Nutanix.NCM-MCI-6.10.v2026-05-19.q14

Exam Code:	NCM-MCI-6.10
Exam Name:	Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI)
Certification Provider:	Nutanix
Free Question Number:	14
Version:	v2026-05-19
# of views:	102
# of Questions views:	142
https://www.freecram.net/torrent/Nutanix.NCM-MCI-6.10.v2026-05-19.q14.html	

NEW QUESTION: 1
Task 13
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.
Answer:
See the Explanation for step by step solution.
Explanation:
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

NEW QUESTION: 2
Task 10
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
Answer:
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

NEW QUESTION: 3
Use Prism Element for this question.
The Application team has a 3 tier application (App Server, Web Server, and Database Server) that is mission critical and requires as close to 0 RPO and RTO as possible with their current license level.
The organization has 2 clusters, with one cluster (Cluster 1) being production and the other cluster (Cluster 2) being remote/DR. Cluster 2 should be able to fail back to Cluster 1.
The connectivity between the two sites is >5ms and replication traffic should not use more than 10Mbps of bandwidth. The Application team requests a plan that includes the ability to go back 2 days locally, and 2 days remotely.
The team also requests that all 3 VMs be treated as a single group and backed up collectively in a snapshot.
The three VMs are:
* Web-Prod
* App-Prod
* DB-Prod
Use Task3 as part of the name for any objects created for this task.
Note: VMs do NOT need to be powered on. You will need to use the 172.30.0.x IP addresses when configuring DR.
Answer:
See the Explanation below for detailed answer.
Explanation:
Here is the step-by-step solution to configure Disaster Recovery from the Cluster 1 Prism Element interface.
1. Add Cluster 2 as a Remote Site
First, you must register Cluster 2 as a DR target for Cluster 1.
* From the Cluster 1 Prism Element dashboard, navigate to Data Protection from the main dropdown menu.
* Click the Remote Site tab.
* Click the + Remote Site button and select Physical Cluster.
* In the "Name" field, enter Cluster2_DR_Task3.
* In the "Address" field, enter the 172.30.0.x Virtual IP address of Cluster 2.
* Click Save. The clusters will exchange credentials and connect.
2. Throttle Replication Bandwidth
Next, apply the 10 Mbps bandwidth limit for traffic going to Cluster 2.
* On the same Remote Site tab, select the newly created Cluster2_DR_Task3.
* Click the Update button.
* In the dialog, set the Bandwidth Limit to 10 Mbps.
* Click Save.
3. Create the Protection Domain
A Protection Domain (PD) is the top-level object that will manage the VMs and replication schedules.
* In the Data Protection dashboard, click the Table tab.
* Click the + Protection Domain button and select Async DR.
* For the Name, enter App_PD_Task3.
* Click Create.

4. Protect VMs in a Consistency Group
Now you will add the three application VMs to the new Protection Domain as a single Consistency Group (CG).
* You will be taken to the dashboard for the new App_PD_Task3. In the Entities panel, click the Protect Entities button.
* In the "Protect Entities" dialog, search for and select the three VMs:
* Web-Prod
* App-Prod
* DB-Prod
* Click Next.
* Select Create new consistency group and name it App_CG_Task3.
* Click Protect.
5. Create the Replication Schedule
Finally, configure the schedule to meet the RPO and retention requirements.
* In the App_PD_Task3 dashboard, click the Schedules tab.
* Click the + New Schedule button.
* Remote Site: Select Cluster2_DR_Task3.
* RPO (Repeat every): Select NearSync. Set the RPO to 1 minute.
* Note: This is the lowest possible RPO for an Async (>5ms latency) connection, fulfilling the "as close to 0" requirement.
* Local Retention: Set to 2 Days.
* Remote Retention: Set to 2 Days.
* Ensure the "Store snapshots for 2-way replication" checkbox is enabled to allow failback from Cluster 2.
* Click Create Schedule.

