Fortinet

Exam Questions FCP_FMG_AD-7.6

FCP - FortiManager 7.6 Administrator

NEW QUESTION 1
Refer to the exhibits.

Diagnose output

```
FortiManager # get system status
Platform Type                    : FMG-VM64-KVM
Platform Full Name               : FortiManager-VM64-KVM
Version                          : v7.6.1-build3344 241023 (GA.M)
Serial Number                    : FMG-VMTM24012945
BIOS version                     : 04000002
```

Diagnose output

```
FortiManager # diagnose dvm device list
--- There are currently 5 devices/vdoms managed ---
--- There are currently 5 devices/vdoms count for license ---

TYPE            OID    SN                HA      IP              NAME               ADOM     IPS                FIRMWARE
fmgfaz-managed  230    FGVM02TM24013423  -       10.0.13.254     FGVM02TM24013423   root     7.0 MR6 (3401)  N/A
                |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; conn: up
                |- vdom:[3]root flags:0 adom:root pkg:[never-installed]
unregistered    167    FGVM02TM24013501  -       192.168.1.3     FGVM02TM24013501   root     7.0 MR6 (3401)  N/A
                |- STATUS: dev-db: unknown; conf: out of sync; cond: unregistered; dm: none; conn: unknown
                |- vdom:[3]root flags:0 adom:root pkg:[never-installed]
unregistered    209    FGVM02TM24013502  -       192.168.1.101   FGVM02TM24013502   root     7.0 MR6 (3401)  N/A
                |- STATUS: dev-db: unknown; conf: out of sync; cond: unregistered; dm: none; conn: unknown
                |- vdom:[3]root flags:0 adom:root pkg:[never-installed]
unregistered    188    FGVM02TM24013504  -       192.168.1.111   FGVM02TM24013504   root     7.0 MR6 (3401)  N/A
                |- STATUS: dev-db: unknown; conf: out of sync; cond: unregistered; dm: none; conn: unknown
                |- vdom:[3]root flags:0 adom:root pkg:[never-installed]
fmgfaz-model    262                    -                       HQ-NGFW            My_ADOM  7.0 MR6 (3401)  N/A
                |- STATUS: dev-db: unknown; conf: unknown; cond: unknown; dm: unknown; conn: unknown
                |- vdom:[3]root flags:0 adom:My_ADOM pkg:[never-installed]

FortiManager # diagnose test deploymanager reloadconf 262
Retriving configuration file from FGT...
Error: Configuration file import error.
```

An administrator runs the reload failure commanddiagnose test deploymanager reloadconf 262on FortiManager.
Why does the administrator receive an error message?

A. The administrator must use the FortiGate name instead of the ID number.
B. The administrator just recently added FortiGate HQ-NGFW as a model device.
C. FortiManager requires the FortiGate serial number instead of the ID number.
D. FortiManager does not support FortiOS version 7.0.

Answer: B

Explanation:
The error occurs because the FortiGate HQ-NGFW device with ID 262 is a newly added model device and has not yet been fully synchronized or installed with a configuration package, which causes the reload configuration command to fail.

NEW QUESTION 2
The administrator uses FortiManager to push a CLI script using the Remote FortiGate Directly (via CLI) option to configure an IPsec VPN. However, when running the script, the administrator receives the following error:
config vpn ipsec phase2-interface [parameter(s) invalid. detail: object mismatch]
What must the administrator do to resolve the script error and successfully apply the IPsec configuration?

A. Add the end command after finishing the IPsec phase 1-interface configuration block.
B. Use IPsec templates to deploy provisioning templates.
C. Add a second config vpn ipsec phase2-interface block without linking it to phase1.
D. Run the script using the policy package or ADOM database method.

Answer: D

Explanation:
Running the script through the policy package or ADOM database method allows FortiManager to properly interpret object relationships and dependencies in the IPsec configuration, preventing object mismatch errors when pushing complex VPN settings directly via CLI.

