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
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 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
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.

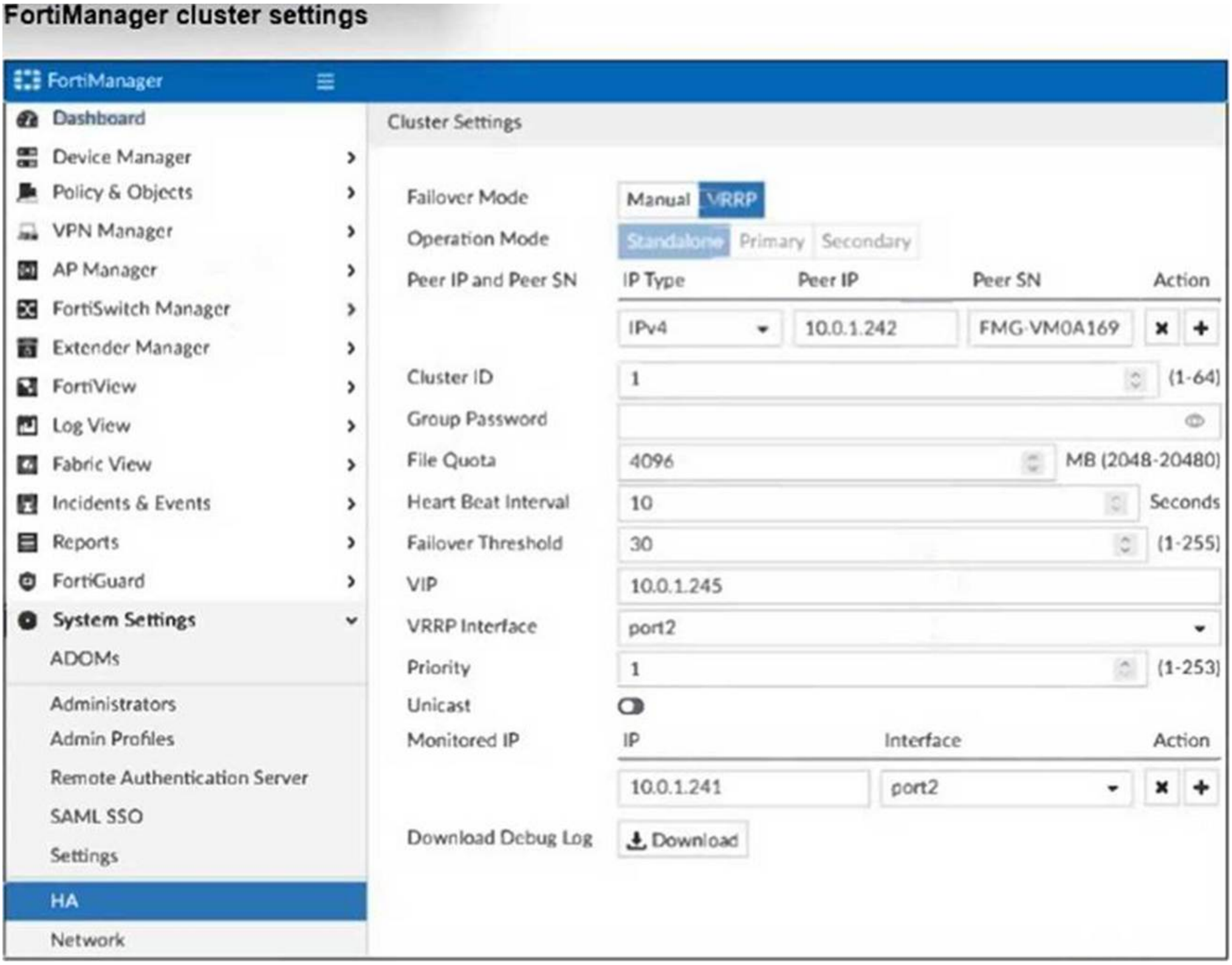
NEW QUESTION 5
You want to let multiple administrators work in the same ADOM without creating configuration conflicts.
What is the best and the most effective solution to apply?

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
While attempting to push a NetFlow configuration script through the FortiManager policy package: an administrator encounters an error stating that an object is unrecognized in line 4.

```
Starting log (Run on database)
config vdom
edit AGEUSR
[line 4] > config sys interface [parameter(s) invalid. detail: object unrecognized]
Failed to commit to DB, reason([line 4] > config sys interface [parameter(s) invalid. detail: object unrecognized]

Running script(NetFlow_Configuration) on DB failed
```

What must the administrator do to successfully apply the NetFlow configuration script and avoid the object unrecognized error?

A. Make sure the user running the script has full access to the VDOM—AGEUSR.
B. Run the script on the device database.
C. Use metadata variables if they use VDOMs in the script.
D. Create a normalized interface on the policy layer before running the script.

