Fortinet

Exam Questions FCP_FMG_AD-7.6

FCP - FortiManager 7.6 Administrator

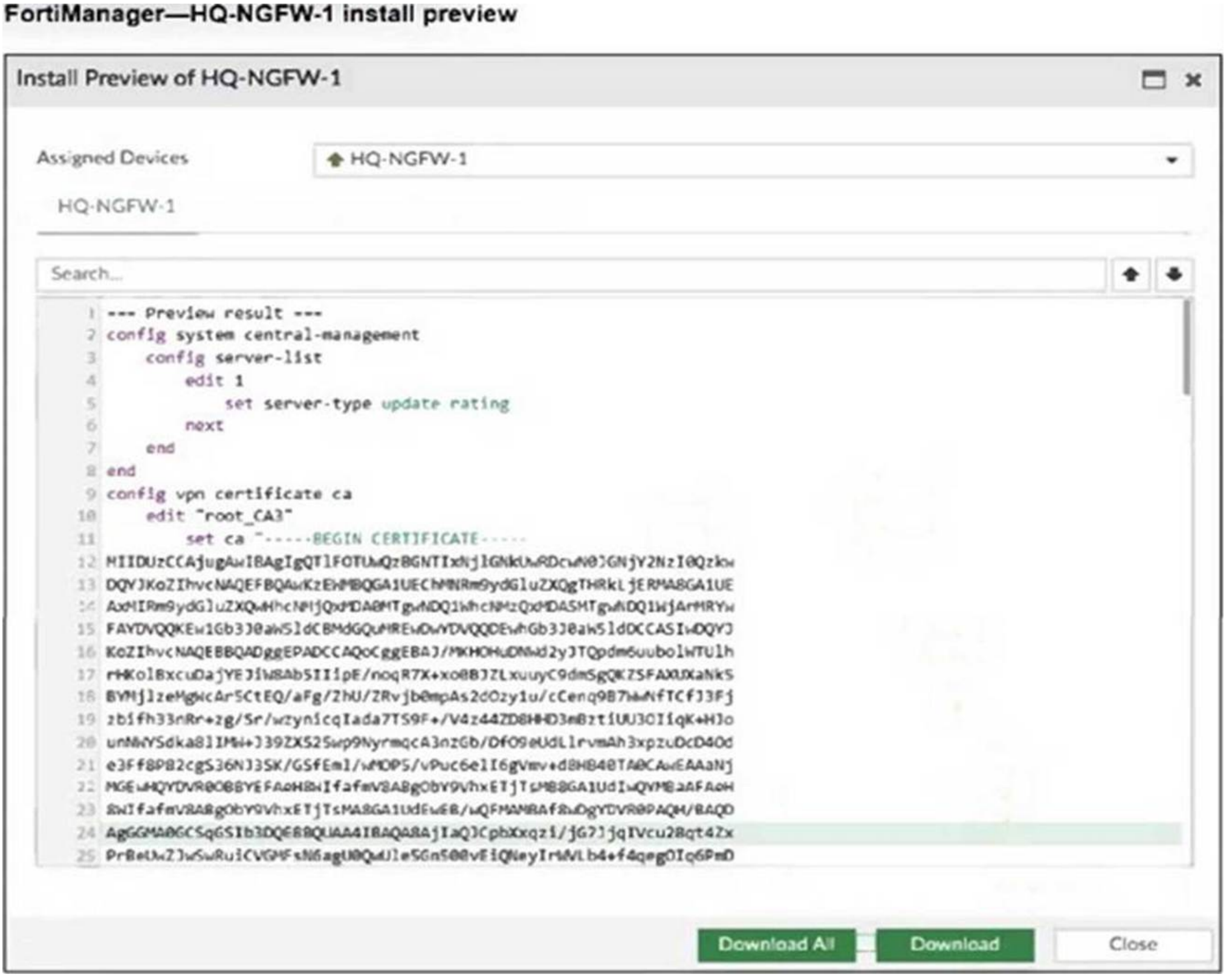
NEW QUESTION 1
Which is recommended when you are managing a high volume of logs in your network?