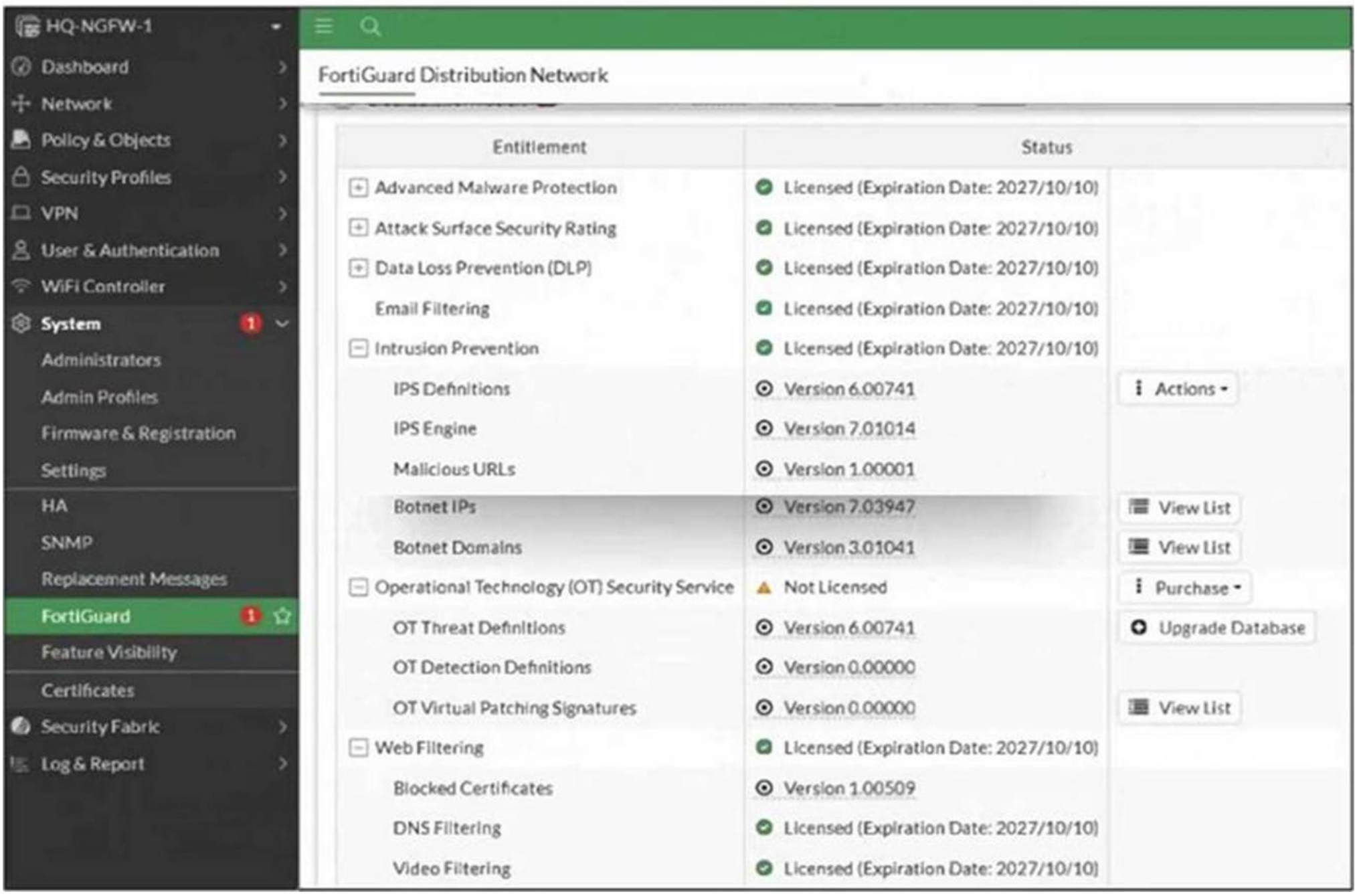
NEW QUESTION 3
An administrator has a FortiGate-HQ device with VDOMs—root, HR and Facilities, currently managed under the FortiManager ADOM—Site1. They try to move VDOM HR to the FortiManager ADOM—Site2, but it does not work.
Why is the administrator not able to move FortiGate-HQ VDOM HR to FortiManager ADOM—Site2?

