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
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 3
Refer to the exhibit.

```
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: pending; dm: installed; conn: up; template:[modified]default
                |- vdom:[3]root flags:0 adom:My_ADOM pkg:[imported]BR1-FGT-1
```

Which two statements about the output are true? (Choose two.)

A. The latest revision history for the managed FortiGate does not match the device-level database.
B. Configuration changes have been installed on FortiGate, updating policy and device-level database.
C. The latest revision history for the managed FortiGate does match the FortiManager policy database.
D. The system template default will override device-level database configurations.

Answer: AD

Explanation:
The status "pending" indicates the latest revision history does not match the device-level database, meaning there are unapplied changes.
The template is marked as [modified], so the system template default will override device-level database configurations when installed.

NEW QUESTION 4
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.

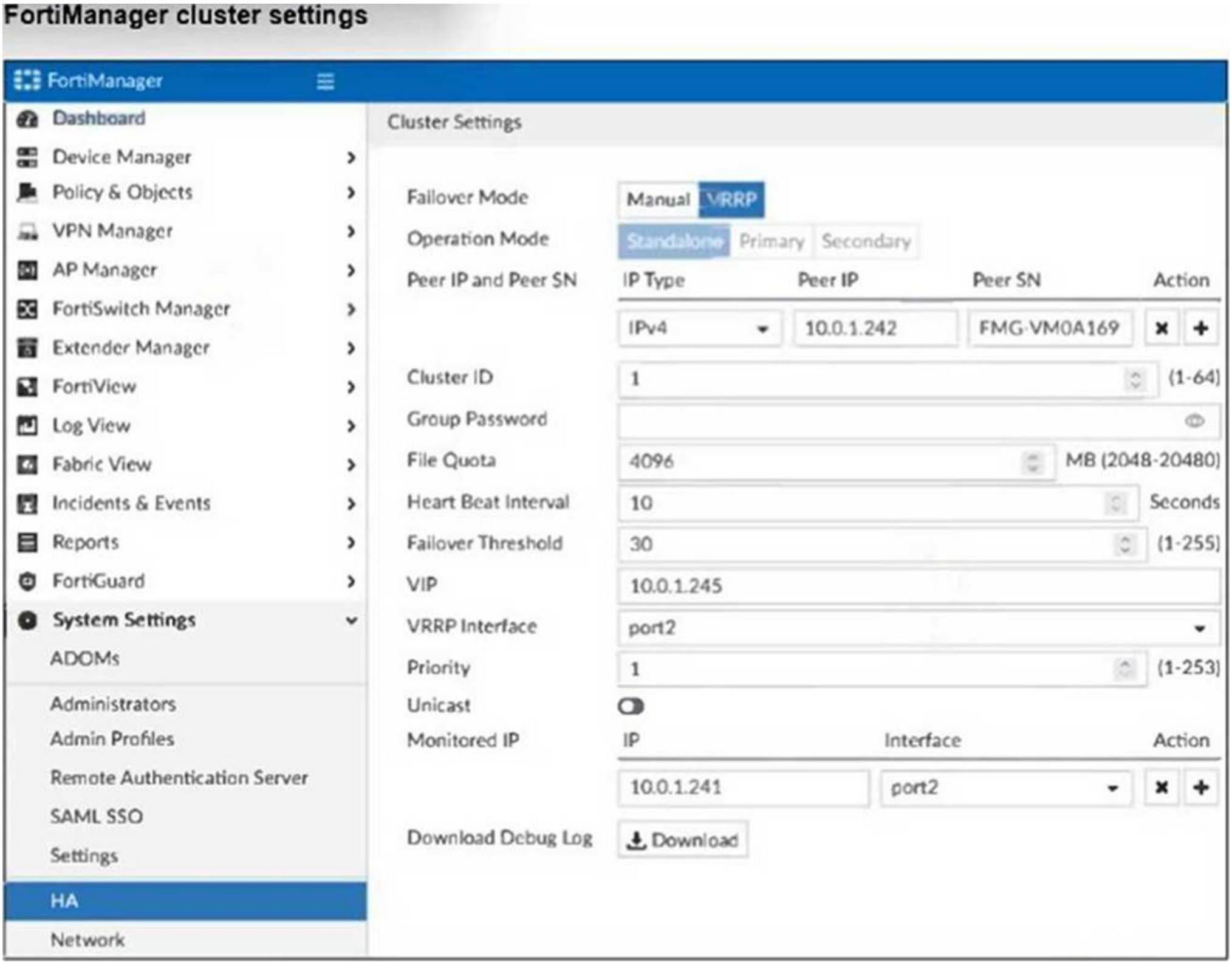
NEW QUESTION 5
You want to let multiple administrators work in the same ADOM without creating configuration conflicts.
What is the best and the most effective solution to apply?

