Boost up Your Certification Score

Nutanix
NCM-MCI
Nutanix Certified Master - Multicloud Infrastructure v6.10 Exam

Exams Boost
Boost Up Your Career

For More Information – Visit link below:

https://www.examsboost.com/

Product Version

✓ Up to Date products, reliable and verified.
✓ Questions and Answers in PDF Format.

Visit us at: https://www.examsboost.com/test/ncm-mci

Latest Version: 7.1

Question: 1

SIMULATION
TASK 1
A newly created Windows VM “SQL02” is experiencing poor storage performance when compared to “SQL01” running within the same cluster, on the same storage container.
The cluster is in a healthy state.
Create a new session named Monitor SQL02 with meaningful metrics. Right click on the session page and click Select All then paste this into Notepad and save it as Task 1.txt on the desktop.
Also, save the analysis as a report named MonitorSQL02 and send the report as a PDF on a daily basis to perf_group@ACME.org. Reports should not be retained. If any new objects need to be created, use monitovm2 in the name.
Finally, correct the issue within “SQL02”.
Notes:
Do not power on the VMs.
While you will be creating a session, you will need to examine the VM configurations to determine the issue.
Do not delete the VM to resolve the issue, any other destructive change is acceptable.

A. See the Explanation below for detailed answer

Answer: A

Explanation:
Here is the step-by-step solution to all three tasks, performed within the Nutanix Prism interface.
Task 1: Create Monitoring Session & Save Metrics
From the Prism Central dashboard, navigate to Operations > Analysis.
Click the + New Session button.
Name the session Monitor SQL02.
In the "Entities" search box, type SQL01 and select VM: SQL01.
In the "Entities" search box, type SQL02 and select VM: SQL02.
Click Add Charts > New Chart.
Title: Storage IOPS
Metric: Storage Controller IOPS
Click Add.
Click Add Charts > New Chart.
Title: Storage Latency
Metric: Storage Controller Latency
Click Add.
Click Add Charts > New Chart.
Title: Storage Bandwidth

Visit us at: https://www.examsboost.com/test/ncm-mci

Metric: Storage Controller Bandwidth
Click Add.
Click Save Session.
With the "Monitor SQL02" session open, right-click anywhere on the page and click Select All.
Right-click again and select Copy.
Open Notepad, paste the content, and save the file to the desktop as Task 1.txt.
(The content pasted into Task 1.txt would be the session's chart configurations, showing metrics for SQL01 and SQL02.)
Task 2: Create and Schedule the Report
While still in the "Monitor SQL02" analysis session, click the Save as Report button (it looks like a bookmark icon).
Name the report MonitorSQL02 and click Save.
Navigate to Operations > Reports.
Find the MonitorSQL02 report in the list. Select its checkbox.
Click the Actions dropdown and select Schedule.
Configure the schedule with the following settings:
Schedule Name: monitovm2_daily_report
Recurrence: Daily
Start Time: (Set to a time, e.g., 8:00 AM)
Repeat every: 1 day(s)
Retention Policy: Uncheck the "Retain a copy of the report" box. (This ensures reports are not retained).
Email Report: Check this box.
Format: PDF
Recipients: perf_group@ACME.org
Click Save.
Task 3: Identify and Correct the Performance Issue
This task is performed without powering on the VMs, indicating a configuration error.
Investigation
Navigate to VMs > Table view.
Click on the SQL01 (the good VM) and select the Configuration tab.
Expand the Disks section. Observe that the primary disk is attached to a SCSI bus (e.g., scsi.0). This is the high-performance standard.
Return to the VM list and click on SQL02 (the problem VM).
Expand the Disks section.
Root Cause
You discover that the primary disk for SQL02 is attached to an IDE bus. The IDE bus has significant performance limitations and is not suitable for a database server, causing the poor storage performance.
Correction
With the SQL02 VM selected, click the Update button.
In the "Update VM" dialog, scroll down to the Disks section.
Find the disk attached to the IDE bus. Click the Edit (pencil) icon for that disk.
Change the Bus Type dropdown from IDE to SCSI.
The Device Index will automatically populate (e.g., scsi.0).
Click Save in the "Update Disk" dialog.
(Note: A "VirtIO SCSI Controller" will be automatically added to the VM configuration if one was not already present.)

Visit us at: https://www.examsboost.com/test/ncm-mci

Click Save in the "Update VM" dialog.
The VM SQL02 is now configured to use the high-performance VirtIO-SCSI controller, which will resolve the storage performance discrepancy once the VM is powered on.