A. The FortiGate-HQ must be managed under the FortiManager ADOM—root to allow moving its VDOMs to different ADOMs.
B. The administrator must have full access in the device layer of FortiGate-HQ VDOM-root before they can VDOMs to different ADOMs.
C. FortiManager must be in ADOM normal mode, which does not allow VDOMs to be managed separately.
D. The administrator must delete the FortiGate-HQ device from FortiManager and add it again using the Add Device wizard before moving the VDOM.

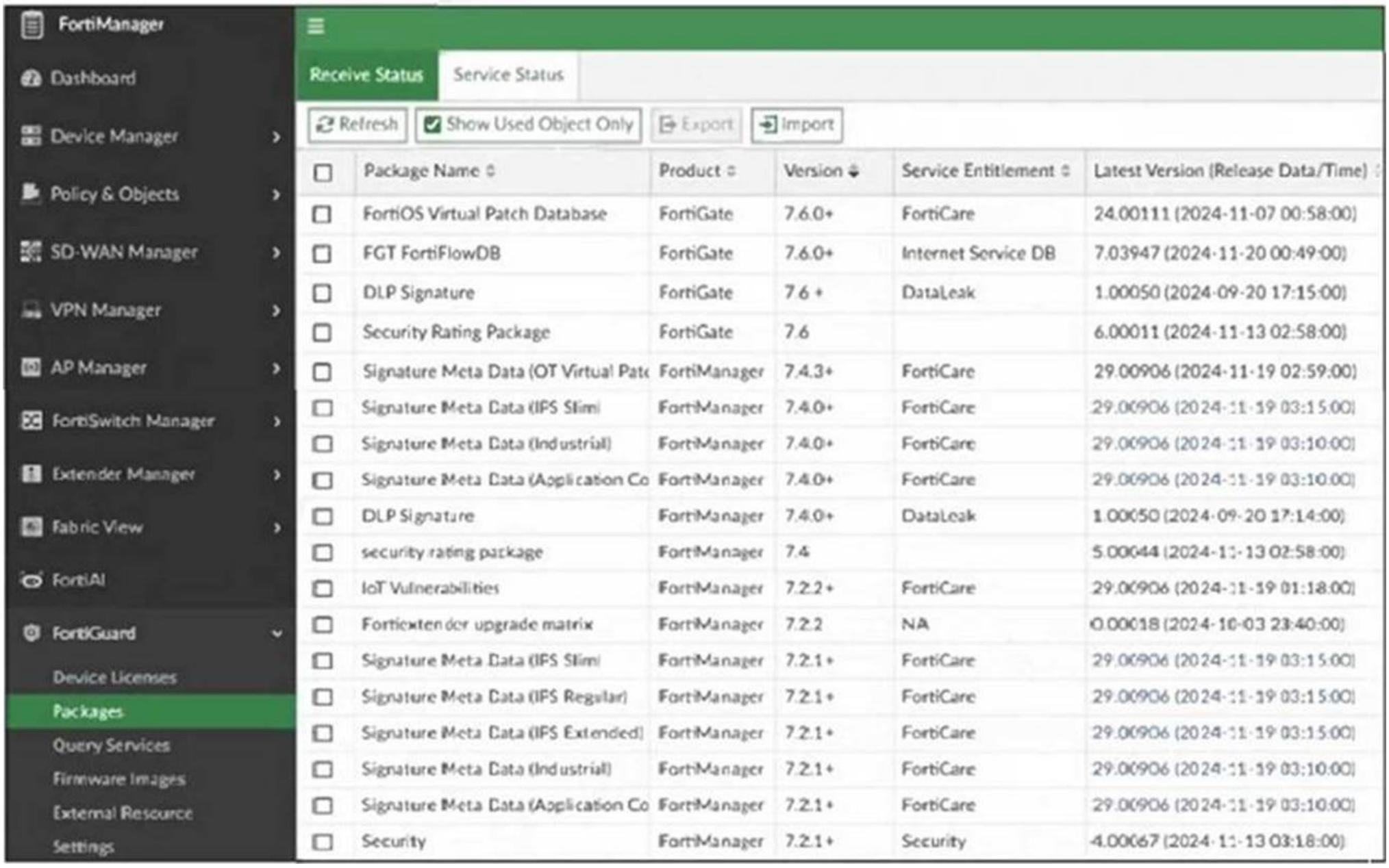
Answer: A

Explanation:
FortiGate devices must be managed under the FortiManager ADOM corresponding to the root VDOM to allow their individual VDOMs to be moved and managed in different ADOMs. Managing the root VDOM in a different ADOM prevents moving subordinate VDOMs across ADOMs.

NEW QUESTION 4
Refer to the exhibits
FortiGate GUI—FortiGuard



FortiManager GUI—FortiGuard



FortiGate CLI—Central management

```
HQ-NGFW-1 (central-management) # sh
config system central-management
    set type fortimanager
    set allow-push-firmware disable
    set allow-remote-firmware-upgrade disable
    set serial-number "FMG-VMTM24012945"
    set fmg "::ffff:10.0.13.120"
    config server-list
        edit 1
            set server-type update
            set server-address 192.168.1.120
        next
    end
    set include-default-servers disable
end
```

FortiGate HQ-NGFW-1 downloads and validates FortiGuard databases from FortiManager which acts as a local FortiGuard Distribution Server (FDS) in a closed network. An administrator pushes a new firewall policy with an intrusion prevention system (IPS) profile from FortiManager to FortiGate HQ- NGFW-1 However, FortiGate does not recognize the new IPS signature from FortiManager.
What is the most likely reason why FortiGate HQ-NGFW-1 does not recognize the new IPS signature?

A. FortiGate must enable rating for the FortiManager IP address, 192.168.1.120, in server list 1.
B. FortiManager and FortiGate have different IPS database versions.
C. The administrator must enable IPv6 connections for FortiGuard services on FortiManager.
D. The administrator must enable the fortiguard-anycast option to correctly download all signatures from the local FDS.

Answer: B

Explanation:
The most likely reason FortiGate HQ-NGFW-1 does not recognize the new IPS signature is that FortiManager and FortiGate have different IPS database versions. The FortiManager may have pushed a signature update that FortiGate has not yet synchronized or validated locally, causing the signature to be unrecognized.