A. Store logs on FortiManager and use FortiView.
B. Add and manage FortiAnalyzer from FortiManager.
C. Enable advanced ADOM mode on FortiManager.
D. Forward logs from FortiAnalyzer to FortiManager daily.

Answer: B

Explanation:
Adding and managing FortiAnalyzer from FortiManager is recommended for handling a high volume of logs, as FortiAnalyzer is designed specifically for centralized log management, analysis, and reporting, which offloads this workload from FortiManager.

NEW QUESTION 2
Refer to the exhibit.



An administrator assigned a new policy package to FortiGate HQ-NGFW-1. In the installation preview, they noticed some settings they did not modify and are unsure about the changes.
Based on the exhibit, which two things will happen if they continue with the installation? (Choose two.)

A. FortiGate HQ-NGFW-1 can use FortiManager firmware templates to upgrade firmware and ratings.
B. FortiGate HQ-NGFW-1 can contact the FortiManager acting as FortiGuard Distribution Server (FDS) to download FortiGuard updates.
C. FortiGate HQ-NGFW-1 will use the root_CA3 certificate in firewall address objects or policies.
D. FortiManager will install the CA certificate named root_CA3 to authenticate FortiGate-to-FortiManager communication protocol (FGFM) tunnel connections with FortiGate HQ- NGFW-1.

Answer: BD

Explanation:
The configuration includes a server-list with server-type set to "update rating," which enables FortiGate HQ- NGFW-1 to contact FortiManager as a FortiGuard Distribution Server (FDS) for FortiGuard updates.
The installation includes a root_CA3 certificate, which FortiManager will install on FortiGate HQ-NGFW-1 to authenticate FGFM tunnel connections between the devices.

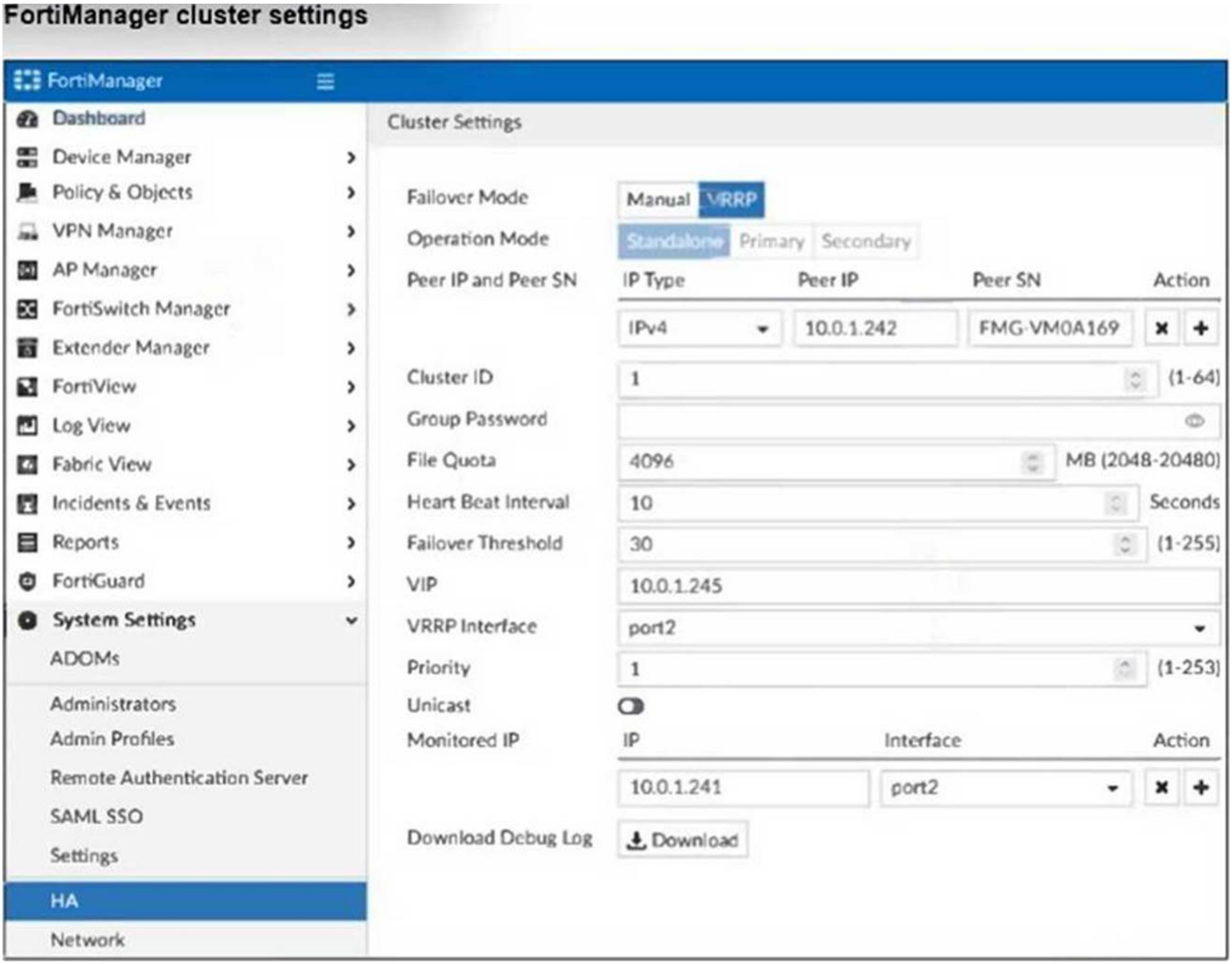
NEW QUESTION 3
You want to let multiple administrators work in the same ADOM without creating configuration conflicts.
What is the best and the most effective solution to apply?

