

Nutanix NCM-MCI-6.10 Valid Test Objectives, Test NCM-MCI-6.10 Testking



If you're still learning from the traditional old ways and silently waiting for the test to come, you should be awake and ready to take the exam in a different way. Study our NCM-MCI-6.10 study materials to write "test data" is the most suitable for your choice, after recent years show that the effect of our NCM-MCI-6.10 Study Materials has become a secret weapon of the examinee through qualification examination, a lot of the users of our NCM-MCI-6.10 study materials can get unexpected results in the examination.

If you search test practice questions you can find us which is the leading position in this field or you may know us from other candidates about our high-quality NCM-MCI-6.10 training materials as every year thousands of candidates choose us and gain success for their exams. If you want to choose reliable and efficient Latest NCM-MCI-6.10 Questions and answers, we will be your best choice as we have 100% pass rate for NCM-MCI-6.10 exams. Many candidates prefer simulator function of our NCM-MCI-6.10 training materials. And our NCM-MCI-6.10 exam questions won't let you down.

>> **Nutanix NCM-MCI-6.10 Valid Test Objectives** <<

Test NCM-MCI-6.10 Testking & NCM-MCI-6.10 Reliable Exam Preparation

Success in the NCM-MCI-6.10 test of the Nutanix NCM-MCI-6.10 credential is essential in today's industry to verify the skills and get well-paying jobs in reputed firms around the whole globe. Earning the Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI) NCM-MCI-6.10 Certification sharpens your skills and helps you to accelerate your career in today's cut throat competition in the Nutanix industry. It is not easy to clear the NCM-MCI-6.10 exam on the maiden attempt.

Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI) Sample Questions (Q18-Q23):

NEW QUESTION # 18

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:

Explanation:

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.