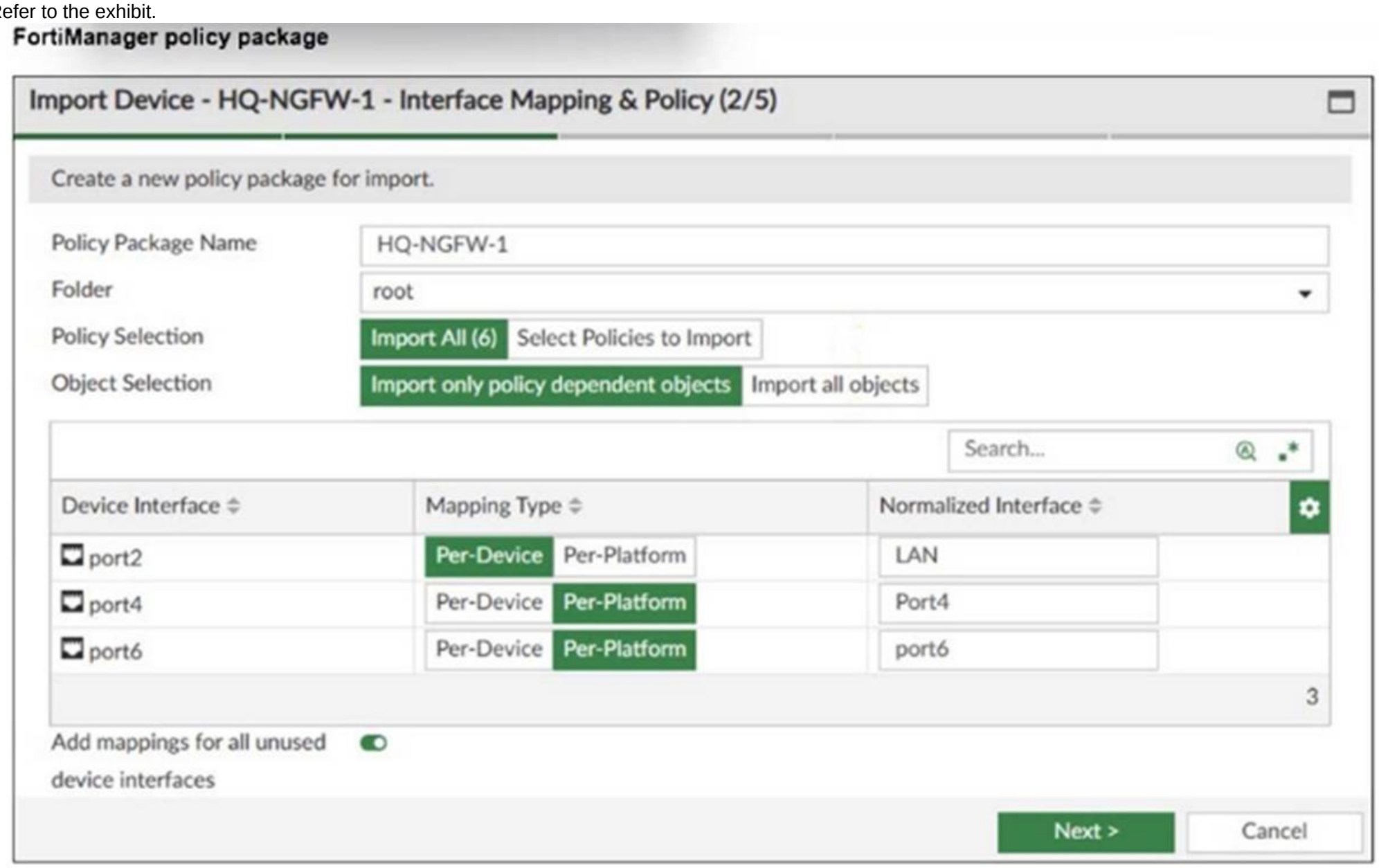
NEW QUESTION 5
Which is recommended when you are managing a high volume of logs in your network?

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 6
Refer to the exhibit.



