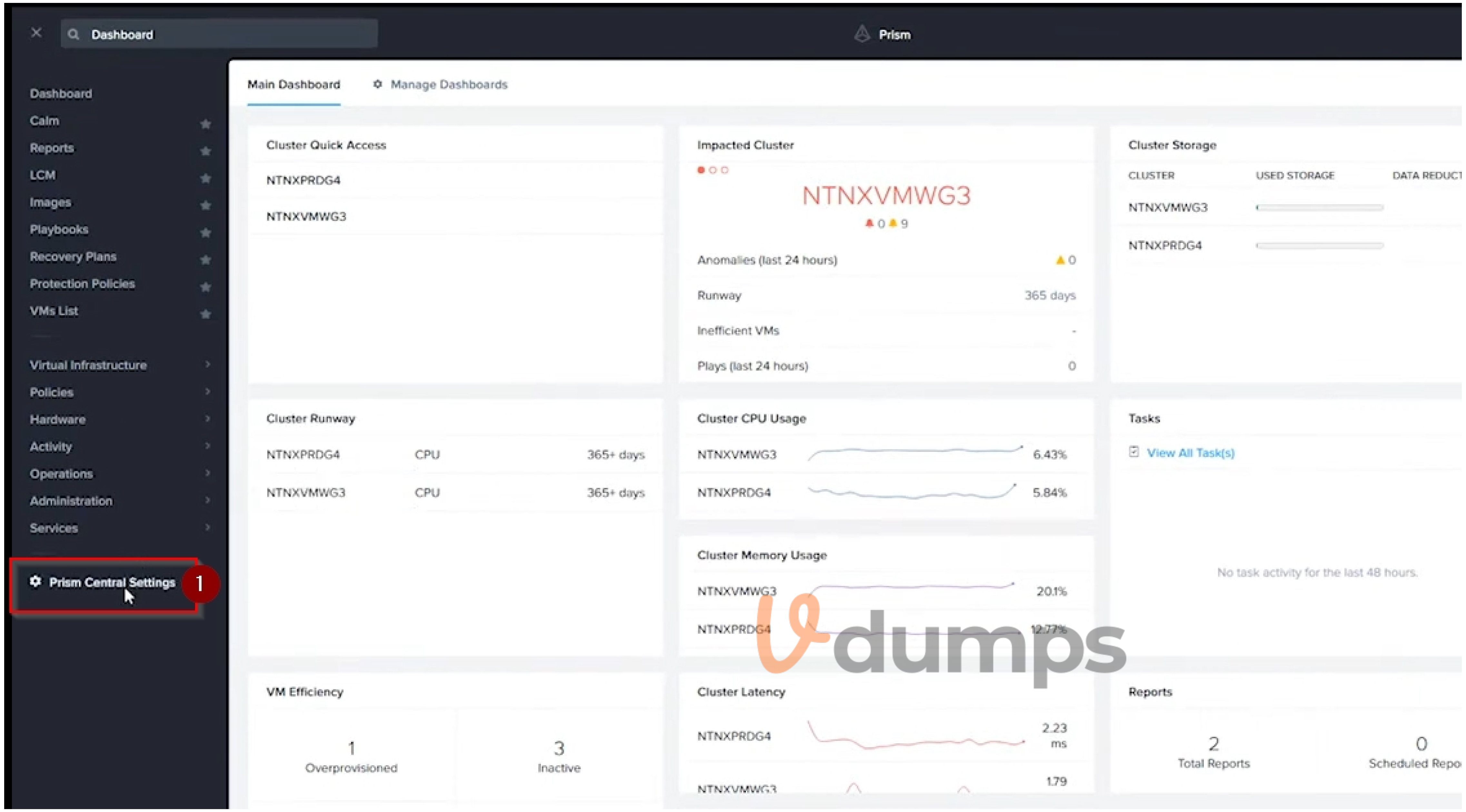
Explanation:

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.



Cluster Quick Access

NTNXPRDG4

NTNXVMWG3

Impacted Cluster

NTNXVMWG3

▲0 ▲9

Anomalies (last 24 hours)	▲0
Runway	365 days
Inefficient VMs	-
Plays (last 24 hours)	0

Cluster Storage

CLUSTER	USED STORAGE	DATA REDUCT
NTNXVMWG3		
NTNXPRDG4		

Cluster Runway

NTNXPRDG4	CPU	365+ days
NTNXVMWG3	CPU	365+ days

Cluster CPU Usage

NTNXVMWG3	6.43%
NTNXPRDG4	5.84%

Tasks

View All Task(s)

No task activity for the last 48 hours.