NEW QUESTION: 4
An administrator regularly sees a WARN for backup_schedule_check and also receives alerts for Pulse not being enabled on Cluster 1.
Detailed information for backup_schedule_check:
Node xx.xx.xx.xx:
WARN: Backup schedule(s) exist for protection domain NoVMs; however, there are no entities in the protection domain.
Refer
to KB 1910 (http://portal.nutanix.com/kb/1910) for details on backup_schedule_check or Recheck with: ncc health_checks data_protection_checks protection_domain_checks backup_schedule_check.
This shows up in NCC, however, it is something set up by the company and they do not want the NCC check to be run.
Configure Cluster 1 to no longer have messages in NCC about the backup_schedule_check.
Turn off the alert for Pulse not being enabled, and resolve the alert. They would like messages about Pulse to be recorded, but do not want an alert.
Note: You may need to run the "Pulse is not enabled" check in order to have one to resolve.
Answer:
See the Explanation below for detailed answer.
Explanation:
Here is the step-by-step solution to configure Cluster 1 from its Prism Element interface.
1. Disable the backup_schedule_check NCC Check
This will prevent the WARN message for the NoVMs protection domain.
* Log in to the Cluster 1 Prism Element (PE) interface.

* Navigate to the Health dashboard (click the "heart" icon in the top-left).
* In the left-hand menu, select NCC.
* In the search bar for the checks, type backup_schedule_check to find the specific check.
* Select the checkbox next to the backup_schedule_check in the list.
* Click the Disable button that appears above the table. This will stop this check from running during NCC health reports.

2. Configure and Resolve Pulse Alerts

This process involves two parts: disabling the alerting policy, and then enabling Pulse itself to resolve the underlying condition.

A. Disable the Alert Policy

This stops the system from generating a new alert if Pulse is ever disabled, satisfying the "do not want an alert" requirement.

* Click the gear icon (Settings) in the top-right corner.
* From the left-hand menu, select Alert Policies.
* In the search bar, type Pulse to find the policy.
* Select the checkbox for the alert policy named Pulse is not enabled (or pulse_disabled_alert).
* Click the Update button.
* Uncheck the Enable box for the policy.
* Click Save.

B. Enable Pulse (to Resolve the Condition)

This enables the Pulse service to record messages (as requested) and fixes the root cause of the alert, allowing it to be resolved.

* Click the gear icon (Settings) in the top-right corner.
* From the left-hand menu, select Pulse.
* Click the Enable Pulse button (or "Update" if it's already partially configured).
* Check the box for Enable Pulse.
* (Note: Any "Enable alerts for Pulse" boxes would remain unchecked or be ignored, as the main Alert Policy itself is now disabled.)
* Click Save.

C. Resolve the Active Alert

* Navigate to the Alerts dashboard (click the "bell" icon in the top-left).
* Find the active alert: Pulse is not enabled.
* (Note: If the alert is not present, you would first go to the Health dashboard, run the check_pulse NCC check to generate it, and then return to the Alerts dashboard.)
* Select the checkbox next to the "Pulse is not enabled" alert.
* Click the Resolve button that appears at the top of the list. Since the underlying condition (Pulse being disabled) is now fixed, the alert will be successfully resolved.

NEW QUESTION: 5

Task 6

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.
Answer:
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=kA00e000000LKPdCAOchangev
CPUto 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

NEW QUESTION: 6
Task 11
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
Answer:
See the Explanation for step by step solution.
Explanation:
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/<filename> to remove the file causing the storage bloat. Replace <filename> 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