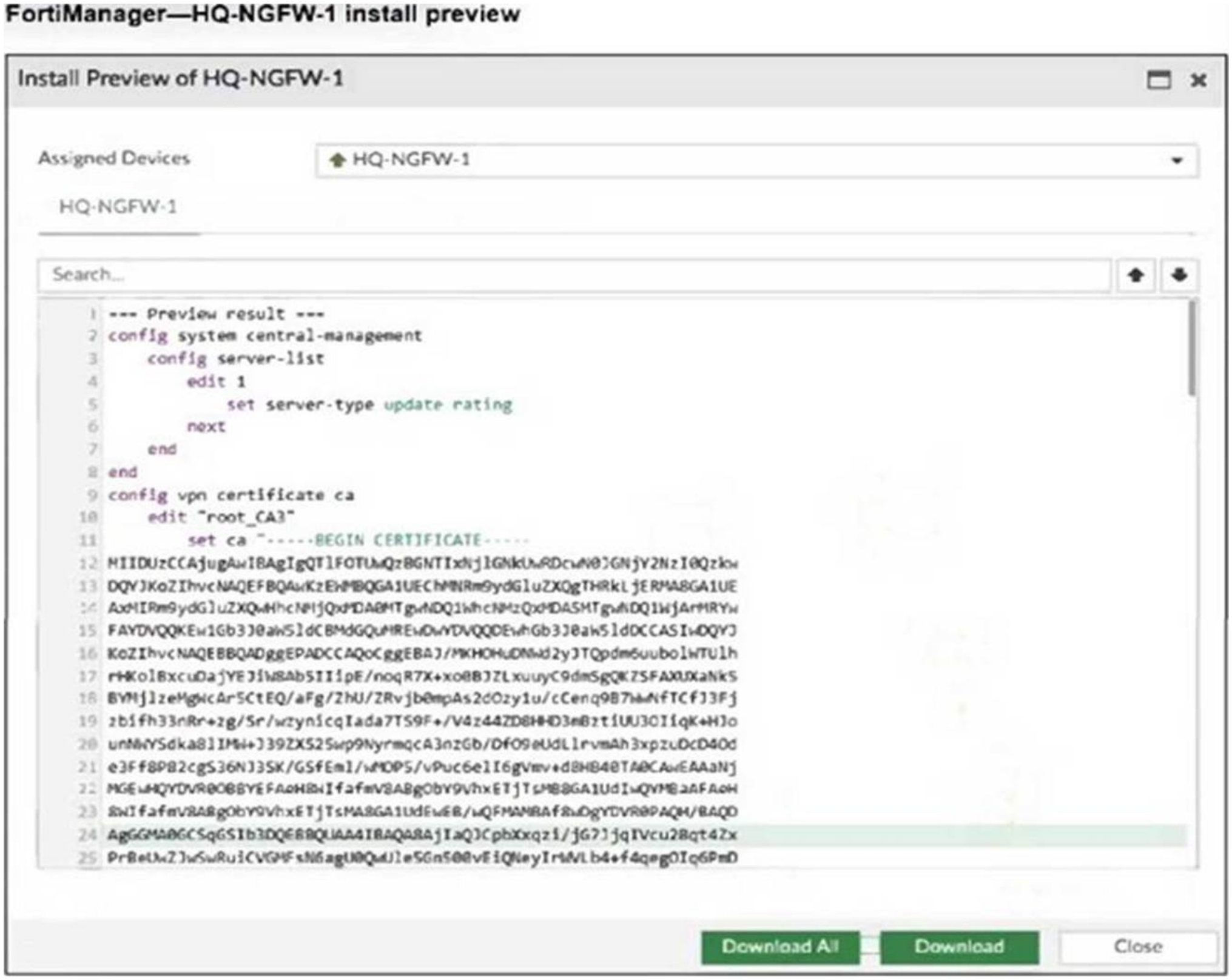
An administrator added a FortiGate device to FortiManager with the default object settings at the ADOM layer.
What can you conclude from the import policy package process of the HQ-NGFW- 1 device?

A. The administrator must select Per Platform for all interfaces to correctly detect all interfaces from HQ- NGFW-1.
B. The administrator must manually create the port4 interface on the ADOM layer to avoid import policy errors.
C. FortiManager will create LAN, port4, and port6 as normalized interfaces at the ADOM layer.
D. FortiGate may not work as expected when the administrator does not import all objects.

Answer: C

Explanation:
The import process shows that FortiManager will create normalized interfaces named LAN, port4, and port6 at the ADOM layer, mapping them to the corresponding device interfaces based on the import settings.

NEW QUESTION 7
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 8
An administrator has assigned a global policy package to a new ADOM named ADOM1.
What will happen if the administrator tries to create a new policy package in ADOM1?

A. The administrator will be able to select the option to assign the global policy package to the new policy package.
B. FortiManager will automatically assign the global policy package to the new policy package.
C. FortiManager will automatically install policies on the policy package in ADOM1.
D. The administrator will have to assign the global policy package from the global ADOM.

Answer: A

Explanation:
When a global policy package is assigned to an ADOM, administrators creating new policy packages within that ADOM have the option to select and assign the global policy package to the new policy package if desired.

