Fortinet

Exam Questions FCP_FMG_AD-7.6

FCP - FortiManager 7.6 Administrator

NEW QUESTION 1
Company policy dictates that any time a change is made to a policy package on FortiManager an ADOM revision is created before the change installed, and that revision is held for a minimum of 90 days.
Over the past three months, each installed change has resulted in several unused policies and duplicate objects. The FortiManager administrator plans to upgrade the FortiGate devices and then upgrade the FortiManager ADOM from version 7.4 to 7.6.
Which action can the administrator take to avoid slow ADOM upgrades?

A. Check and repair the global configuration database before upgrading.
B. Export firewall policies to Excel, delete them on the ADO
C. then reimport them after upgradingthe ADOM.
D. Find unused firmware templates, then delete them before upgrading.
E. Limit ADOM revisions before upgrading.

Answer: D

Explanation:
Limiting ADOM revisions reduces the number of stored historical configurations, which helps avoid performance degradation and slow ADOM upgrades caused by a large volume of revisions.

NEW QUESTION 2
An administrator must create a policy and install it on a FortiGate device within an ADOM in backup mode. How can the administrator perform this task?

A. Use the Install Wizard located on the device manager.
B. Enable workflow mode to allow policy creation and approval.
C. Make sure the ADOM and FortiGate firmware versions match and use the ADOM policy package.
D. Use a FortiManager script to apply the configuration changes.

Answer: D

Explanation:
In backup mode, FortiManager does not directly manage policy installation via the usual ADOM policy packages; instead, administrators use FortiManager scripts to push configuration changes, including policies, to FortiGate devices.

NEW QUESTION 3
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.

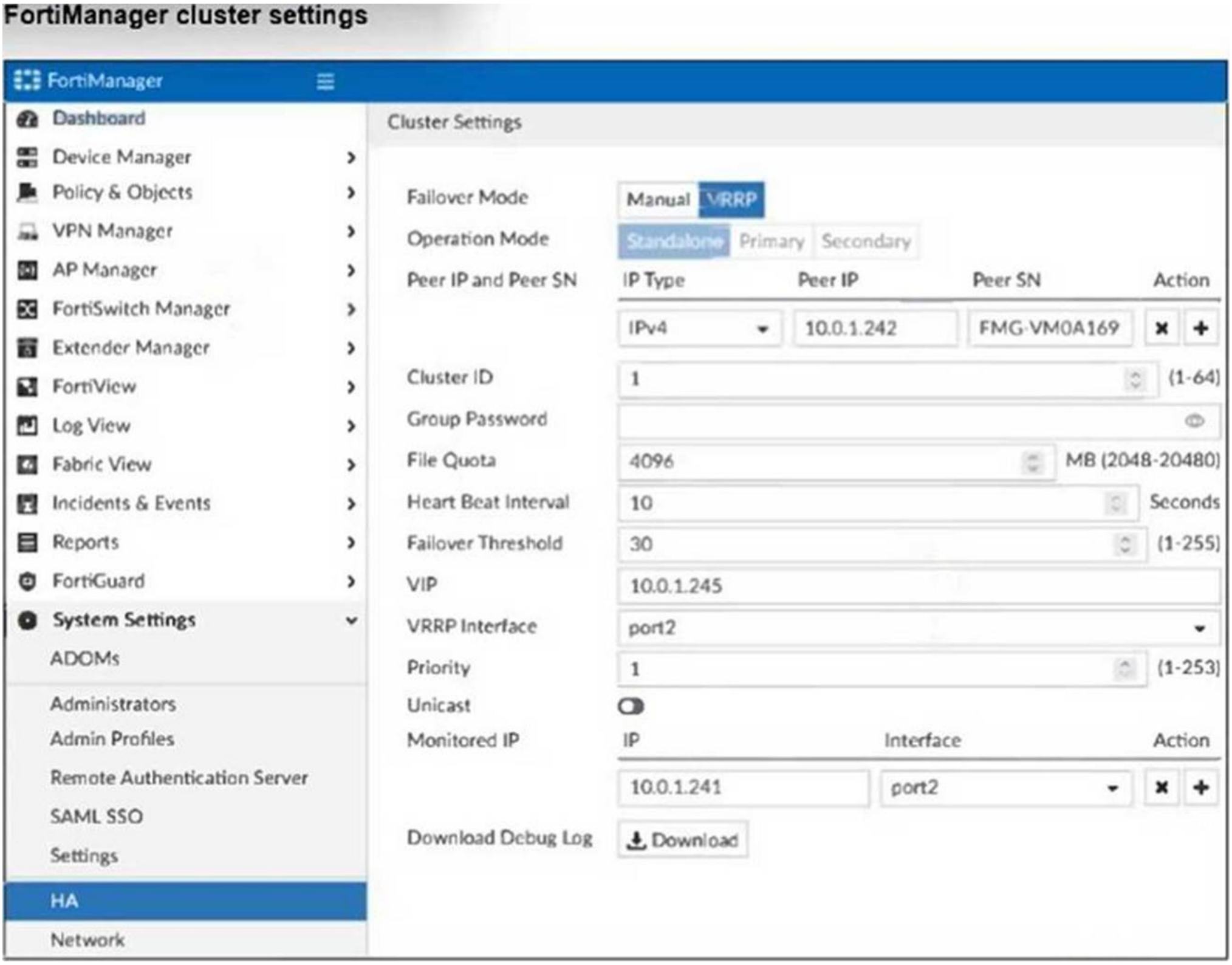
NEW QUESTION 4
You want to let multiple administrators work in the same ADOM without creating configuration conflicts.
What is the best and the most effective solution to apply?