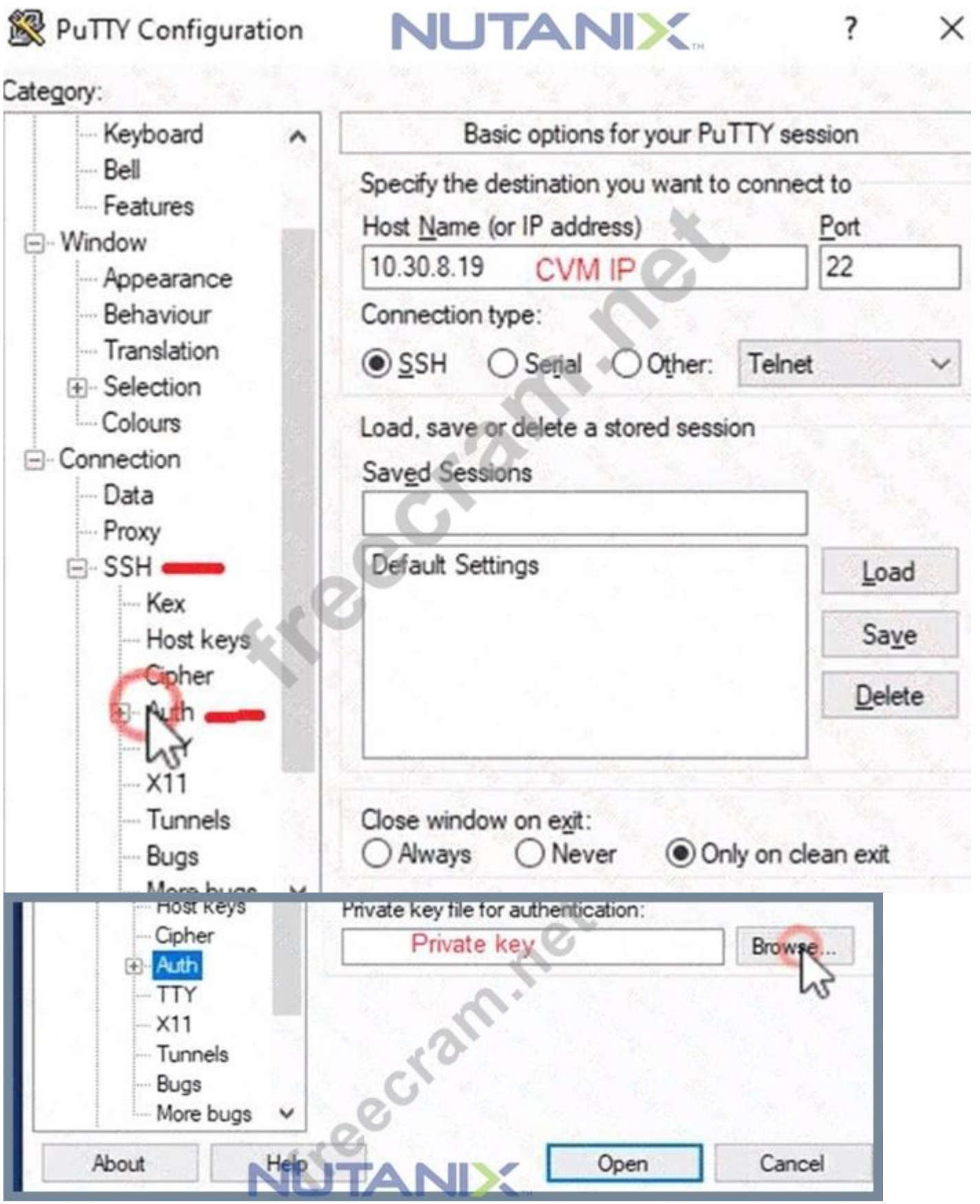
rm files_name
df -h
ncc health_checks hardware_checks disk_checks disk_usage_check

NEW QUESTION: 7
Task 2
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.
Answer:
See the Explanation for step by step solution.
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 $i "ls -ltr /home/nutanix/data/logs/*.FATAL"; done NCC Health Check: cluster_services_down_check (nutanix.com) Part2 Vlad Drac2023-06-05T13:22:00.86I'll update this one with a smaller, if possible, command Update the default password for the root user on the node to match the admin user password echo -e "CHANGING ALL AHV HOST ROOT PASSWORDS.\nPlease input new password: "; read -rs password1; echo "Confirm new password: "; read -rs password2; if ["$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

freecram.net



NEW QUESTION: 8
Task 4

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 xxxxxxxxxx --interfaces ethX,ethX update_uplinks manage_ovs --bridge_name brX-up --interfaces ethX,ethX --bond_name bond1 --bond_mode xxxxxxxxxx update_uplinks See the Explanation for step by step solution.
Answer:
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