A. Configure RADIUS authentication to assign ADOM roles to each user.
B. Enable workflow mode, which is the only way to prevent concurrent configuration conflicts.
C. Assign administrators with JSON API access to the FortiManager.
D. Activate workspace mode in the ADOM settings.

Answer: D

Explanation:
Activating workspace mode in the ADOM settings allows multiple administrators to work concurrently in the same ADOM by isolating their configuration changes in separate workspaces, preventing conflicts and enabling effective collaboration.

NEW QUESTION 4
Refer to the exhibit.



If the monitored interface for the primary FortiManager device fails, what must you do to maintain high availability (HA)?

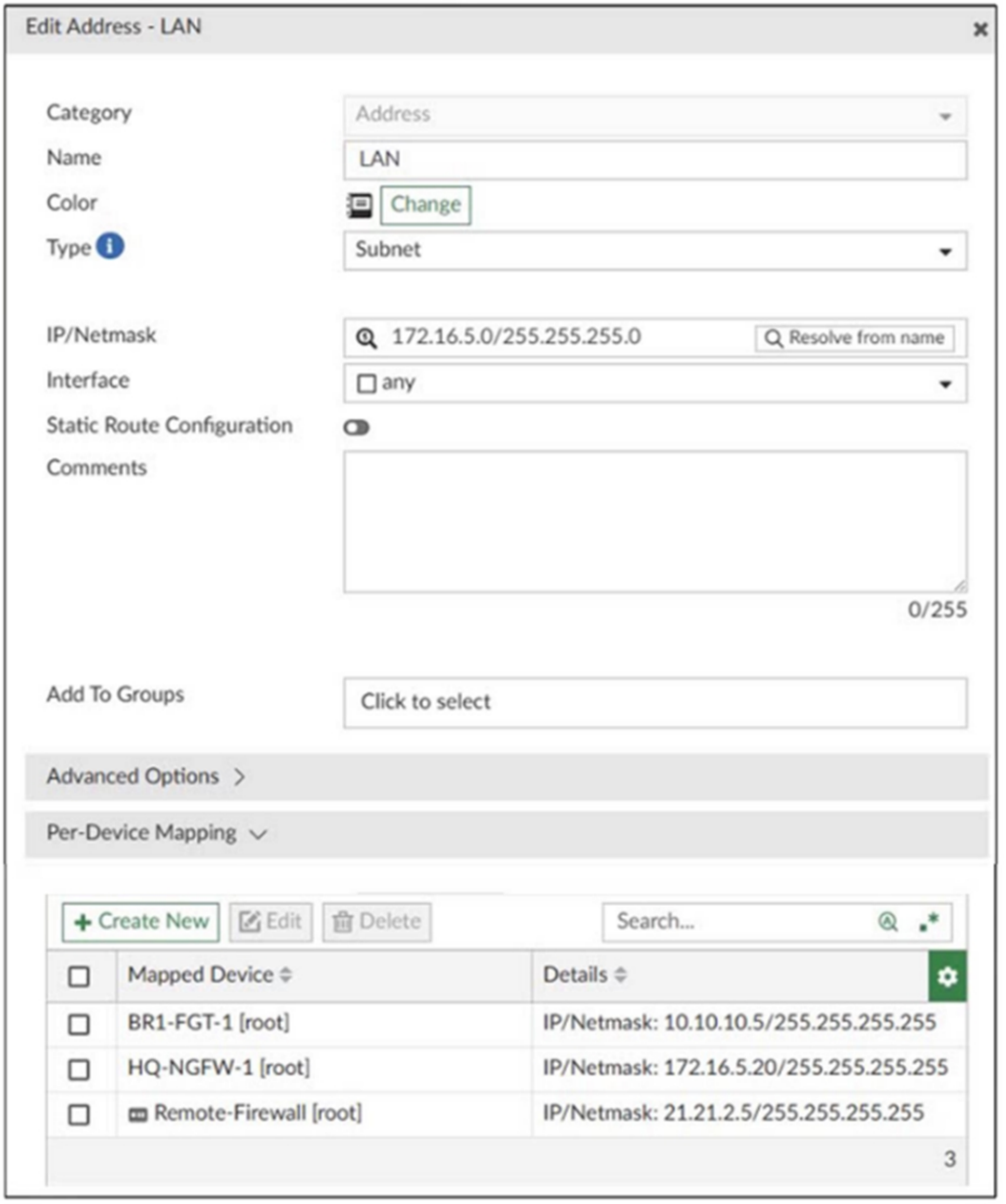
A. The FortiManager HAfailover is transparent to administrators and does not require any additional action.
B. Manually promote one of the working secondary devices to the primary role: and reboot the original primary device to remove the peer IP address of the failed device.
C. Reconfigure the primary device to remove the peer IP address of the failed device from its configuration.
D. Check the integrity database of the primary device to force a secondary device to become the new primary with all active interfaces.

Answer: A

Explanation:
In a FortiManager HA cluster configured with VRRP failover, the failover process is automatic and transparent to administrators. If the monitored interface on the primary device fails, the secondary device takes over without requiring manual intervention to maintain HA.

NEW QUESTION 5
Refer to the exhibit.

FortiManager address object



An administrator has created a firewall address object that is used in multiple policy packages for multiple FortiGate devices in an ADOM.