Cluster Memory Usage

NTNXVMWG3	20.1%
NTNXPRDG4	12.77%

VM Efficiency

1 Overprovisioned

3 Inactive

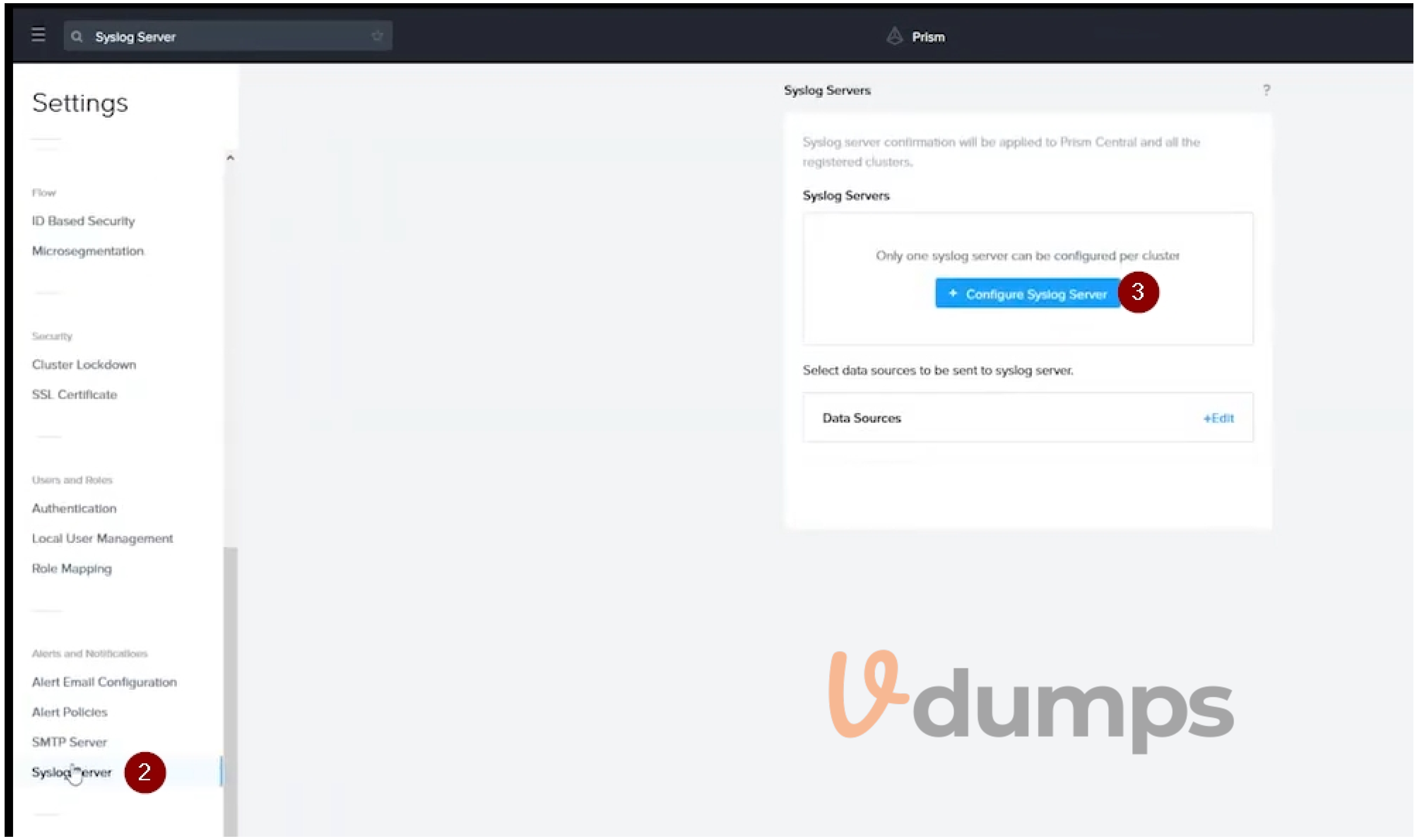
Cluster Latency

NTNXPRDG4	2.23 ms
NTNXVMWG3	1.79

Reports

2 Total Reports

0 Scheduled Repo

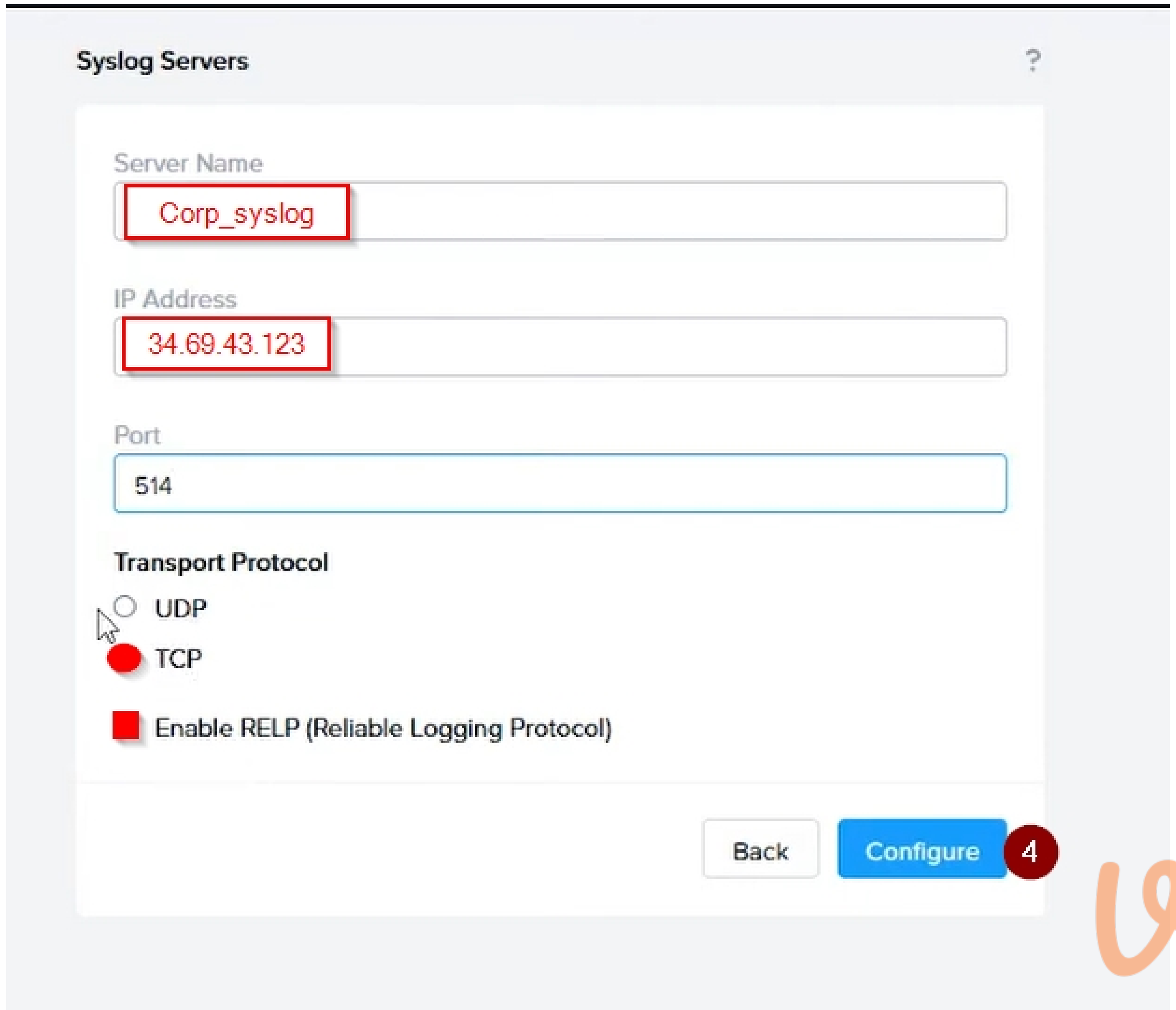


Syslog server confirmation will be applied to Prism Central and all the registered clusters.

Syslog Servers

Only one syslog server can be configured per cluster

Select data sources to be sent to syslog server.



Syslog Servers

Server Name: Corp_syslog

IP Address: 34.69.43.123

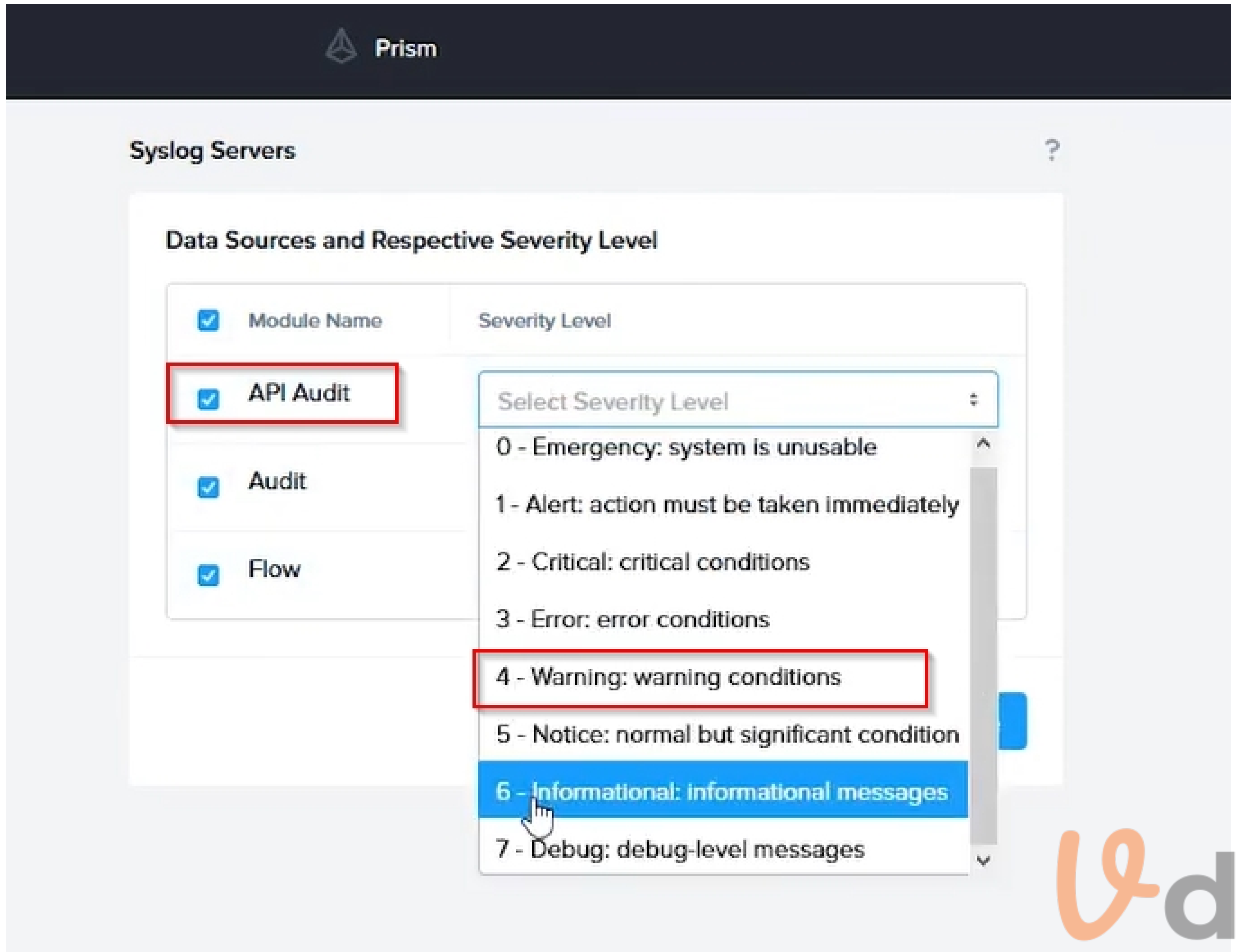
Port: 514

Transport Protocol

○ UDP

● TCP

☑ Enable RELP (Reliable Logging Protocol)


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
<ncli> rsyslog-config set-status enable=false
<ncli> rsyslog-config add-server name=Corp_Syslog ip-address=34.69.43.123 port=514 network-protocol=tdp relp-enabled=false
<ncli> rsyslog-config add-module server-name= Corp_Syslog module-name=APLOS level=INFO
<ncli> rsyslog-config add-module server-name= Corp_Syslog module-name=CEREBRO level=INFO
<ncli> rsyslog-config set-status enable=true
```

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

QUESTION 4

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 the default password.

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. See the Explanation for step by step solution

Correct Answer: A

Section:

Explanation:

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=<host id> enable-maintenance-mode=false
```

You can determine the host ID by using ncli host ls.

See the troubleshooting topics related to failed cluster services in the Advanced Administration Guide available from the Nutanix Portal's Software Documentation page. (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

Update the default password for the root user 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.