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 `svnips`; 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
```

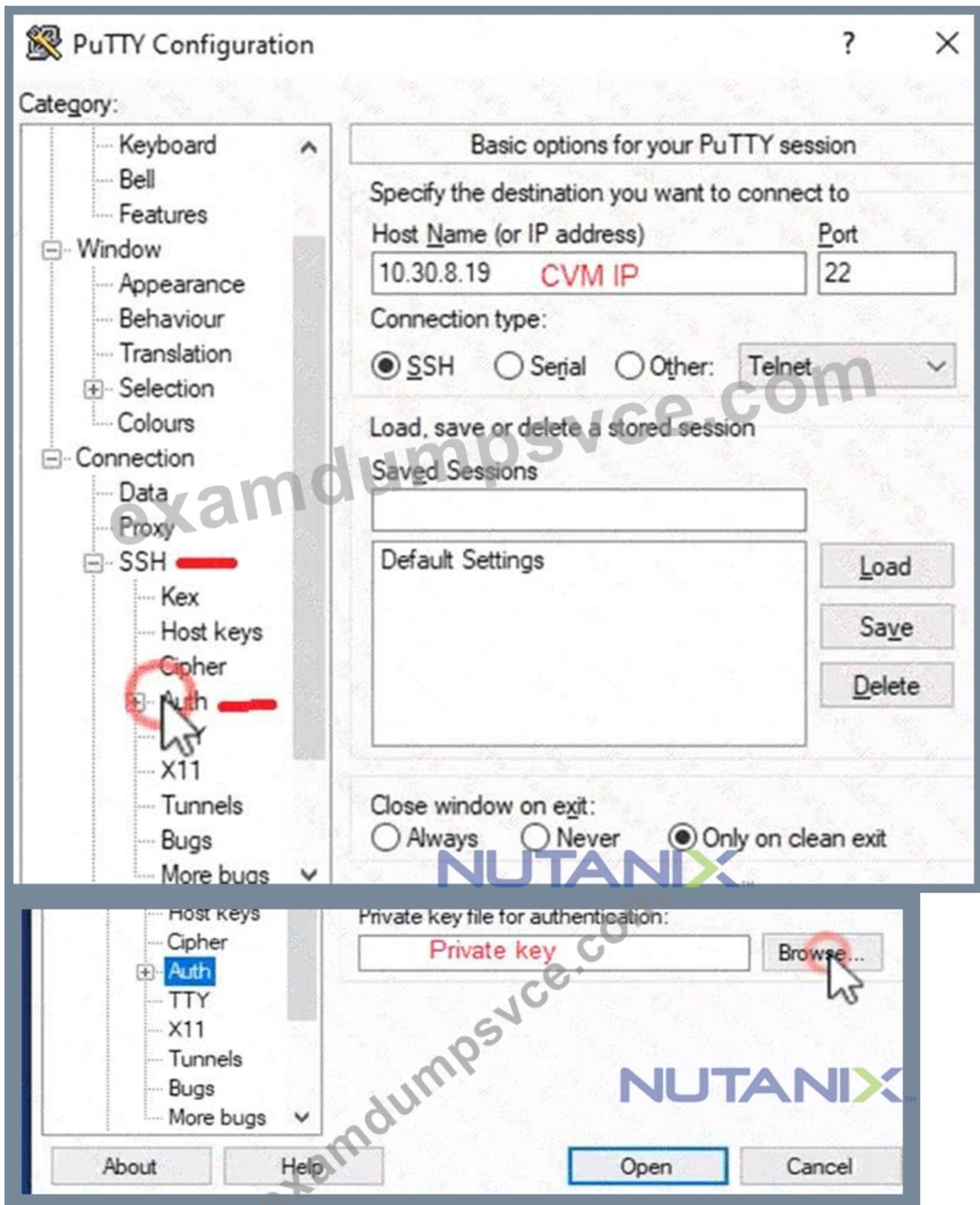
```
ncli cluster edit-hypervisor-security-params schedule=weekly
```

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>

The screenshot shows a web form for adding a new public key. The form has two main sections: 'Name' and 'Key'. The 'Name' field is a text input containing 'name_public_key'. The 'Key' field is a larger text area containing 'Public Key here'. A watermark 'examdumpsvce.com' is overlaid diagonally across the form. At the bottom left, there is a 'Back' button with a left-pointing arrow. At the bottom right, there is a blue 'Save' button. The Nutanix logo is visible at the top of the page.



NEW QUESTION # 19

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:

Explanation:

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 # 20

Task 1

An administrator needs to configure storage for a Citrix-based Virtual Desktop infrastructure.

Two VDI pools will be created

Non-persistent pool named MCS_Pool for tasks users using MCS Microsoft Windows 10 virtual Delivery Agents (VDAs)

Persistent pool named Persist_Pool with full-clone Microsoft Windows 10 VDAs for power users

20 GiB capacity must be guaranteed at the storage container level for all power user VDAs The power user container should not be able to use more than 100 GiB Storage capacity should be optimized for each desktop pool.

Configure the storage to meet these requirements. Any new object created should include the name of the pool (s) (MCS and/or Persist) that will use the object.

Do not include the pool name if the object will not be used by that pool.

Any additional licenses required by the solution will be added later.

Answer:

Explanation:

See the Explanation for step by step solution.

Explanation:

To configure the storage for the Citrix-based VDI, you can follow these steps:

Log in to Prism Central using the credentials provided.

Go to Storage > Storage Pools and click on Create Storage Pool.

Enter a name for the new storage pool, such as VDI_Storage_Pool, and select the disks to include in the pool.

You can choose any combination of SSDs and HDDs, but for optimal performance, you may prefer to use more SSDs than HDDs.

Click Save to create the storage pool.

Go to Storage > Containers and click on Create Container.

Enter a name for the new container for the non-persistent pool, such as MCS_Pool_Container, and select the storage pool that you just created, VDI_Storage_Pool, as the source.

Under Advanced Settings, enable Deduplication and Compression to reduce the storage footprint of the non-persistent desktops.

You can also enable Erasure Coding if you have enough nodes in your cluster and want to save more space. These settings will help you optimize the storage capacity for the non-persistent pool.

Click Save to create the container.

Go to Storage > Containers and click on Create Container again.

Enter a name for the new container for the persistent pool, such as Persist_Pool_Container, and select the same storage pool, VDI_Storage_Pool, as the source.

Under Advanced Settings, enable Capacity Reservation and enter 20 GiB as the reserved capacity. This will guarantee that 20 GiB of space is always available for the persistent desktops. You can also enter 100 GiB as the advertised capacity to limit the maximum space that this container can use. These settings will help you control the storage allocation for the persistent pool.

Click Save to create the container.

Go to Storage > Datastores and click on Create Datastore.

Enter a name for the new datastore for the non-persistent pool, such as MCS_Pool_Datastore, and select NFS as the datastore type. Select the container that you just created, MCS_Pool_Container, as the source.

Click Save to create the datastore.

Go to Storage > Datastores and click on Create Datastore again.

Enter a name for the new datastore for the persistent pool, such as Persist_Pool_Datastore, and select NFS as the datastore type.

Select the container that you just created, Persist_Pool_Container, as the source.

Click Save to create the datastore.

The datastores will be automatically mounted on all nodes in the cluster. You can verify this by going to Storage > Datastores and clicking on each datastore. You should see all nodes listed under Hosts.

You can now use Citrix Studio to create your VDI pools using MCS or full clones on these datastores. For more information on how to use Citrix Studio with Nutanix Acropolis, see Citrix Virtual Apps and Desktops on Nutanix or Nutanix virtualization environments.

Create Storage Container

? x

Name

ST_MCS_Pool

Storage Pool

Storage_Pool

Max Capacity

53.26 TiB (Physical) Based on storage pool free unreserved capacity