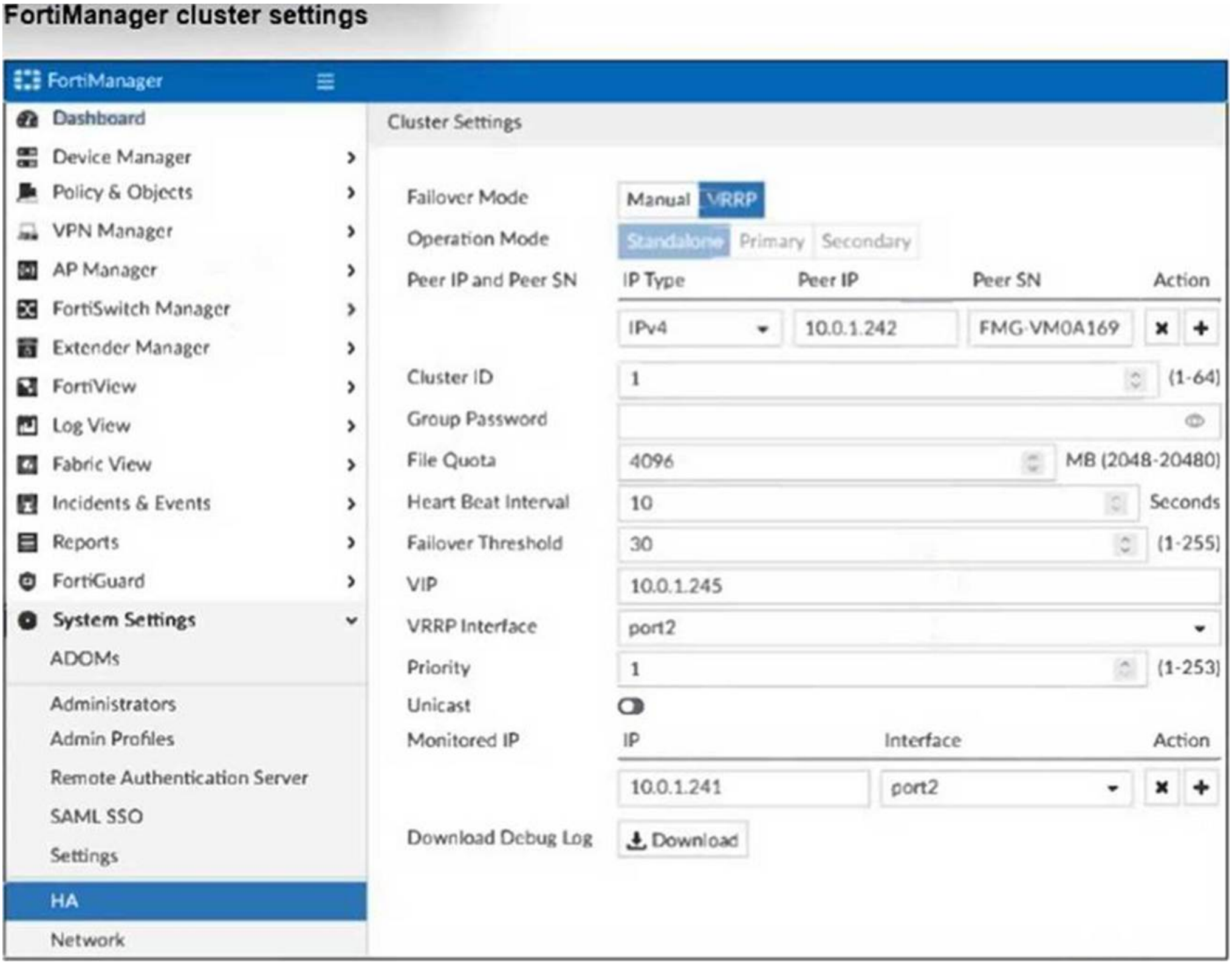
NEW QUESTION 9
What is the best explanation of how FortiManager helps with mass provisioning?

A. It upgrades the OS of each FortiGate device.
B. It provides local FortiGuard Distribution Server (FDS) services to the network.
C. It uses templates to configure the same settings on many devices simultaneously.
D. It sends email alerts when new devices connect.

Answer: C

Explanation:
FortiManager helps with mass provisioning by using templates that allow administrators to configure the same settings on multiple FortiGate devices simultaneously, streamlining deployment and management.

NEW QUESTION 10
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 10
Refer to the exhibit.

```
FortiManager # config system global
(global)# set workspace-mode normal
(global)# end
FortiManager #
```

What are two results from the configuration shown in the exhibit? (Choose two.)