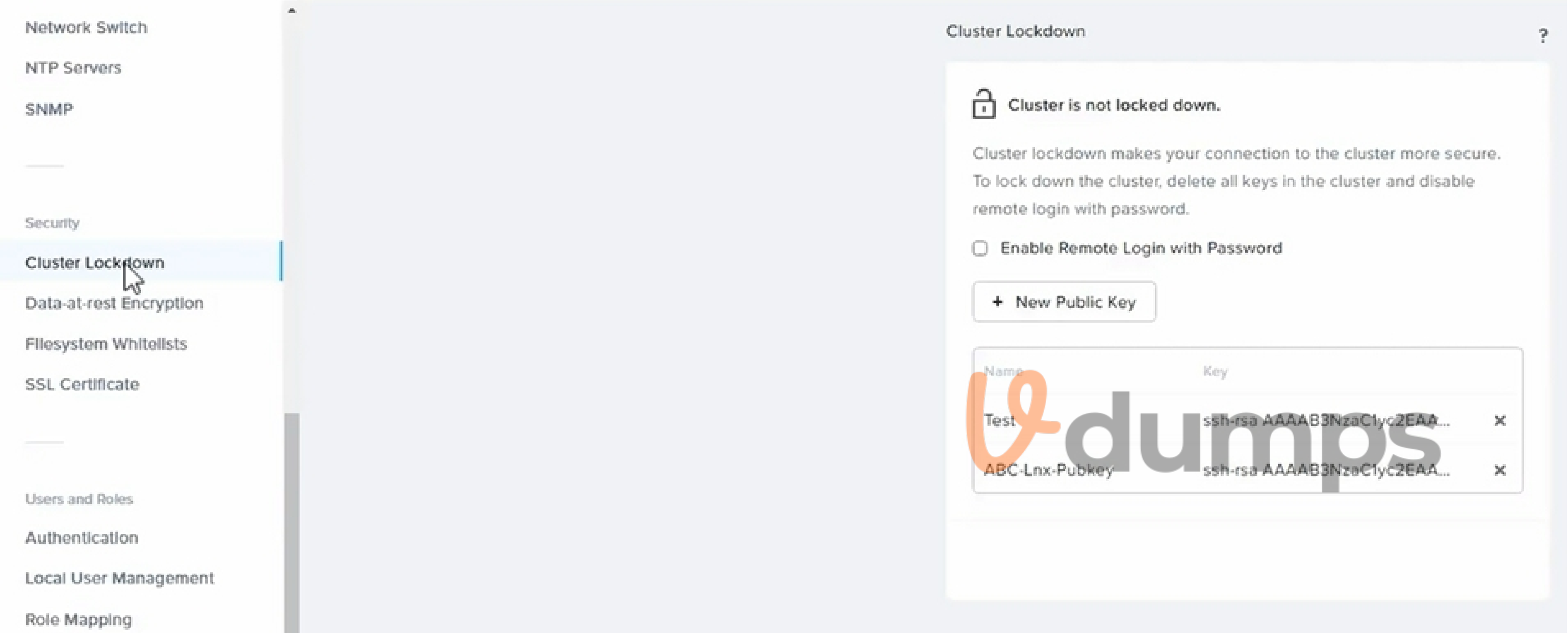
```
ncli cluster edit-hypervisor-security-params enable-aide=true
ncli cluster edit-hypervisor-security-params schedule=weekly
```

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



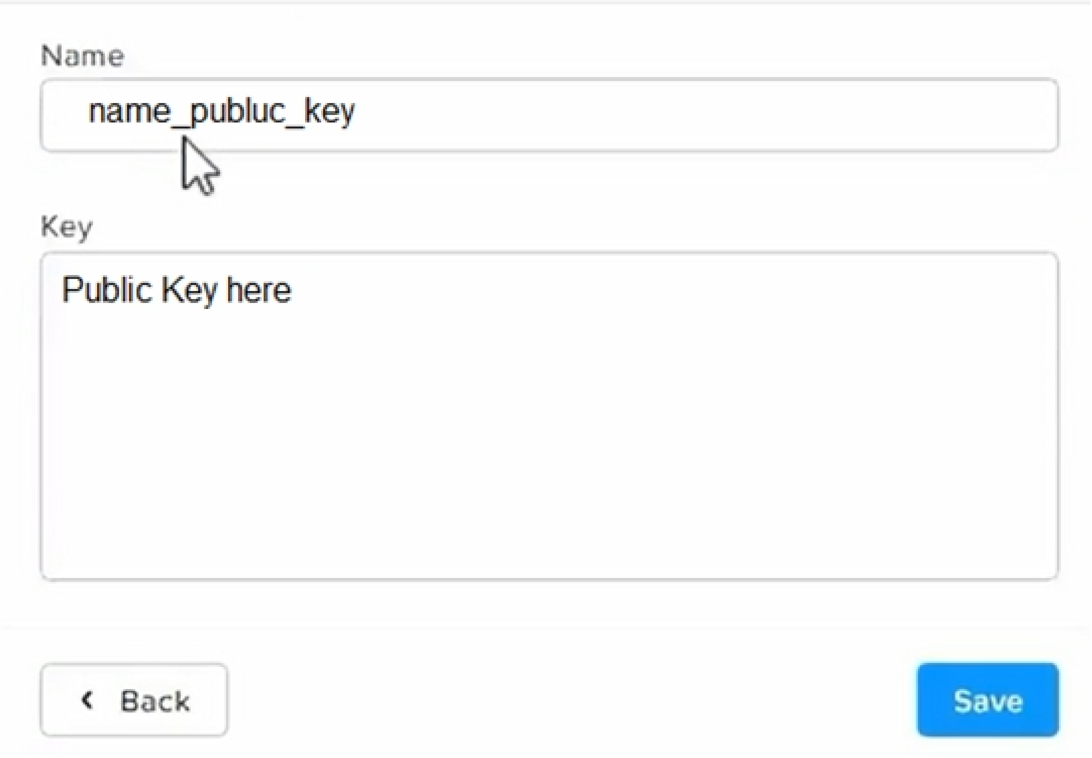
Cluster is not locked down.