Question: 2

SIMULATION
The security team has provided some new security requirements for cluster level security on Cluster 2.
Security requirements:
Update the password for the root user on the Cluster 2 node to match the admin user password.
Note: The 192.168.x.x network is not available. To access a node use the host IP (172.30.0.x) from the CVM.
Output the cluster-wide configuration of the SCMA policy to desktop\output.txt before changes are made.
Enable the Advanced Intrusion Detection Environment (AIDE) to run on a weekly basis for the hypervisor and cvms for Cluster 2.
Enable high-strength password policies for the hypervisor and cluster.
Ensure CVMs require SSH keys for login instead of passwords. (SSH keys are located in the desktop\Files\SSH folder.)
Ensure the cluster meets these requirements. Do not reboot any cluster components.
Note: Please ensure you are modifying the correct components.

A. See the Explanation below for detailed answer

Answer: A

Explanation:
Here is the step-by-step solution to apply the security requirements to Cluster 2.
1. Access Cluster 2 Prism Element
First, we must access the Prism Element (PE) interface for Cluster 2, as most security settings are cluster-specific.
From the Prism Central dashboard, navigate to Hardware > Clusters.
Find Cluster 2 in the list and click its name. This will open the Prism Element login page for that specific cluster in a new tab.
Log in to Cluster 2's Prism Element using the admin credentials.
2. Requirement: Update Node Root Password
This task syncs the root password for all AHV hypervisor nodes with the cluster's admin user password.
In the Cluster 2 PE interface, click the gear icon (Settings) in the top right corner.
Select Cluster Lockdown from the left-hand menu.
Click the Set Root Password on All Hosts button.
A dialog box will appear. Enter the current admin password (the one you just used to log in) into both the New Password and Confirm New Password fields.
Click Save. This will propagate the admin password to the root user on all nodes in Cluster 2.

Visit us at: https://www.examsboost.com/test/ncm-mci

3. Requirement: Add CVM SSH Key
This task adds the security team's public key to the admin user, which is required before we can disable password-based login.
On the desktop, navigate to the Files > SSH folder.
Open the id_rsa.pub file (or equivalent public key file) with Notepad.
Copy the entire string of text (e.g., ssh-rsa AAAA...).
In the Cluster 2 PE interface, go to Settings (gear icon) > User Management.
Select the admin user and click Modify User.
Paste the copied public key into the Public Keys text box.
Click Save.
4. Requirement: Apply SCMA Policies (All other requirements)
The remaining requirements are all applied via the command line on a CVM using Nutanix's Security Configuration Management Automation (SCMA).
Access the CVM:
Find a CVM IP for Cluster 2 by going to Hardware > CVMs in the PE interface.
Open an SSH client (like PuTTY) and connect to that CVM's IP address.
Log in with the username admin and the corresponding password.
Output Current Policy (Req 2):
Before making changes, run the following command to see the current policy:
ncli scma status
Copy the entire output from your SSH terminal.
Open Notepad on the desktop, paste the copied text, and Save the file to the desktop as output.txt.
Apply New Policies (Req 3, 4, 5):
Run the following commands one by one. The cluster will apply them immediately without a reboot.
Enable AIDE (Req 3):
ncli scma update aide-status=enabled aide-schedule=weekly
Enable High-Strength Passwords (Req 4):
ncli scma update password-policy=high
Require SSH Keys for CVMs (Req 5):
ncli scma update ssh-login=keys-only
Verification
You can verify all changes by running the status command again. The output should now reflect the new, hardened security posture.
ncli scma status
AIDE Status: should show Enabled
AIDE Schedule: should show Weekly
Password Policy: should show High
SSH Login: should show keys-only

Question: 3

SIMULATION
Your security team is working on automation to manage Security Policies.

Visit us at: https://www.examsboost.com/test/ncm-mci

They have exported some of the existing rules to the file "Security Policy.txt" located on the desktop. This file needs to be modified for the test environment.
All rules except the quarantine rule should be logged.
Only the Quarantine rule should be enforced, the other rules will only be logged.
The quarantine rule should affect the SecOps environment.
The SMB rule should only affect VMs with the “smbhost” and “smbclient” tags.
The “DN test” policy should allow ipv6 and should not restrict any protocols between the included tiers.
There are three rules in the file, do not delete, add or copy lines. Only replace xxxx with the correct value as appropriate. It is possible that not all “xxxxx” will be replaced.
Save the file with the same name.
Possible values to replace the “xxxxx”:
8080
ALL
APPLY
false
MONITOR
Non-Prod
SecOps
smbhost
smbclient
TCP
True