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 6
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.

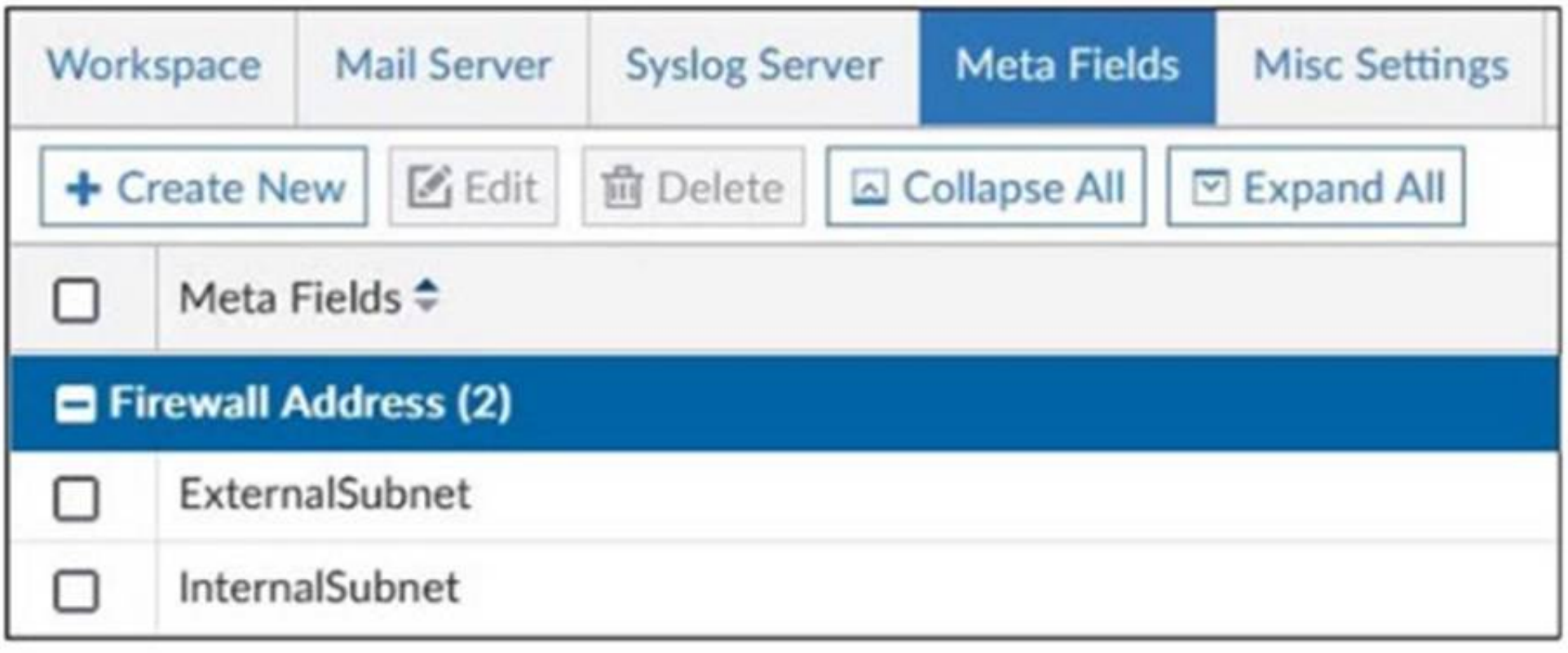
NEW QUESTION 7
Push updates are failing on a FortiGate device located behind a network address translation (NAT) device? Which two settings should the administrator check to correct this problem? (Choose two.)

A. Make sure the NAT device IP address and the correct ports are configured on FortiManager.
B. Make sure FortiGuard updates and web service are enabled on the FortiGuard service interface.
C. Make sure the virtual IP address and the correct ports are configured on the NAT device.
D. Make sure the Bind to IP address option on the FortiGuard service interface is set to the virtual IP address from the NAT device.

Answer: AC

Explanation:
FortiManager must have the NAT device's IP address and correct ports configured to communicate properly with the FortiGate behind NAT.
The NAT device must have the correct virtual IP address and ports configured to allow push updates to reach the FortiGate device.

NEW QUESTION 8
Refer to the exhibit.



An administrator created two new meta fields in FortiManager. Which operation can you perform with these parameters?

A. You can add them to objects as custom attributes.
B. You can export them to be used in other ADOMs.
C. You can use them as variables in scripts.
D. You can invoke them using the $ character.

