Fortinet
FCP_FMG_AD-7.6
Fortinet NSE 5 - FortiManager 7.6 Administrator

For More Information – Visit link below:
https://www.examsempire.com/

Product Version

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

Latest Version: 8.2

Question: 1

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?

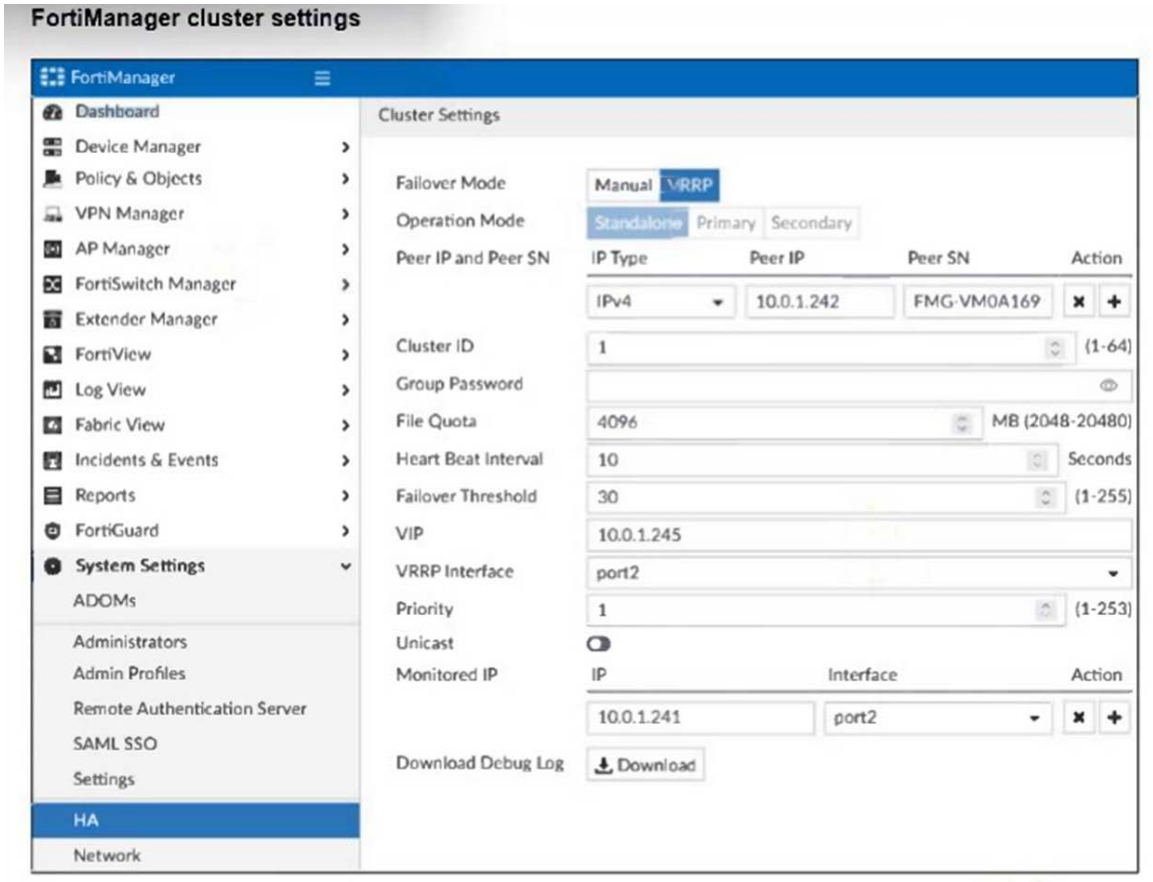
A. Configure RADIUS authentication to assign ADOM roles to each user.
B. Enable workflow mode, which is the only way to prevent concurrent configuration conflicts.
C. Assign administrators with JSON API access to the FortiManager.
D. Activate workspace mode in the ADOM settings.

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.

Question: 2

Refer to the exhibit.