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...	×

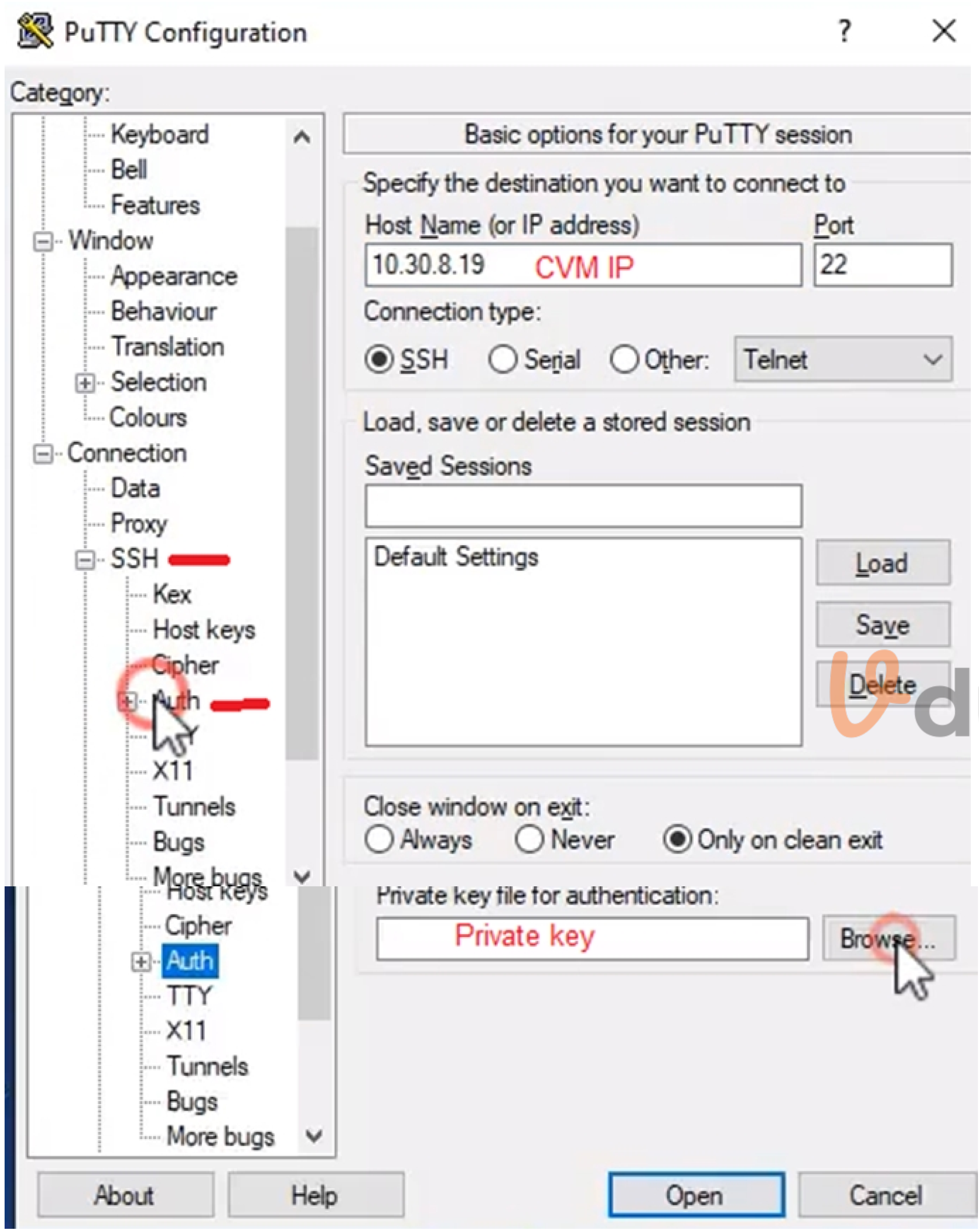


Name

name_publuc_key

Key

Public Key here



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 10.30.8.19 CVM IP

Port: 22

Connection type: ● SSH ○ Serial ○ Other: Telnet

Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

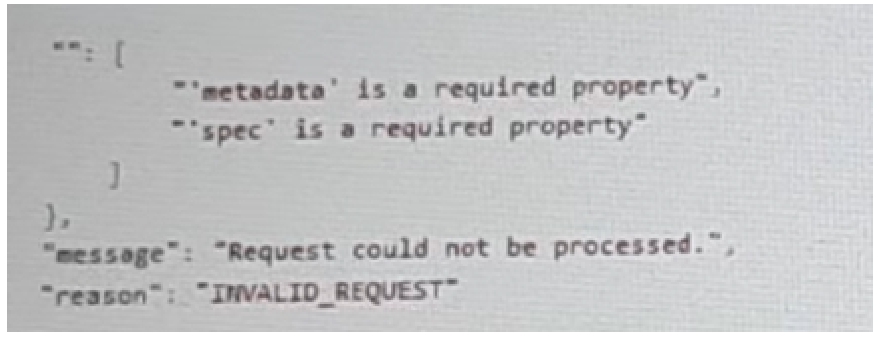
Private key file for authentication: Private key

QUESTION 5

Task 10

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

* VM specifications:



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

* 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. See the Explanation for step by step solution