Answer: A

Explanation:
Meta fields in FortiManager can be added to objects as custom attributes, allowing administrators to categorize and add additional information to firewall objects for easier management and identification.

NEW QUESTION 9
Refer to the exhibit.

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

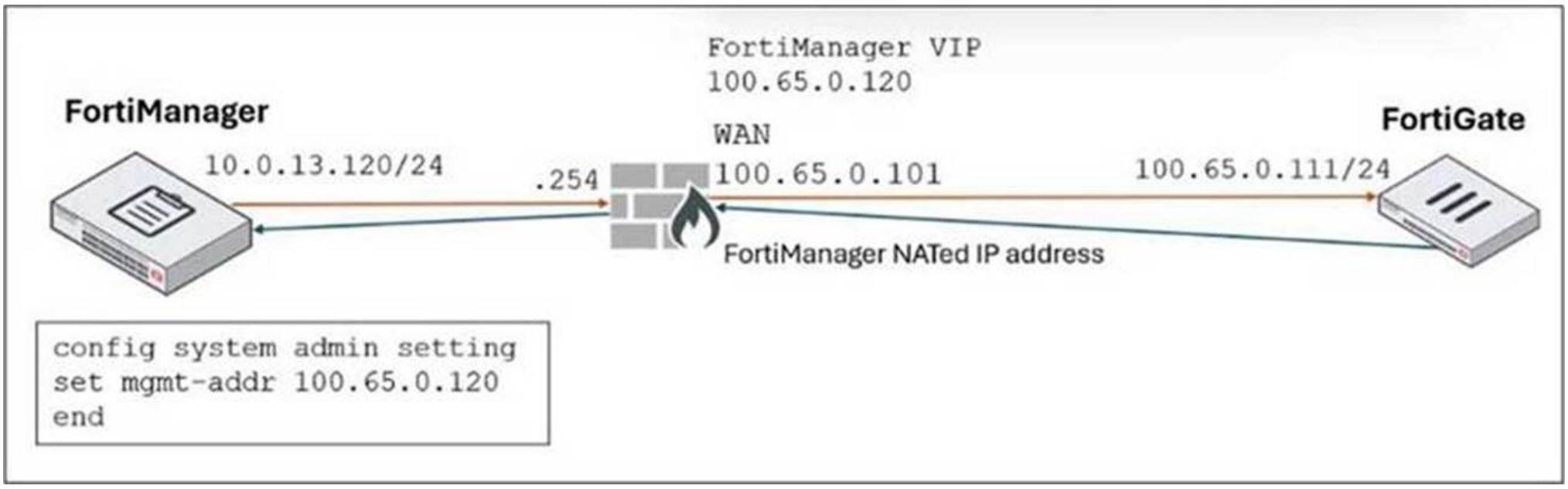
What are two results from the configuration shown in the exhibit? (Choose two.)

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 10
Refer to the exhibit.



FortiManager is operating behind a network address translation (NAT) device, and the administrator configured the FortiManager NATed IP address under the FortiManager system administration settings.
What is the expected result during discovery?

A. FortiManager sets both the 100.65.0.120 IP address and 10.0.13.120 IP address on FortiGate.
B. FortiManager sets both the 100.65.0.120 IP address and 100.65.0.101 IP address on FortiGate.
C. FortiManager sets the 100.65.0.101 IP address on FortiGate.
D. FortiManager sets the 100.65.0.120 IP address on FortiGate.

Answer: D

Explanation:
When FortiManager is behind a NAT device, setting the NATed IP address (100.65.0.120) in the system admin settings causes FortiManager to use that NATed IP address for communication and configuration with FortiGate during discovery and management operations.

NEW QUESTION 10
An administrator configures a new BGP peer in the FortiManager device-level database of FortiGate. They reinstall the policy package to the managed FortiGate device without any errors. However, when the administrator logs in to FortiGate, they do not see the BGP configuration changes.
What is the most likely reason why FortiManager did not push the BGP peer changes to FortiGate?

A. The administrator must run a sanity check on FortiManager to make sure the database is not corrupted.
B. Fortigate has a BGP template assigned on the FortiManager database.
C. The administrator must use the Install Wizard and select Install device settings only to push BGP settings
D. The FortiGate firmware version is different from the FortiManager ADOM version.

Answer: B

Explanation:
If a BGP template is assigned to the FortiGate device on FortiManager, device-level BGP configurations made directly in the device-level database are overridden by the template settings, so the changes do not get pushed to the device.

NEW QUESTION 14
.....

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