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

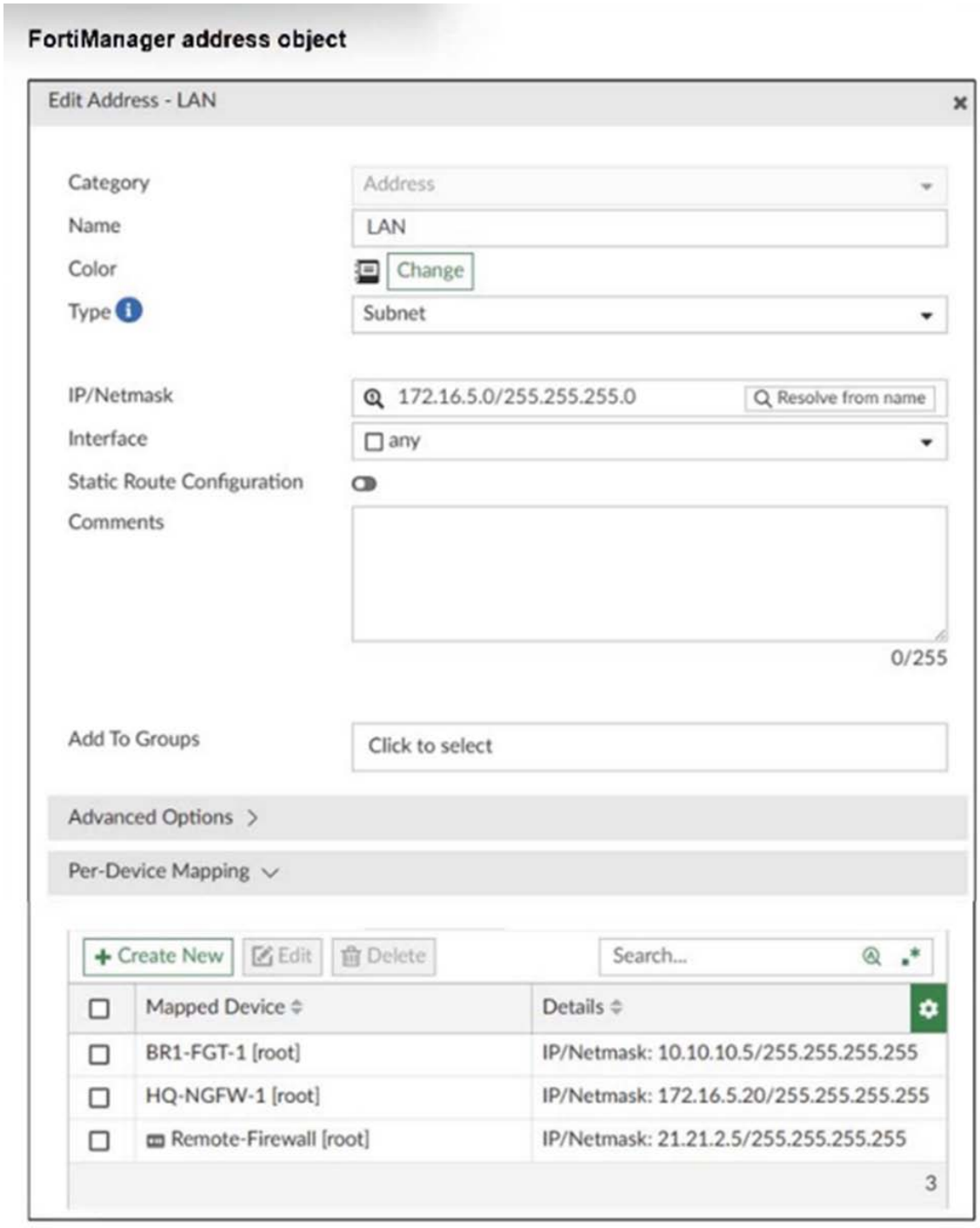
A. The FortiManager HA failover is transparent to administrators and does not require any additional action.
B. Manually promote one of the working secondary devices to the primary role: and reboot the original primary device to remove the peer IP address of the failed device.
C. Reconfigure the primary 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.

Question: 3

Refer to the exhibit.



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?