Correct Answer: A
Section:
Explanation:
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'
}
}
```

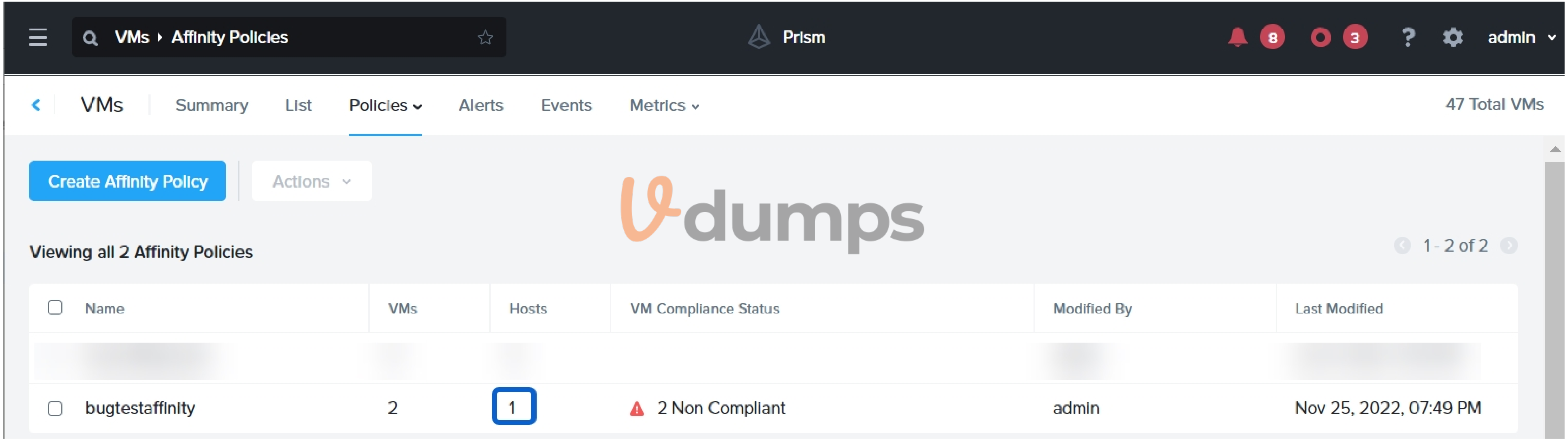
https://www.nutanix.dev/2019/08/26/post-a-package-building-your-first-nutanix-rest-api-post-request/
Reference

QUESTION 6
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. See the Explanation for step by step solution

Correct Answer: A
Section:
Explanation:
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



Viewing all 2 Affinity Policies

□ Name	VMs	Hosts	VM Compliance Status	Modified By	Last Modified
[redacted]	[redacted]	[redacted]		[redacted]	[redacted]
□ bugtestaffinity	2	1	⚠ 2 Non Compliant	admin	Nov 25, 2022, 07:49 PM

QUESTION 7
Task 12
An administrator needs to create a report named VMs_Power_State that lists the VMs in the cluster and their basic details including the power state for the last month.
No other entities should be included in the report.
<a target='_blank' href='mailto:admin@syberdyne.net'>The report should run monthly and should send an email to admin@syberdyne.net when it runs.</a>
Generate an instance of the report named VMs_Power_State as a CSV and save the zip file as Desktop\Files\VMs_Power_state.zip
Note: Make sure the report and zip file are named correctly. The SMTP server will not be configured.

A. See the Explanation for step by step solution

Correct Answer: A
Section:
Explanation:

To create a report named VMs_Power_State that lists the VMs in the cluster and their basic details including the power state for the last month, 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 VMs_Power_State 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 VM. Click Next.

Under the Custom Columns option, add the following variables: Name, Cluster Name, vCPUs, Memory, Power State. Click Next.

Under the Time Period option, select Last Month. Click Next.

Under the Report Settings option, select Monthly from the Schedule drop-down menu. Enter admin@syberdyne.net as the Email Recipient. Select CSV as the Report Output Format. Click Next.

Review the report details and click Finish.

To generate an instance of the report named VMs_Power_State as a CSV and save the zip file as Desktop\Files\VMs_Power_state.zip, you can follow these steps:

Log in to Prism Central and click on Operations on the left menu.

Select Reports from the drop-down menu and find the VMs_Power_State report from the list. Click on Run Now.

Wait for the report to be generated and click on Download Report. Save the file as Desktop\Files\VMs_Power_state.zip.

1. Open the Report section on Prism Central (Operations > Reports)
2. Click on the New Report button to start the creation of your custom report
3. Under the Custom Views section, select Data Table
4. Provide a title to your custom report, as well as a description if required.
5. Under the Entity Type option, select VM
6. This report can include all as well as a selection of the VMs
7. Click on the Custom Columns option and add the below variables:

a. Name - Name of the listed Virtual Machine

b. vCPUs - A combination of the vCores and vCPU's assigned to the Virtual Machine

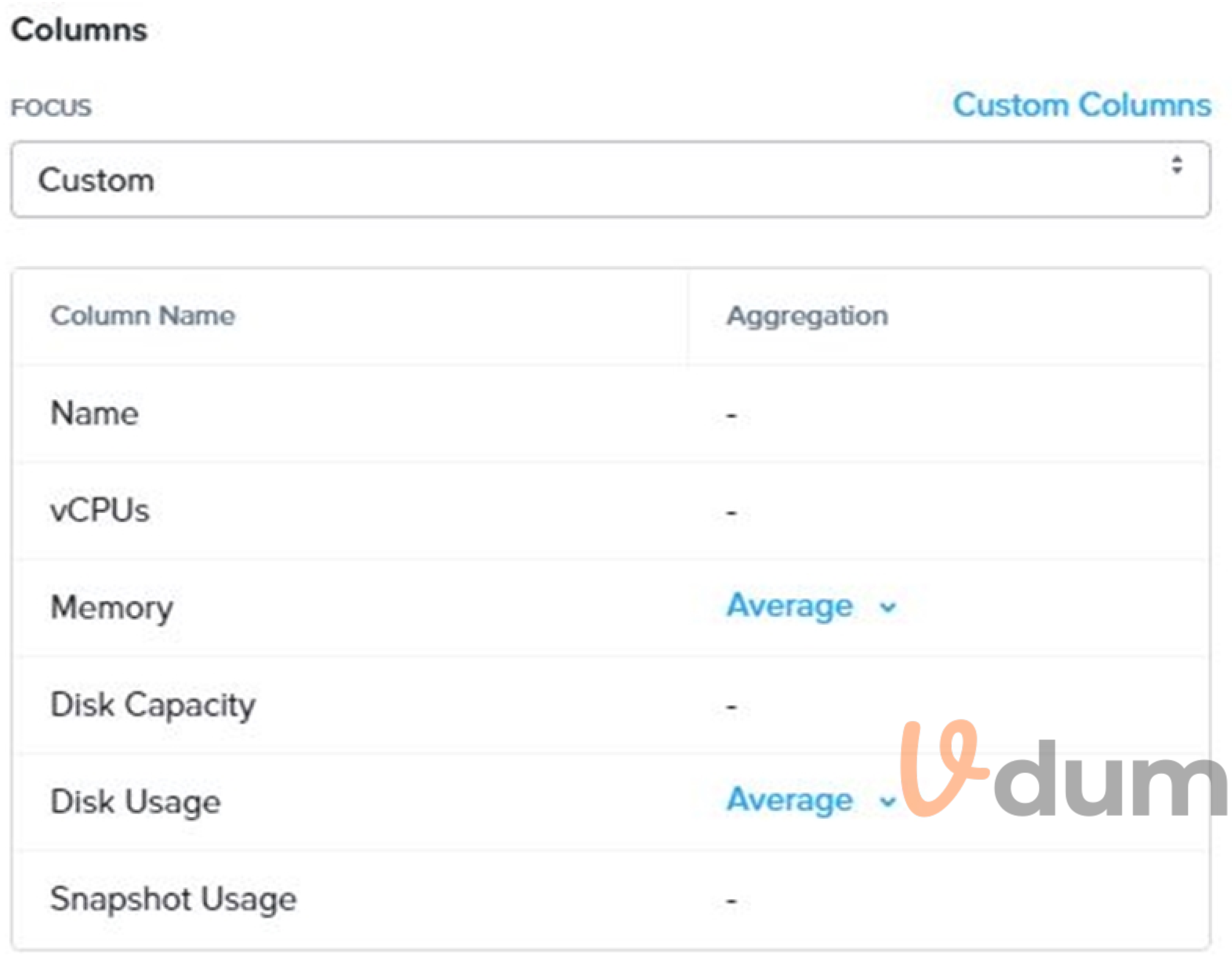
c. Memory - Amount of memory assigned to the Virtual Machine

d. Disk Capacity - The total amount of assigned virtual disk capacity

e. Disk Usage - The total used virtual disk capacity

f. Snapshot Usage - The total amount of capacity used by snapshots (Excluding Protection Domain snapshots)

8. Under the Aggregation option for Memory and Disk Usage accept the default Average option



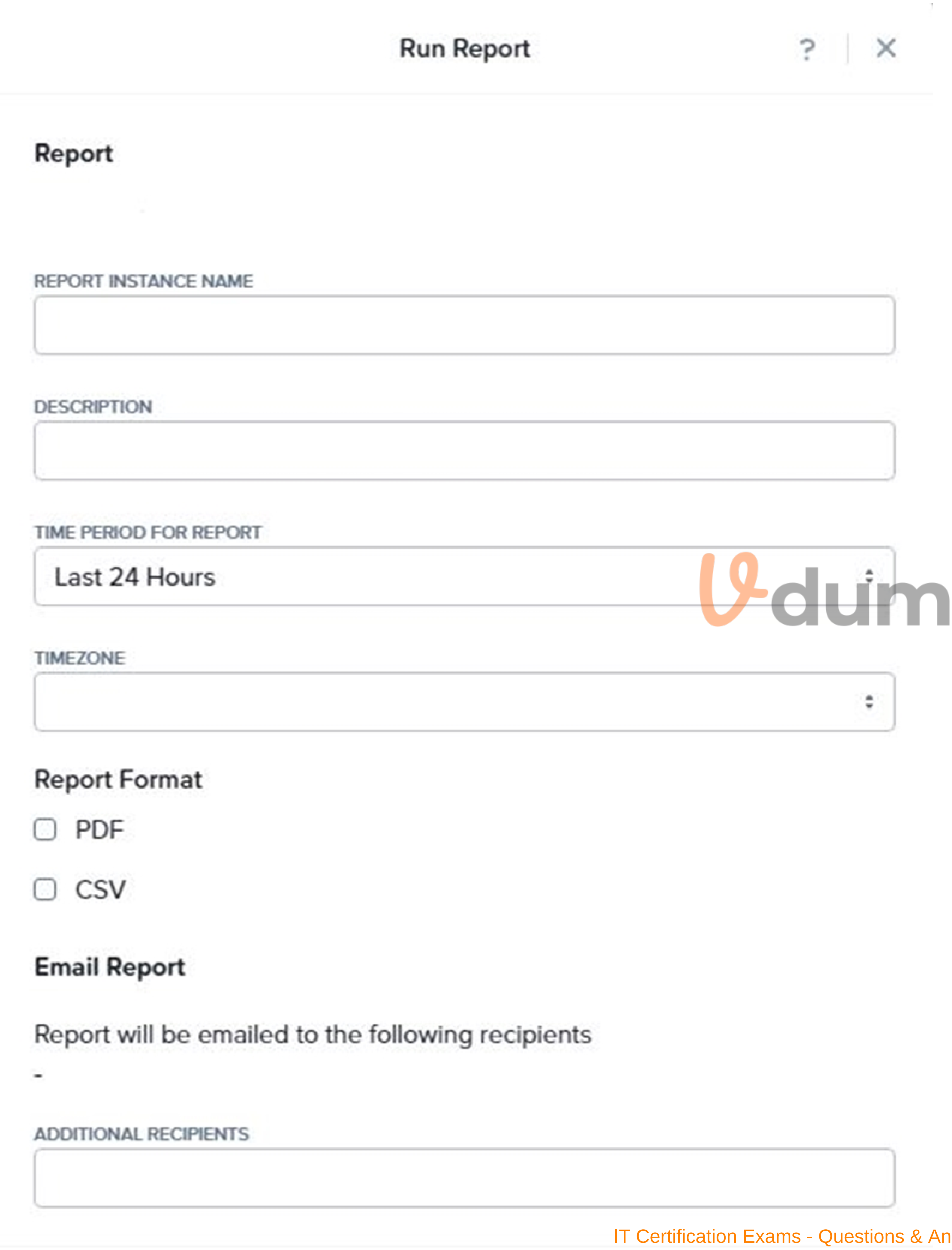
Columns

FOCUS

Custom

Column Name	Aggregation
Name	-
vCPUs	-
Memory	Average ⌄
Disk Capacity	-
Disk Usage	Average ⌄
Snapshot Usage	-

9. Click on the Add button to add this custom selection to your report
10. Next click on the Save and Run Now button on the bottom right of the screen
11. Provide the relevant details on this screen for your custom report:



Run Report

Report

REPORT INSTANCE NAME

DESCRIPTION

TIME PERIOD FOR REPORT

Last 24 Hours

TIMEZONE

Report Format

□ PDF

□ CSV

Email Report

Report will be emailed to the following recipients

-

ADDITIONAL RECIPIENTS

12. You can leave the Time Period For Report variable at the default of Last 24 Hours
13. Specify a report output of preference (PDF or CSV) and if required Additional Recipients for this report to be mailed to. The report can also simply be downloaded after this creation and initial run if required
14. Below is an example of this report in a CSV format:

QUESTION 8

Task 12

An administrator needs to create a report named VMs_Power_State that lists the VMs in the cluster and their basic details including the power state for the last month.

No other entities should be included in the report.

<a target='_blank' href='mailto:admin@syberdyne.net'>The report should run monthly and should send an email to admin@syberdyne.net when it runs.</a>

Generate an instance of the report named VMs_Power_State as a CSV and save the zip file as Desktop\Files\VMs_Power_state.zip

Note: Make sure the report and zip file are named correctly. The SMTP server will not be configured.

A. See the Explanation for step by step solution

Correct Answer: A

Section:

Explanation:

To create a report named VMs_Power_State that lists the VMs in the cluster and their basic details including the power state for the last month, 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 VMs_Power_State 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 VM. Click Next.

Under the Custom Columns option, add the following variables: Name, Cluster Name, vCPUs, Memory, Power State. Click Next.

Under the Time Period option, select Last Month. Click Next.

Under the Report Settings option, select Monthly from the Schedule drop-down menu. Enter admin@syberdyne.net as the Email Recipient. Select CSV as the Report Output Format. Click Next.

Review the report details and click Finish.

To generate an instance of the report named VMs_Power_State as a CSV and save the zip file as Desktop\Files\VMs_Power_state.zip, you can follow these steps:

Log in to Prism Central and click on Operations on the left menu.

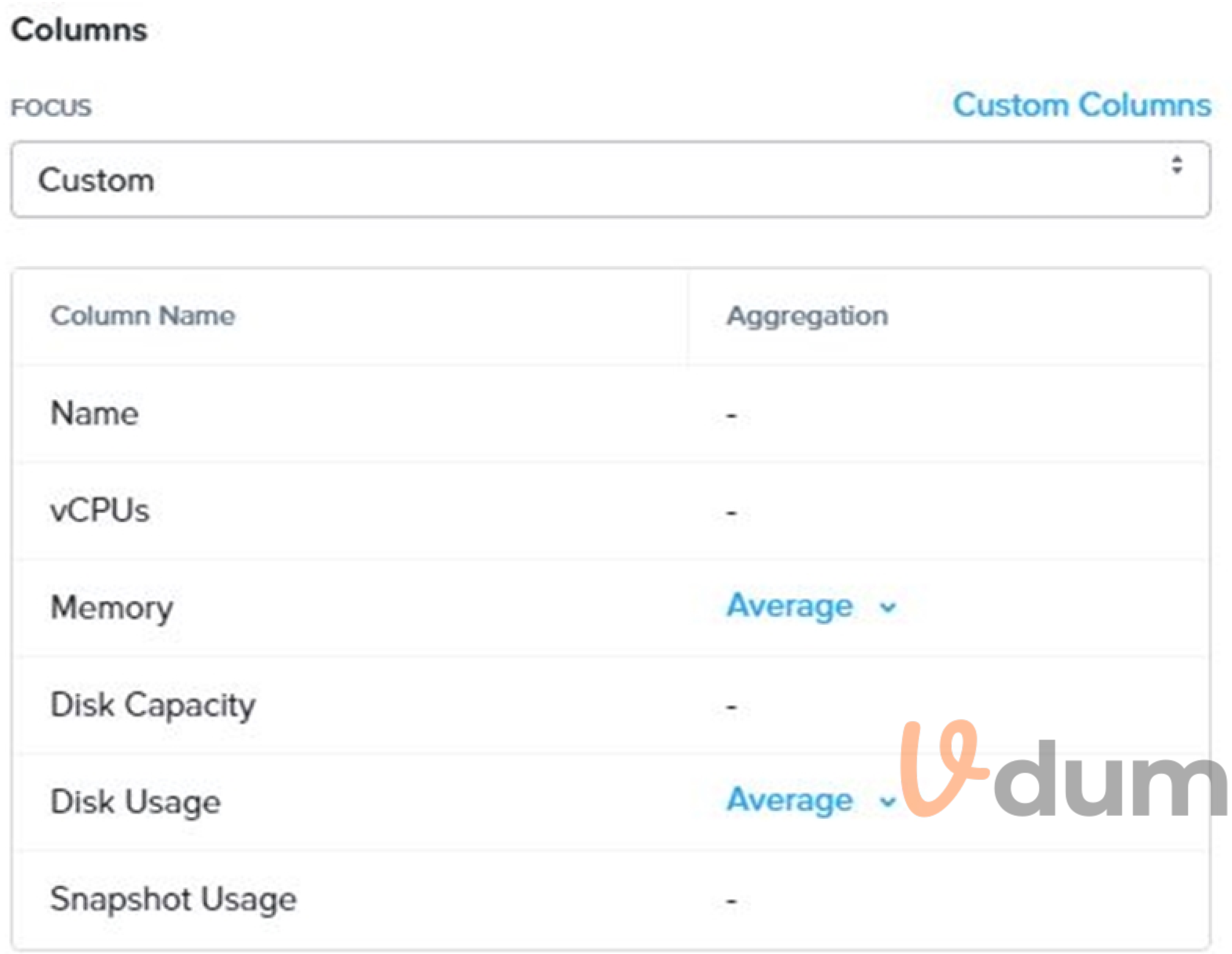
Select Reports from the drop-down menu and find the VMs_Power_State report from the list. Click on Run Now.

Wait for the report to be generated and click on Download Report. Save the file as Desktop\Files\VMs_Power_state.zip.

1. Open the Report section on Prism Central (Operations > Reports)
2. Click on the New Report button to start the creation of your custom report
3. Under the Custom Views section, select Data Table
4. Provide a title to your custom report, as well as a description if required.
5. Under the Entity Type option, select VM
6. This report can include all as well as a selection of the VMs
7. Click on the Custom Columns option and add the below variables:

a. Name - Name of the listed Virtual Machine
b. vCPUs - A combination of the vCores and vCPU's assigned to the Virtual Machine
c. Memory - Amount of memory assigned to the Virtual Machine
d. Disk Capacity - The total amount of assigned virtual disk capacity
e. Disk Usage - The total used virtual disk capacity
f. Snapshot Usage - The total amount of capacity used by snapshots (Excluding Protection Domain snapshots)