A. Ungraceful closed sessions will keep the ADOM in a locked state until the administrator session times out.
B. The administrator can lock policy blocks and FortiManager global ADOM.
C. The same administrator can lock more than one ADOM at the same time.
D. The administrator must have access to the ADOM to approve changes.

Answer: AB

Explanation:
In normal workspace mode, ungraceful session closures will keep the ADOM locked until the session times out, preventing other administrators from editing. Normal workspace mode allows administrators to lock policy blocks and the global ADOM, providing granular locking control.

NEW QUESTION 13
Which output is displayed right after moving the ISFW device from one ADOM to another?
A)

```
FortiManager # diagnose dvm device list ISFW
--- There are currently 4 devices/vdoms managed ---
--- There are currently 4 devices/vdoms count for license ---

TYPE            OID   SN                HA   IP            NAME   ADOM   IPS                 FIRMWARE
fmgfaz-managed  325   FGVM010000077646  -    10.0.1.200    ISFW   ADOM76 7.00741 (regular)   7.0 MR6 (2463)
                |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: autoupdated; conn: up
                |- vdom:[3]root flags:1 adom:ADOM76 pkg:[out-of-sync]ISFW
```

B)

```
FortiManager # diagnose dvm device list ISFW
--- There are currently 4 devices/vdoms managed ---
--- There are currently 4 devices/vdoms count for license ---

TYPE            OID   SN                HA   IP            NAME   ADOM   IPS                 FIRMWARE
fmgfaz-managed  325   FGVM010000077646  -    10.0.1.200    ISFW   ADOM76 7.00741 (regular)   7.0 MR6 (2463)
                |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: installed; conn: up
                |- vdom:[3]root flags:0 adom:ADOM76 pkg:[imported]ISFW
```

C)

```
FortiManager # diagnose dvm device list ISFW
--- There are currently 4 devices/vdoms managed ---
--- There are currently 4 devices/vdoms count for license ---

TYPE            OID   SN                HA   IP            NAME   ADOM   IPS                 FIRMWARE
fmgfaz-managed  325   FGVM010000077646  -    10.0.1.200    ISFW   ADOM76 7.00741 (regular)   7.0 MR6 (2463)
                |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: installed; conn: up
                |- vdom:[3]root flags:0 adom:ADOM76 pkg:[never-installed]
```

D)

```
FortiManager # diagnose dvm device list ISFW
--- There are currently 4 devices/vdoms managed ---
--- There are currently 4 devices/vdoms count for license ---

TYPE            OID   SN                HA   IP            NAME   ADOM   IPS                 FIRMWARE
fmgfaz-managed  325   FGVM010000077646  -    10.0.1.200    ISFW   ADOM76 7.00741 (regular)   7.0 MR6 (2463)
                |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; conn: up
                |- vdom:[3]root flags:0 adom:ADOM76 pkg:[unknown]ISFW
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: C

Explanation:
Right after moving the ISFW device to a new ADOM, the status typically shows the policy package as never-installed, indicating that the device has been assigned to the new ADOM but no policy package has yet been installed in that ADOM.

NEW QUESTION 16
A service provider administrator has assigned a global policy package to a managed customer ADOM named My_ADOM. The customer administrator has access only to My_ADOM.
How can the customer administrator edit the global header policy of the global policy package?

A. The customer administrator can edit the header policy by using workspace mode on the global ADOM.
B. The customer administrator can edit the header policy by using workflow mode on the global ADOM and My_ADOM.
C. The service provider administrator can unlock the global policy from the global ADOM to authorize changes to the customer administrator.
D. The customer administrator cannot edit the global header policy; only the service provider administrator can make changes from the global ADOM.

Answer: D

Explanation:
The global policy package is managed only from the global ADOM by the service provider administrator. Customer administrators with access solely to their ADOM (My_ADOM) cannot edit the global header policy; such changes must be made by the service provider administrator in the global ADOM.

NEW QUESTION 18
.....

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

100% Actual & Verified — Instant Download, Please Click
Order The FCP_FMG_AD-7.6 Practice Test Here