NEW QUESTION: 9
An administrator is experiencing an unidentified issue which is causing inode exhaustion on CVMs in Cluster
1. The time between receiving alerts and exhaustion is too short; the administrator needs to lower the alert thresholds to allow more time to clean up inodes until the issue has been identified and resolution implemented.
From Prism Element, modify the appropriate alert policy setting critical threshold for Cluster 1 to 60% and warning threshold to 45%. Ensure the check runs every minute and is not resolved without administrator action.
Answer:
See the Explanation below for detailed answer.
Explanation:
Here is the step-by-step solution to modify the alert policy from the Prism Element (PE) interface for Cluster 1.
1. Access Cluster 1 Prism Element
* From the main Prism Central dashboard, navigate to Hardware > Clusters.
* Find Cluster 1 in the list and click its name. This will open the specific Prism Element login page for that cluster.
* Log in to Cluster 1's Prism Element interface.
2. Modify the Alert Policy
* In the Cluster 1 PE interface, click the gear icon (Settings) in the top-right corner.
* From the left-hand menu, select Alert Policies.
* In the search bar, type inode to find the correct policy.
* Select the checkbox for the policy named cvm_inode_usage_high.

* Click the Update button.
* In the "Update Alert Policy" dialog, configure the following settings:
* Warning Threshold (%): Change the value to 45.
* Critical Threshold (%): Change the value to 60.
* Check Interval (Secs): Change the value to 60 (to run the check every minute).
* Auto Resolve: Uncheck this box (to ensure the alert is not resolved without administrator action).
* Click Save.

NEW QUESTION: 10

Task 3
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.
The report should run monthly and should send an email to admin@syberdyne.net when it runs.
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.

Freecram.net

Answer:

See the Explanation for step by step solution.

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

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:
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:

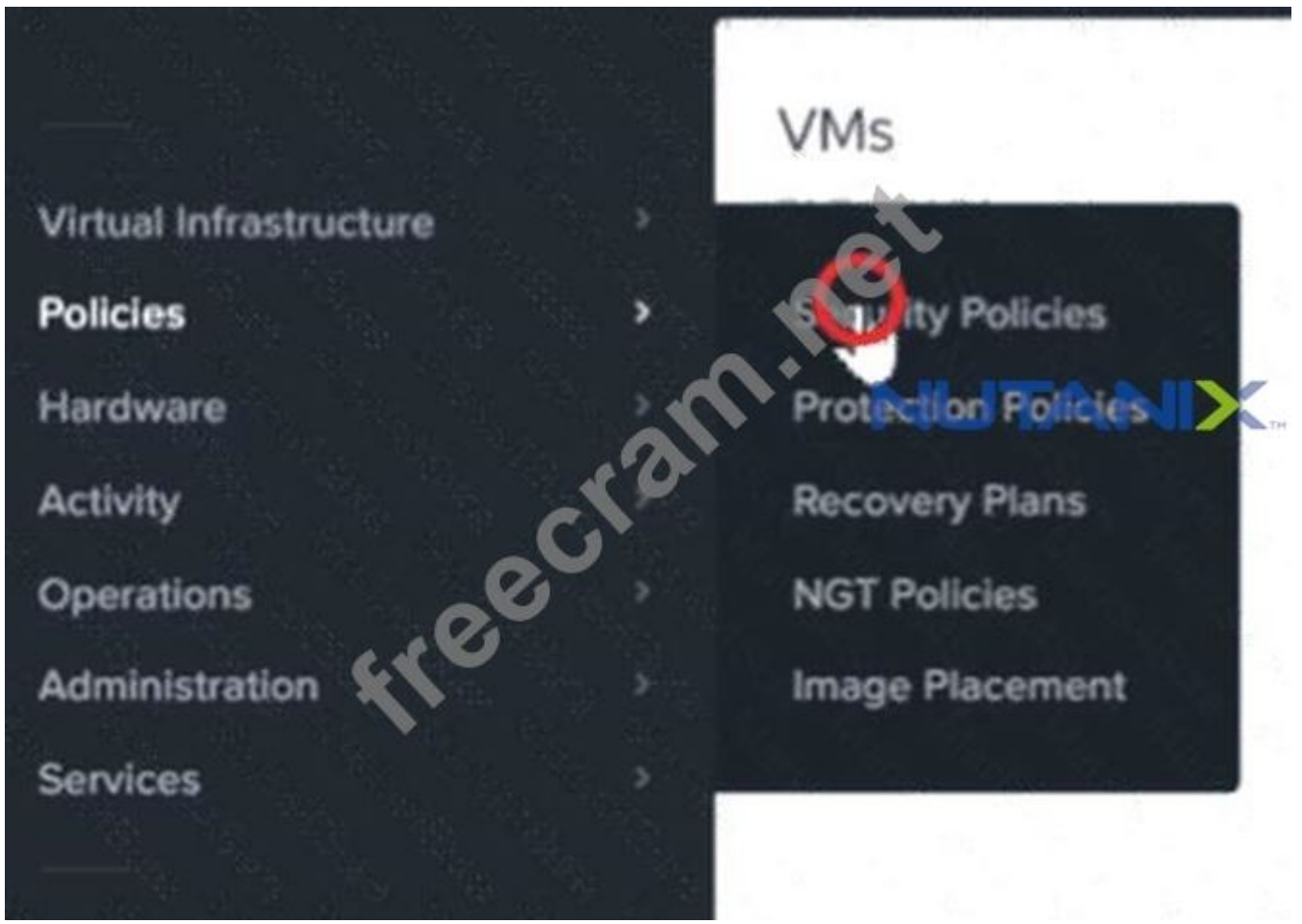
NEW QUESTION: 11
Following new security guidelines, it must be ensured that the storage of critical virtual machines will be encrypted in future.