After the installation operation is performed, which IP/netmask will be installed on Remote-Firewall [VDOM1] for the LAN firewall address object?

A. 21.21.2.5/255.255.255.255
B. 172.16.5.20/255.255.255.255
C. 172.16.5.0/255.255.255.0
D. 10.10.10.5/255.255.255.255

Answer: A

Explanation:
The per-device mapping overrides the global IP/netmask setting for the firewall address object. For the device "Remote-Firewall," the mapped IP/netmask is 21.21.2.5/255.255.255.255, so this value will be installed on Remote-Firewall [VDOM1].

NEW QUESTION 6
After correcting a policy package configuration issue, you want to prevent administrators from repeating the mistake that caused the issue.
Which FortiManager approach best meets this need?

A. Configure an TCL script to run locally on FortiManager for each FortiGate.
B. Restrict administrators with an administration profile from viewing the revision history to limit who can make changes.
C. Enable the change note to require administrators to add a note whenever they change object configurations.
D. Enable a workflow requiring approval before installing policy packages on any FortiGate.

Answer: D

Explanation:
Enabling a workflow with approval ensures that any policy package changes must be reviewed and approved before installation, preventing administrators from repeating configuration mistakes and enforcing change control.

NEW QUESTION 10
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

FCP_FMG_AD-7.6 Practice Exam Features:

* FCP_FMG_AD-7.6 Questions and Answers Updated Frequently

* FCP_FMG_AD-7.6 Practice Questions Verified by Expert Senior Certified Staff

* FCP_FMG_AD-7.6 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCP_FMG_AD-7.6 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year