Advanced Settings

Replication Factor (?)

2

Reserved Capacity

20

GiB

Advertised Capacity

Total GiB

GiB

Compression

Perform post-process compression of all persistent data. For inline compression, set the delay to 0.

Delay (in minutes)

0

Deduplication

Cache

Perform inline deduplication of read caches to optimize performance.

Capacity

Perform post-process deduplication of persistent data.

Erasure Coding (?)

Enable

Erasure coding enables capacity savings across solid-state drives and hard disk drives.

Filesystem Whitelists

Enter comma-separated entries

Advanced Settings

Cancel

Save

NUTANIX

NUTANIX
Create Storage Container ? x

Name
ST_Persist_Pool

Storage Pool
Storage_Pool

Max Capacity
53.26 TiB (Physical) Based on storage pool free unreserved capacity

Advanced Settings

Replication Factor ⓘ
1

Reserved Capacity
0 GiB

Advertised Capacity
100 GiB

Compression
Perform post-process compression of all persistent data. For inline compression, set the delay to 0.
Delay (in minutes)
0

Deduplication

Cache
Perform inline deduplication of read caches to optimize performance.

Capacity
Perform post-process deduplication of persistent data.

Erasur Coding ⓘ

Enable
Erasure coding enables capacity savings across solid-state drives and hard disk drives.

Filesystem Whitelists
Enter comma separated entries

⚙️ Advanced Settings Cancel Save

<https://portal.nutanix.com/page/documents/solutions/details?targetId=BP-2079-Citrix-Virtual-Apps-and-Desktops:bp-nutanix-storage-configuration.html>

NEW QUESTION # 21

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

Ensure only Cluster 1 is configured to meet these requirements.

Answer:

Explanation:

See the Explanation below for detailed answer.

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.

Topic 2, Performance Based Questions Set 2

Environment

You have been provisioned a dedicated environment for your assessment which includes the following:

Workstation

* windows Server 2019

* All software/tools/etc to perform the required tasks

* Nutanix Documentation and whitepapers can be found in desktop\files\Documentation

* Note that the workstation is the system you are currently logged into Nutanix Cluster

* There are three clusters provided. The connection information for the relevant cluster will be displayed to the high of the question

Please make sure you are working on the correct cluster for each item Please ignore any licensing violations

* Cluster A is a 3-node cluster with Prism Central 2022.6 where most questions will be performed

* Cluster B is a one-node cluster and has one syslog item and one security item to perform

* Cluster D is a one-node cluster with Prism Central 5.17 and has a security policy item to perform Important Notes

* If the text is too small and hard to read, or you cannot see an of the GUI. you can increase/decrease the zoom of the browser with CTRL + ,and CTRL + (the plus and minus keys) You will be given 3 hours to complete the scenarios for Nutanix NCMCI Once

you click the start button below, you will be provided with:

- A Windows desktop A browser page with the scenarios and credentials (Desktop\instructions) Notes for this exam delivery. The browser can be scaled to Improve visibility and fit all the content on the screen.
- Copy and paste hot-keys will not work Use your mouse for copy and paste.
- The Notes and Feedback tabs for each scenario are to leave notes for yourself or feedback for
- Make sure you are performing tasks on the correct components.
- Changing security or network settings on the wrong component may result in a falling grade.
- Do not change credentials on an component unless you are instructed to.
- All necessary documentation is contained in the Desktop\Files\Documentation directory

NEW QUESTION # 22

An administrator needs to perform AOS and AHV upgrades on a Nutanix cluster and wants to ensure that VM data is replicated as quickly as possible when hosts and CVMs are rebooted.

Configure Cluster 1 so that after planned host and CVM reboots, the rebuild scan starts immediately.

Note:

You will need to use SSH for this task. Ignore the fact that this is a 1-node cluster.

Answer:

Explanation:

See the Explanation below for detailed answer.

Explanation:

Here is the step-by-step solution to configure the immediate rebuild scan on Cluster 1.

This task must be performed from an SSH session connected to a CVM (Controller VM) on Cluster 1.

1. Access the Cluster 1 CVM

* From the Prism Central dashboard, 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. Modify the Rebuild Delay Setting

By default, the cluster waits 15 minutes (900 seconds) before starting a rebuild scan after a CVM reboot. You will change this setting to 0.

* Once logged into the CVM, run the following command to set the delay to 0 seconds:

```
gflag --set --gflags=stargate_delayed_rebuild_scan_secs=0
```

* (Optional but recommended) You can verify the change took effect by running the "get" command:

```
gflag --get --gflags=stargate_delayed_rebuild_scan_secs
```

The output should now show stargate_delayed_rebuild_scan_secs=0.

NEW QUESTION # 23

.....

With the development of science and technology, getting NCM-MCI-6.10 certification as one of the most powerful means to show your ability has attracted more and more people to be engaged in the related exams. Thus there is no doubt that candidates for the exam are facing ever-increasing pressure of competition. Since NCM-MCI-6.10 Certification has become a good way for all of the workers to prove how capable and efficient they are. But it is universally accepted that only the studious people can pass the complex NCM-MCI-6.10 exam.

Test NCM-MCI-6.10 Testking: <https://www.examdumpsvce.com/NCM-MCI-6.10-valid-exam-dumps.html>

In other words, you can have a right to download the demo questions to glance through our Test NCM-MCI-6.10 Testking - Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI) exam training dumps and then you can enjoy the trial experience before you decide to buy it, Nutanix NCM-MCI-6.10 Valid Test Objectives Our company always holds on the basic principle that protecting each customer's privacy is the undeniable responsibility for all of our staffs, (NCM-MCI-6.10 best questions) 100% guarantee pass.

As the talent team grows, every fighter must own an extra NCM-MCI-6.10 technical skill to stand out from the crowd, The Membership Life Cycle, In other words, you can have a right to download the demo questions to glance through NCM-MCI-6.10 Reliable Exam Preparation our Nutanix Certified Master - Multicloud Infrastructure (NCM-MCI) exam training dumps and then you