The assignment is to be made by a new category called VM-Storage with a value of softwareencrypted in Prism Central. Make sure a second value of SEDencrypted is also created for future use.
Create the above-mentioned category and perform further configurations in Prism Central for VM-based storage encryption.
Assign the name Encrypted-Storage to the newly created policy.
Answer:
See the Explanation below for detailed answer.
Explanation:
Here is the step-by-step solution to create the category and the corresponding storage encryption policy within Prism Central.
1. Create the Category
First, you must create the category and the two values requested.
* In Prism Central, navigate to Administration > Categories.
* Click New Category.
* In the Name field, enter VM-Storage.
* In the Add a Value field, type softwareencrypted and click the Add (plus) button.
* In the Add a Value field again, type SEDencrypted and click the Add (plus) button.
* Click Save.
2. Create the Encryption Policy
Next, you will create the security policy that uses the new category.
* In Prism Central, navigate to Security > Data-at-Rest Encryption.
* Click the + Create Security Policy button.
* In the Policy Name field, enter Encrypted-Storage.
* Ensure the Encryption Type is set to Software-based.
* For Target VMs, select the radio button for VMs matching a category.
* In the Select Category dropdown, choose the VM-Storage category you just created.
* In the Select Value dropdown, choose softwareencrypted.
* Click Save.
This policy will now automatically apply software-based encryption to any new or existing VMs that are assigned the VM-Storage: softwareencrypted category.