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 5
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 6
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 7
Which two conditions trigger FortiManager to create a new revision history? (Choose two.)

A. When FortiManager installs device-level changes on a managed device
B. When changes to the device-level database are made on FortiManager
C. When FortiManager is auto-updated with configuration changes made directly on a managed device

D. When a provisioning template is assigned to a managed device on the device-level database

Answer: BC

Explanation:
FortiManager creates a new revision history entry whenever changes are made to the device-level database on FortiManager.
FortiManager also creates a new revision when it auto-updates its database with configuration changes detected directly on a managed device.

NEW QUESTION 8
An administrator is copying a system template profile between ADOMs by running the following command:
execute fmprofile export-profile ADOM 3547 /tmp/Backup_File
output dump to file: [/tmp/Backup_File]
Where does this command export the system template profile from?

A. FortiManager /tmp/Backup_File folder
B. FortiManager ADOM policy database
C. ADOM device database
D. FortiManager configuration backup file

Answer: B

Explanation:
The command exports the system template profile from the FortiManager ADOM policy database, which stores the configuration templates for devices within that ADOM.

NEW QUESTION 9
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.

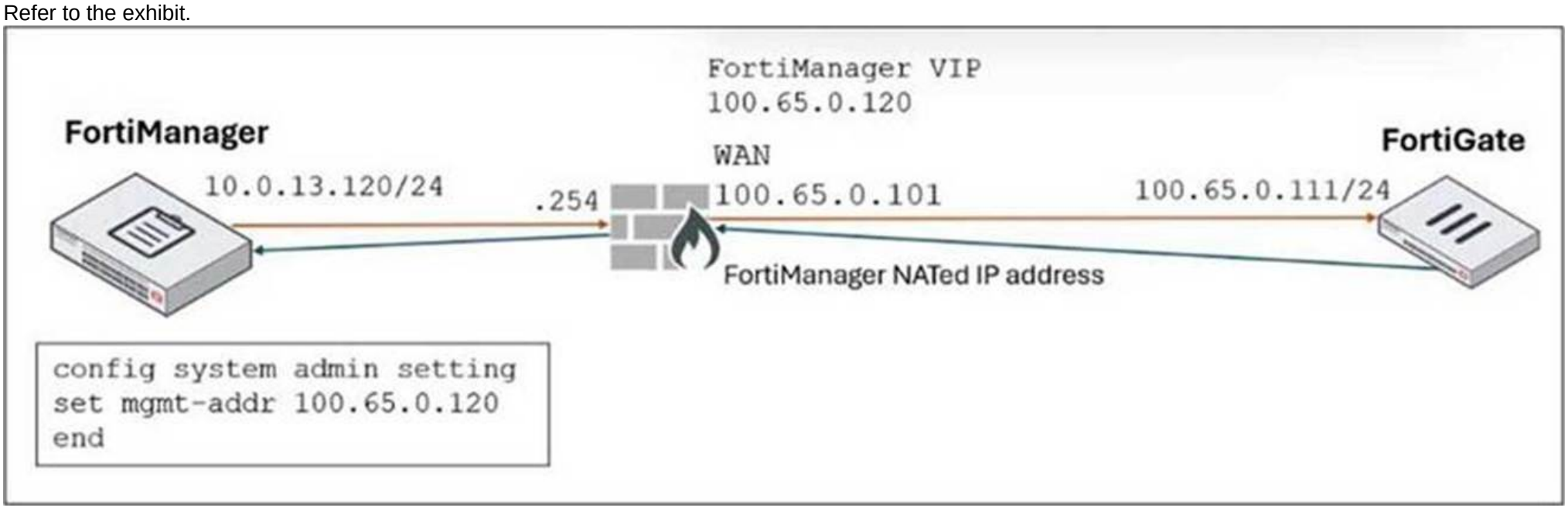
NEW QUESTION 10
A service provider administrator has assigned a global policy package to a managed customer ADOM named My_ADOM. The customer administrator has access only to My_ADOM.
How can the customer administrator edit the global header policy of the global policy package?

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 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 14
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 19
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 20

.....

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