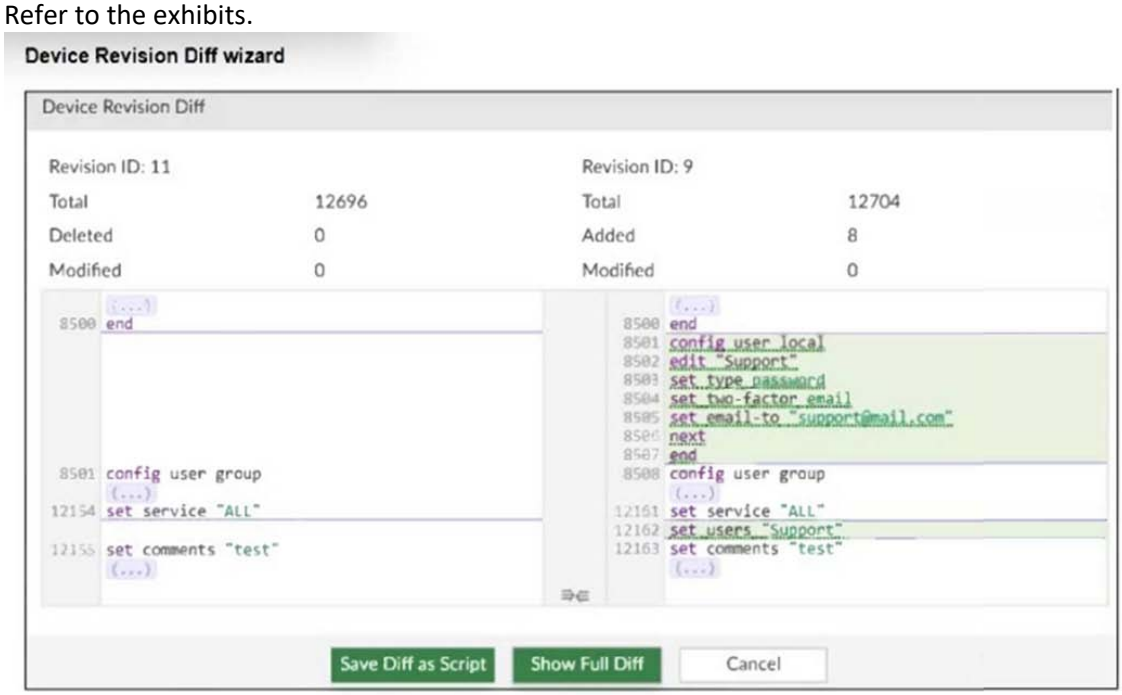
A. 21.21.2.5/255.255.255.255
B. 172.16.5.20/255.255.255.255
C. 172.16.5.0/255.255.255.0
D. 10.10.10.5/255.255.255.255

Answer: C

Explanation:
The exhibit shows the default value of the LAN address object as 172.16.5.0/255.255.255.0. It also shows Per-Device Mapping entries only for BR1-FGT-1 [root], HQ-NGFW-1 [root], and Remote-Firewall [root]. There is no mapping shown for Remote-Firewall [VDOM1].
The FortiManager 7.6 Administrator Study Guide gives the exact rule: “The devices in the ADOM that do not have a dynamic mapping for LAN have a default value.” It also states that dynamic mappings are configured per device in the Per-Device Mapping section.
Since Remote-Firewall [VDOM1] does not have its own mapping entry, it will use the object’s default value, which is 172.16.5.0/255.255.255.0.

Question: 4

Refer to the exhibits.



CLI output

```
FortiManager # diagnose dvm device list
--- There are currently 6 devices/vdoms managed ---
--- There are currently 6 devices/vdoms count for license ---

TYPE            OID    SN              HA      IP              NAME            ADOM     IPS                FIRMWARE        HW_GenX
fmgfaz-managed  188    FGVM02TM24013504 -      100.65.1.111    BR1-FGT-1       My_ADOM  7.0 MR6 (3401)  N/A
                |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: installed; conn: up; template:[installed]default
                |- vdom:[3]root flags:0 adom:My_ADOM pkg:[unknown]BR1-FGT-1
```

An administrator needed to recover all the configurations related to the user, Support. The configurations were saved in configuration revision ID 9.
The administrator reverted the configuration using the Configuration Revision History window and received the CLI output shown in the exhibit.
What can you conclude from the CLI output?

A. The administrator set the flag to 0 to prevent configuration overrides.
B. The administrator reinstalled the policy package.
C. The administrator needs to retrieve the device to correctly detect the FortiGate firmware version.
D. The administrator installed only the device-level configuration.

Answer: D

Explanation:
The correct answer is D. The exact extract from the study guide says a revert operation "Reverts only the device database to the previous revision" and "Does not revert policies and objects—you must import them." It further states: "Performing a revert operation followed by an installation only reverts device-level changes and does not revert policy packages."
That exactly matches the CLI output. The device shows the device manager portion as installed and synchronized, while the policy package appears as unknown, which indicates the revert and installation affected the device-level configuration only. It did not reinstall or synchronize the policy package. Therefore B is incorrect. A is unsupported by the source, and C is unrelated because the firmware version is already shown in the device list output. The study guide also states that after revert you must use Import Configuration to synchronize policy information.

Question: 5

An administrator wants to configure and manage multiple objects in the FortiManager database and give access to other users who work in the same database.
To stay in control of the changes made to firewall policies by other team members, the administrator needs a setup where all modifications go through a central check before they can be installed.
How can the administrator create this setup?

A. Enable the prompt asking the administrator to accept firewall policies changes before saving.
B. Enable the workspace (for all ADOMs) to control all changes made by any administrator.
C. Enable device lock and the advanced mode feature in the ADOM.
D. Enable workflow mode and the ADOM lock feature.

Answer: D

Explanation:

Enabling workflow mode along with the ADOM lock feature ensures that all configuration changes go through a centralized review and approval process before installation, allowing controlled and coordinated management of firewall policies by multiple administrators.

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/