A. See the Explanation below for detailed answer

Answer: A

Explanation:
Here is the step-by-step solution to modify the security policy file as required.
Navigate to the desktop and open the file Security Policy.txt (which corresponds to the provided Security Policy.bak content) using a text editor like Notepad.
Modify the file content by replacing the xxxxx and xxxx placeholders according to the security requirements.
Modifications by Rule
Here are the specific changes to make within the file:
1. Quarantine Rule
Requirement 1 (No Logging): The quarantine rule should not be logged.
Change "is_policy_hitlog_enabled": "xxxxx" to "is_policy_hitlog_enabled": "false"
Requirement 2 (Enforce): This rule must be enforced.
Change "action": "xxxxx" (under quarantine_rule) to "action": "APPLY"
Requirement 3 (Environment): The rule must affect the "SecOps" environment.
Change "Environment": ["xxxxx"] to "Environment": ["SecOps"]
2. SMB-block Rule
Requirement 1 (Logging): This rule must be logged.
Change "is_policy_hitlog_enabled": "xxxxx" to "is_policy_hitlog_enabled": "True"
Requirement 2 (Monitor): This rule must not be enforced, only logged.

Visit us at: https://www.examsboost.com/test/ncm-mci

Change "action": "xxxxx" (under isolation_rule) to "action": "MONITOR"
Requirement 4 (Tags): The rule must affect the "smbhost" and "smbclient" tags.
Change "SMBv1": ["xxxxx"] to "SMBv1": ["smbhost"]
Change "SMRv1": ["xxxxx"] to "SMRv1": ["smbclient"]
3. DN test (dn-policy1) Rule
Requirement 2 (Monitor): This rule must not be enforced, only logged.
Change "action": "xxxx" (under app_rule) to "action": "MONITOR"
Requirement 5 (Allow IPv6): This policy must allow IPv6 traffic.
Change "allow_ipv6_traffic": "xxxx" to "allow_ipv6_traffic": "True"
Final Step
After making all the replacements, Save the file, overwriting the original Security Policy.txt on the desktop.
Example of completed rules (replace xxxxx accordingly):
Rule Name: Quarantine Rule
Logged: false
Action: APPLY
Environment: SecOps
Protocols: TCP
Ports: 8080
Rule Name: SMB Rule
Logged: True
Action: MONITOR
Tags: smbhost, smbclient
Protocols: TCP
Ports: 8080
Rule Name: DN Test Policy
Logged: True
Action: MONITOR
Environment: Non-Prod
Protocols: ALL
Ports: 8080

Question: 4

SIMULATION
The Infosec team has requested that all operational tasks performed within Cluster 1 be properly logged to include the top 4 severity levels and pushed to their syslog system using highest reliability possible for analysis. This is to include any Virtual Machine changes only.
The Infosec team has also requested that monitor logs for the given RSyslog Server Module be included for now. No extra logs should be included.
No other clusters should connect to this syslog server.
Syslog configuration:
Syslog Name: Corp_Syslog
Syslog IP: 34.142.155.231
Port: TCP/514

Visit us at: https://www.examsboost.com/test/ncm-mci

Ensure only Cluster 1 is configured to meet these requirements.

A. See the Explanation below for detailed answer

Answer: A

Explanation:
Here is the step-by-step solution to configure syslog for Cluster 1.
1. Access Cluster 1 Prism Element
Since the requirement is to only configure Cluster 1 and not other clusters, this task must be performed in the Prism Element (PE) interface for Cluster 1.
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. Add the Syslog Server
In the Cluster 1 PE interface, click the gear icon (Settings) in the top-right corner.
From the left-hand menu, select Syslog.
In the "Remote Syslog Server" section, click the + Add Syslog Server button.
Fill in the server details as required:
Name: Corp_Syslog
IP Address: 34.142.155.231
Port: 514
Protocol: TCP (This provides the highest reliability, as requested).
Click Save.
3. Configure Log Modules and Severities
Now, we must specify which logs to send to the new server.
On the same Syslog settings page, find the "Syslog Configuration" section and click the Configure button (or Modify if a default is present).
A dialog box "Select Modules and Levels" will appear.
Uncheck all modules to ensure no extra logs are sent.
Check the box for the RSyslog Server Module (or rsyslog_forwarder).
For this module, check the boxes for the severities: Critical, Warning, and Info.
Check the box for the ApiServer module.
This module logs all operational tasks and audit trails, which includes all Virtual Machine changes.
For this module, check the boxes for the top severity levels: Critical, Warning, and Info.
Ensure no other modules (like Stargate, Cerebro, Zookeeper, etc.) are checked.
Click Save.
Cluster 1 is now configured to send its audit logs (including VM changes) and its own syslog monitoring logs to the Corp_Syslog server via TCP, fulfilling all security requirements.

Question: 5

SIMULATION

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.

A. See the Explanation below for detailed answer

Answer: A

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

Visit us at: https://www.examsboost.com/test/ncm-mci

[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.

Visit us at: https://www.examsboost.com/test/ncm-mci

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer