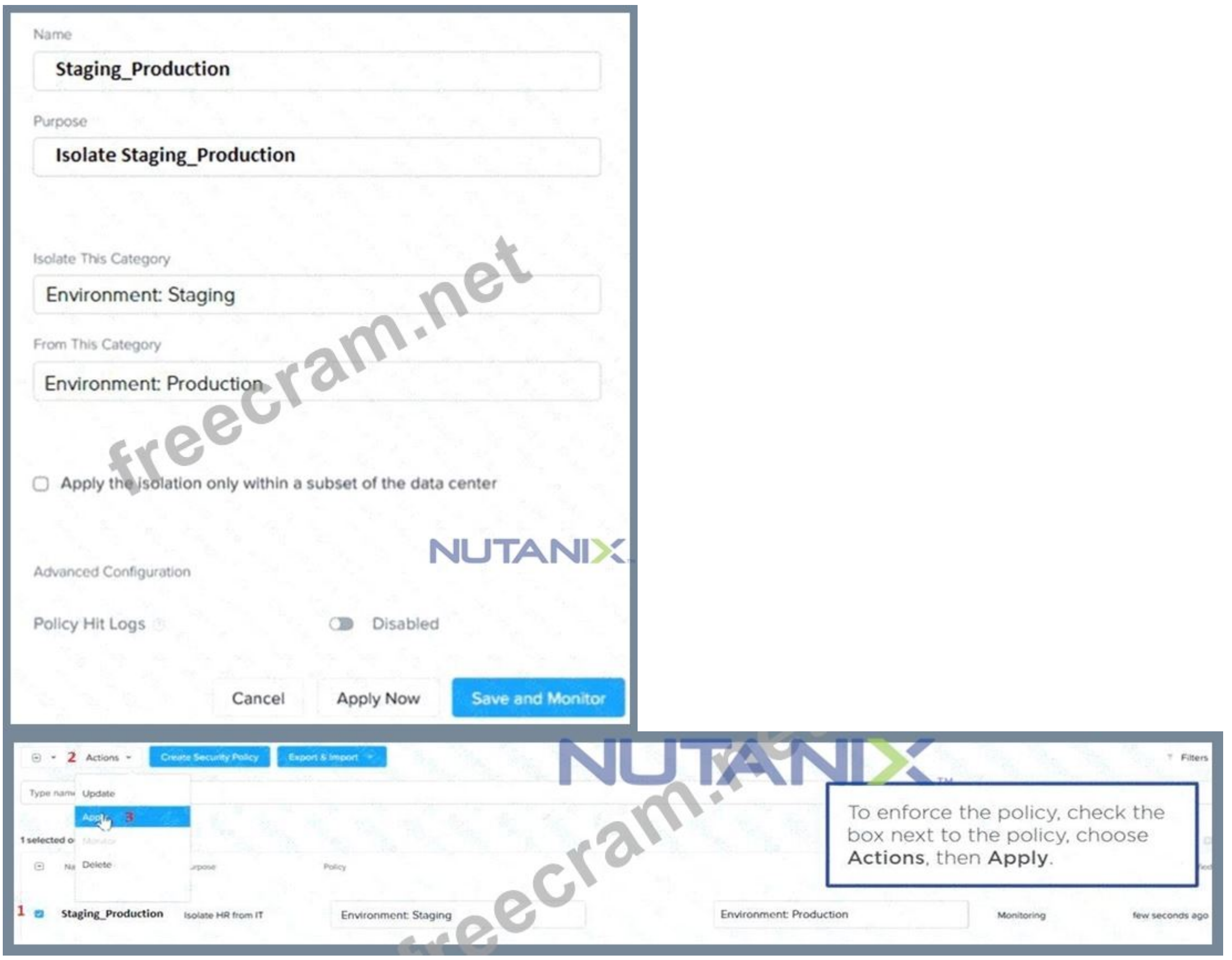
NEW QUESTION: 12
An administrator wants to increase the performance of their Database virtual machine.
Database_VM has a database that is spread across three vDisks in the volume group Database_VM. The volume group is directly attached to the virtual machine. Previous performance analysis has indicated all storage requests are going to the same node. While this test environment has 1 node, the production environment has 3 nodes.
Configure the Volume Group Database_VM so that it's optimized for the user's VM and the production environment. The virtual machine has been powered off and moved to this test cluster for the maintenance work.
Note: Do not power on the VM.
Answer:
See the Explanation below for detailed answer.
Explanation:
Here is the step-by-step solution to configure the Volume Group for optimized performance in the production environment.

This task is performed in Prism Central.
* From the main dashboard, navigate to Compute & Storage > Volume Groups.
* Find the Volume Group named Database_VM in the list.
* Select the checkbox next to Database_VM.
* Click the Actions dropdown menu and select Update.
* In the "Update Volume Group" dialog, scroll to the bottom of the "Basic Configuration" section.
* Find the checkbox labeled Enable Client Side Load Balancing and check it.
Note: This setting allows the iSCSI initiator within the guest VM to connect to all CVMs in the cluster, distributing the storage load from the three vDisks across all three nodes in the production environment instead of focusing all I/O on just one.
Click Save.

NEW QUESTION: 13
Task 8
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.
Answer:
See the Explanation for step by step solution.
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.



freecram.net



NEW QUESTION: 14
Due to new security requirements, an administrator has been tasked with updating the security settings for user accounts within Prism Element on Cluster 1.