8. Under the Aggregation option for Memory and Disk Usage accept the default Average option



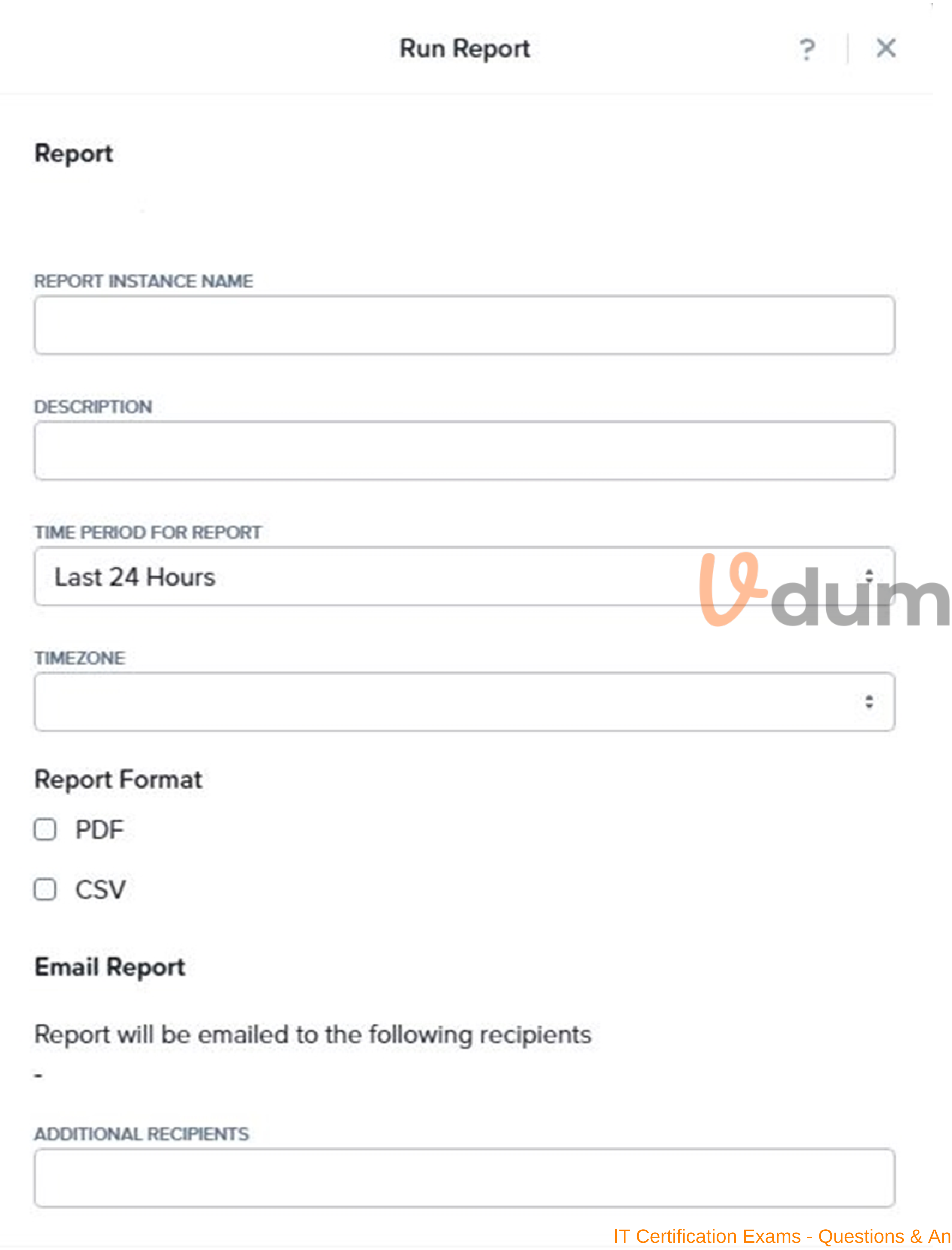
Columns

FOCUS Custom Columns

Custom

Column Name	Aggregation
Name	-
vCPUs	-
Memory	Average ⌄
Disk Capacity	-
Disk Usage	Average ⌄
Snapshot Usage	-

9. Click on the Add button to add this custom selection to your report
10. Next click on the Save and Run Now button on the bottom right of the screen
11. Provide the relevant details on this screen for your custom report:



Run Report

Report

REPORT INSTANCE NAME

DESCRIPTION

TIME PERIOD FOR REPORT

Last 24 Hours

TIMEZONE

Report Format

□ PDF

□ CSV

Email Report

Report will be emailed to the following recipients

-

ADDITIONAL RECIPIENTS

12. You can leave the Time Period For Report variable at the default of Last 24 Hours
13. Specify a report output of preference (PDF or CSV) and if required Additional Recipients for this report to be mailed to. The report can also simply be downloaded after this creation and initial run if required
14. Below is an example of this report in a CSV format:

QUESTION 9

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. See the Explanation for step by step solution

Correct Answer: A

Section:

Explanation:

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.

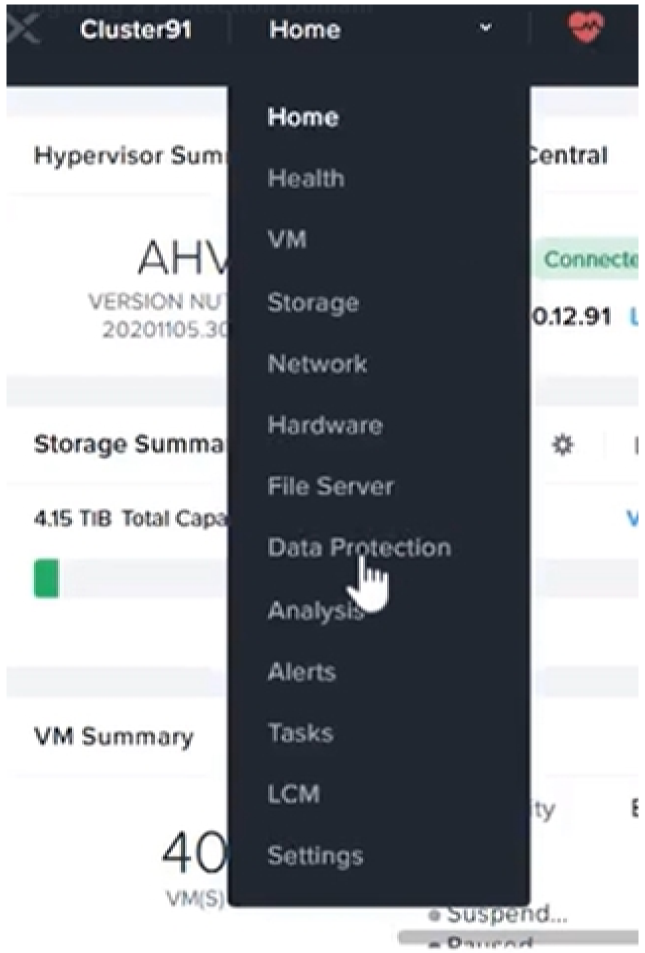
Select Schedule Based from the drop-down menu and enter 2 hours as the interval. Click Next.

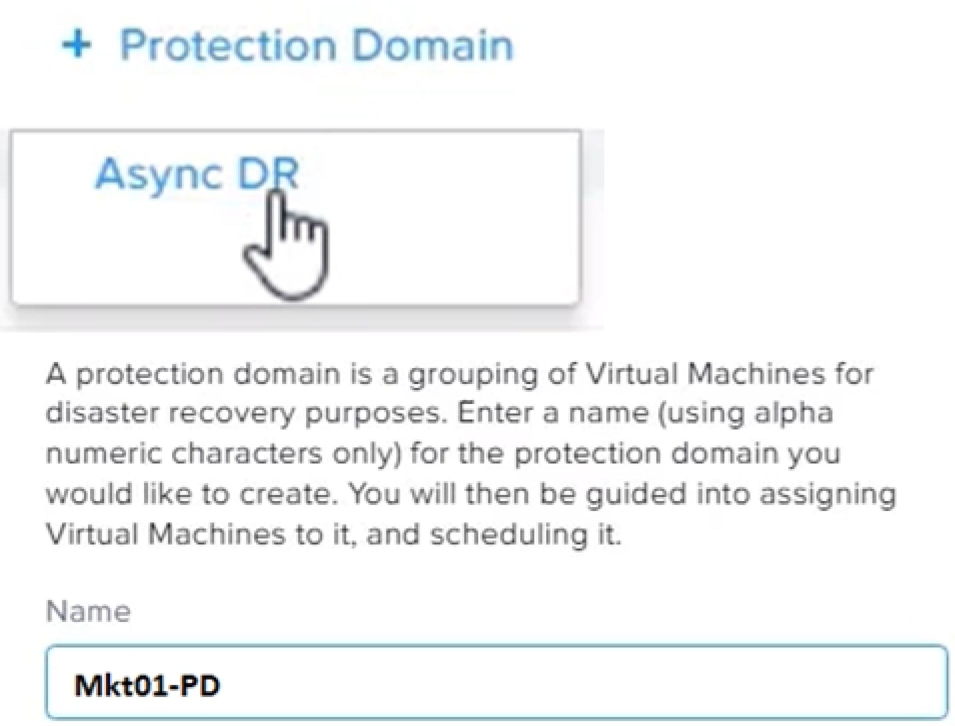
Select Remote Site from the drop-down menu and choose the remote site where you want to replicate the VM. Click Next.

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.

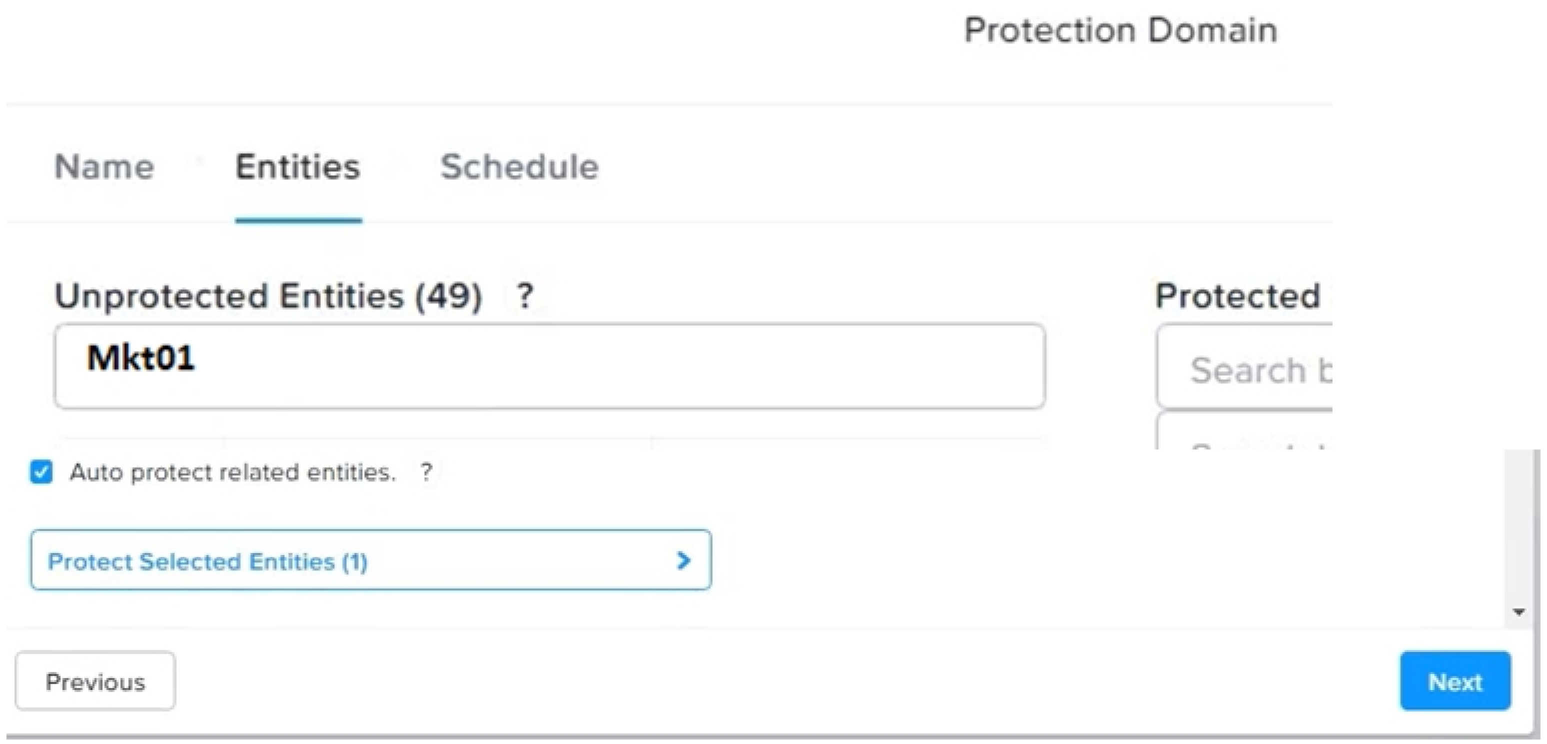




A protection domain is a grouping of Virtual Machines for disaster recovery purposes. Enter a name (using alpha numeric characters only) for the protection domain you would like to create. You will then be guided into assigning Virtual Machines to it, and scheduling it.

Name

Mkt01-PD

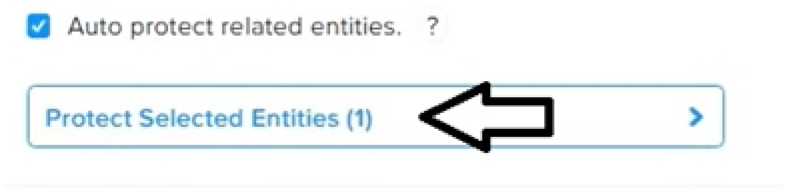


Unprotected Entities (49) ?

Mkt01

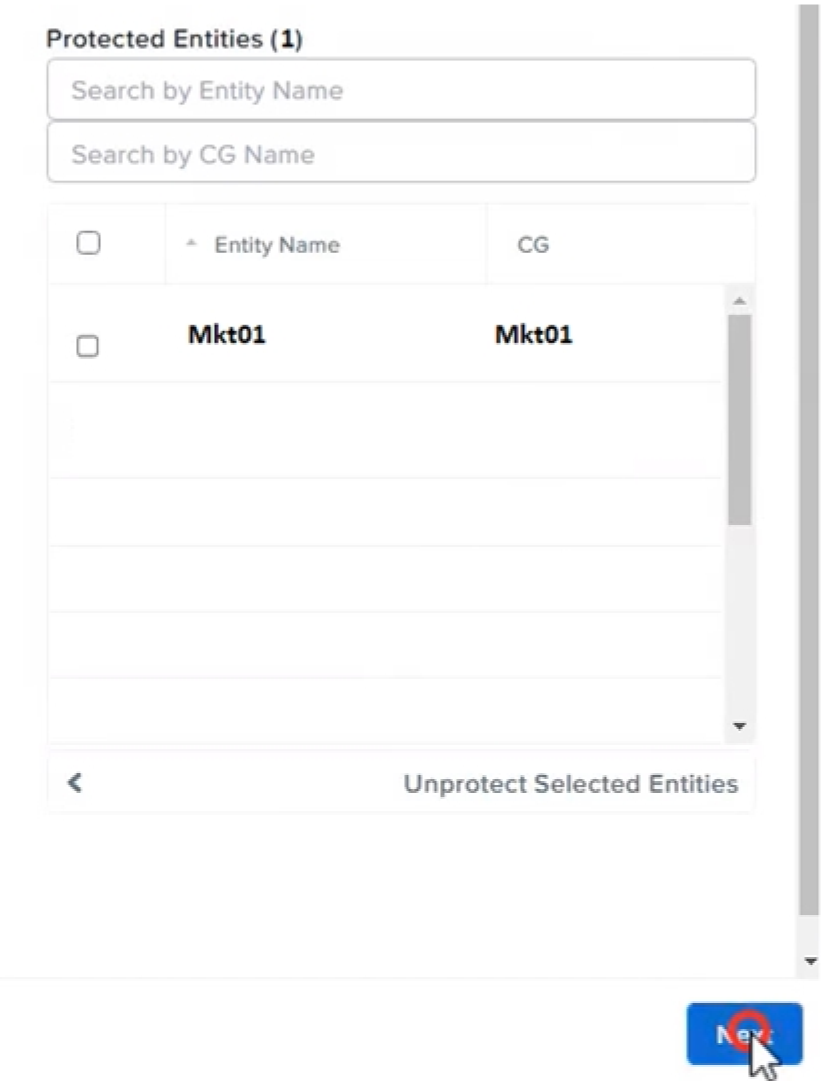
☑ Auto protect related entities. ?

Protect Selected Entities (1) >



☑ Auto protect related entities. ?

Protect Selected Entities (1) >

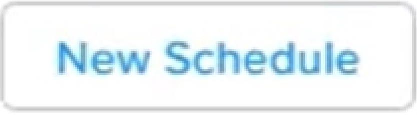


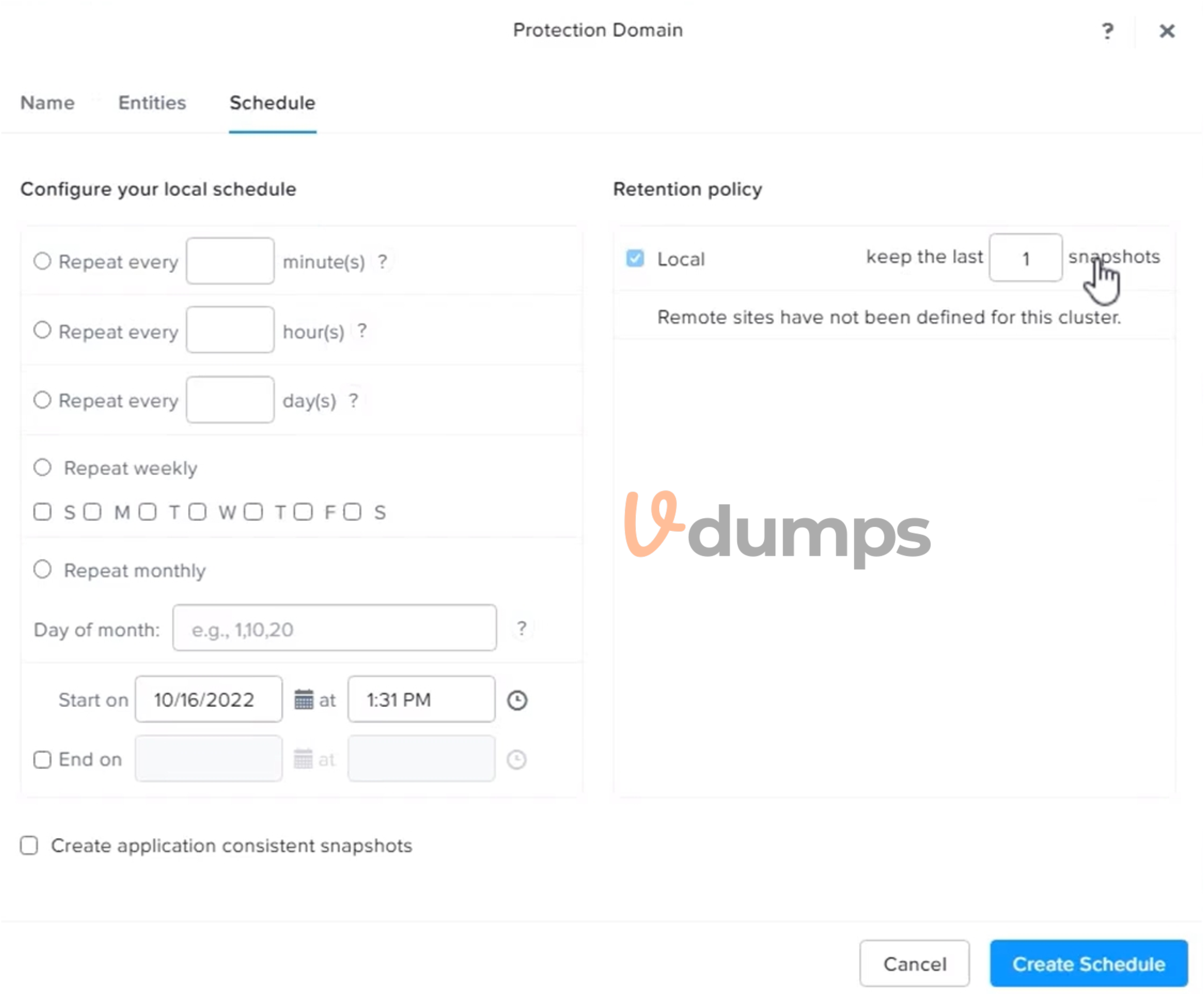
Protected Entities (1)

Search by Entity Name

Search by CG Name

□	Entity Name	CG
□	Mkt01	Mkt01





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