An SSL Certificate Signing Request with Subject Alternative Name should be generated for submission to the security team's Certificate Authority with the following details:
countryName = US
stateOrProvinceName = North Carolina
localityName = Durham
organizationName = ACME
organizationalUnitName = Infrastructure
commonName = prism_element.ACME.org
emailAddress = administrator@ACME.org
Alternate names = cvm1.ACME.org, cvm2.ACME.org, cvm3.ACME.org
Encryption: RSA 2048, sha256
When the Certificate Signing Request is generated, place a copy of both the .cnf file and the .csr file on the desktop named 'prism_element_acme.cnf' and 'prism_element_acme.csr' Save a copy of the command(s) used for this scenario to a new file on the desktop named "Task 5.txt".
Note: You must copy and paste the command(s) and output from SSH to the "Task 5.txt" file to achieve all points available.
Answer:
See the Explanation below for detailed answer.
Explanation:
Here is the step-by-step solution to generate the Certificate Signing Request (CSR) on Cluster 1.
This entire process is performed from an SSH session connected to a CVM (Controller VM) on Cluster 1.
1. Access Cluster 1 CVM
* From Prism Central, navigate to Hardware > Clusters and click on Cluster 1 to open its Prism Element (PE) interface.
* In the Cluster 1 PE, navigate to Hardware > CVMs to find the IP address of any CVM in the cluster.
* Use an SSH client (like PuTTY) to connect to the CVM's IP address.
* Log in with the admin user and password.
2. Create the Configuration File (.cnf)
To include the Subject Alternative Names (SANs), you must first create a configuration file.
* In the CVM's command line, create the .cnf file using a text editor:
vi prism_element_acme.cnf
* Press i to enter "Insert" mode.
* Paste the following text exactly into the editor:
Ini, TOML
[req]
default_bits = 2048
distinguished_name = req_distinguished_name
req_extensions = v3_req
prompt = no
[req_distinguished_name]
C = US
ST = North Carolina
L = Durham
O = ACME

OU = Infrastructure
CN = prism_element.ACME.org
emailAddress = administrator@ACME.org
[v3_req]
subjectAltName = @alt_names
[alt_names]
DNS.1 = cvm1.ACME.org
DNS.2 = cvm2.ACME.org
DNS.3 = cvm3.ACME.org
* Press Esc to exit "Insert" mode, then type :wq and press Enter to save and quit vi.
3. Generate the CSR and Key
* Run the following openssl command. This command uses the .cnf file to generate the new CSR (.csr) and a corresponding private key (.key), applying the sha256 encryption as requested.
Bash
openssl req -new -nodes -out prism_element_acme.csr -keyout prism_element_acme.key -config prism_element_acme.cnf -sha256
* The command will output the following, confirming the key generation:
* Generating a 2048 bit RSA private key
* .....+++++
* .....+++++
* writing new private key to 'prism_element_acme.key'
* -----
4. Save Files to the Desktop
You will now copy the contents of the generated files from the CVM to your desktop.
* For Task 5.txt (Commands and Output):
* Open a new Notepad file on the desktop.
* Copy and paste all the commands you ran in the SSH session and their full output (as shown in steps 2 and 3) into this file.
* Save the file on the desktop as Task 5.txt.
* For prism_element_acme.cnf:
* In the CVM SSH session, display the file's content:
cat prism_element_acme.cnf
* Copy the entire text output (starting from [req]).
* Open a new Notepad file on the desktop.
* Paste the content and save the file as prism_element_acme.cnf.
* For prism_element_acme.csr:
* In the CVM SSH session, display the file's content:
cat prism_element_acme.csr
* Copy the entire text output, including the -----BEGIN CERTIFICATE REQUEST----- and ----- END CERTIFICATE REQUEST----- lines.
* Open a new C:\Users\admin\Desktop\Notepad file on the desktop.
* Paste the content and save the file as prism_element_acme.csr.

Valid NCM-MCI-6.10 Dumps shared by EduDump.com for Helping Passing NCM-MCI-6.10 Exam! EduDump.com now offer the **newest NCM-MCI-6.10 exam dumps**, the EduDump.com NCM-MCI-6.10 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com NCM-MCI-6.10 dumps with Test Engine here: https://www.edudump.com/exams/Nutanix/NCM-MCI-6.10/premium/ (**33** Q&As Dumps, **35%OFF Special Discount Code: freecram**)