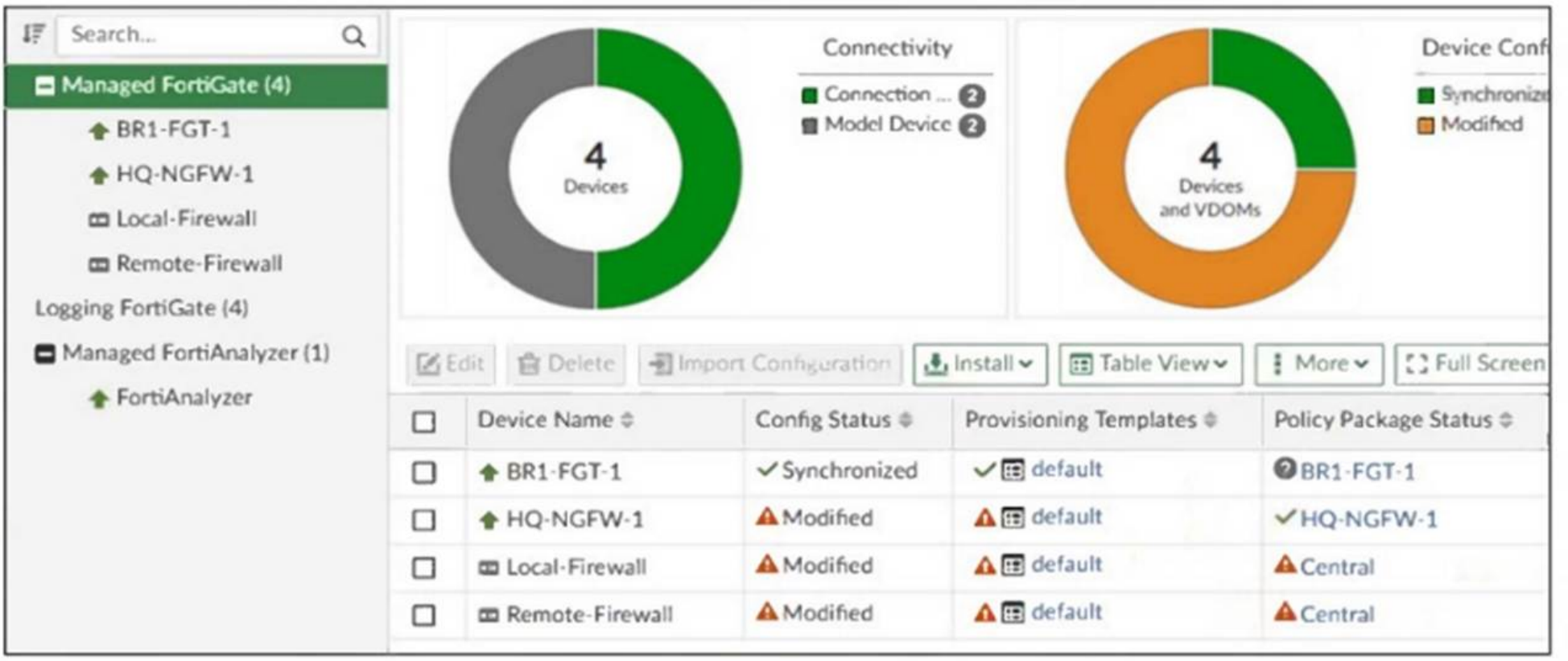
Answer: C

Explanation:
When using scripts that reference VDOM-specific objects, such as interfaces, in FortiManager, metadata variables must be used to correctly map those objects per

VDOM. This prevents "object unrecognized" errors during script execution.

NEW QUESTION 8
Refer to the exhibits.

FortiManager device database



Installation Targets Central policy package

An administrator has been asked to install the same policies from a central policy package onto the BR1-FGT- 1 firewall.
The administrator added BR1-FGT-1 as a target in the central policy package installation.
What should the administrator do when reinstalling the central policy package on the BR1-FGT-1 firewall?

A. Assign only one policy package to the firewall because FortiManager does not allow more than one policy package assigned per device at the same time.
B. Import the policy package to change the unknown status and synchronize the policy package.
C. Use the install wizard to install the central policy package on the BR1-FGT-1 firewall.
D. First resolve the modified status in the configuration and provisioning templates to allow a smooth installation.

Answer: C

Explanation:
Using the Install Wizard is the recommended method to reinstall the central policy package on the BR1-FGT- 1 firewall, ensuring all settings, installation targets, and dependencies are correctly processed during installation.

NEW QUESTION 9
What is the purpose of ADOM revisions?

A. ADOM revisions find unused, duplicate, and unnecessary firewall policies and objects.
B. ADOM revisions show specific changes in a policy package when it is installed.
C. ADOM revisions compare previous snapshots of the Policy Package and ADOM-level objects with the device-level database.
D. ADOM revisions save the current state of all policy packages and objects for an ADOM.

Answer: D

Explanation:
ADOM revisions save the current state of all policy packages and objects within an ADOM, allowing administrators to track changes over time and revert to previous configurations if needed.

NEW QUESTION 10
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 10
Which two conditions trigger FortiManager to create a new revision history? (Choose two.)

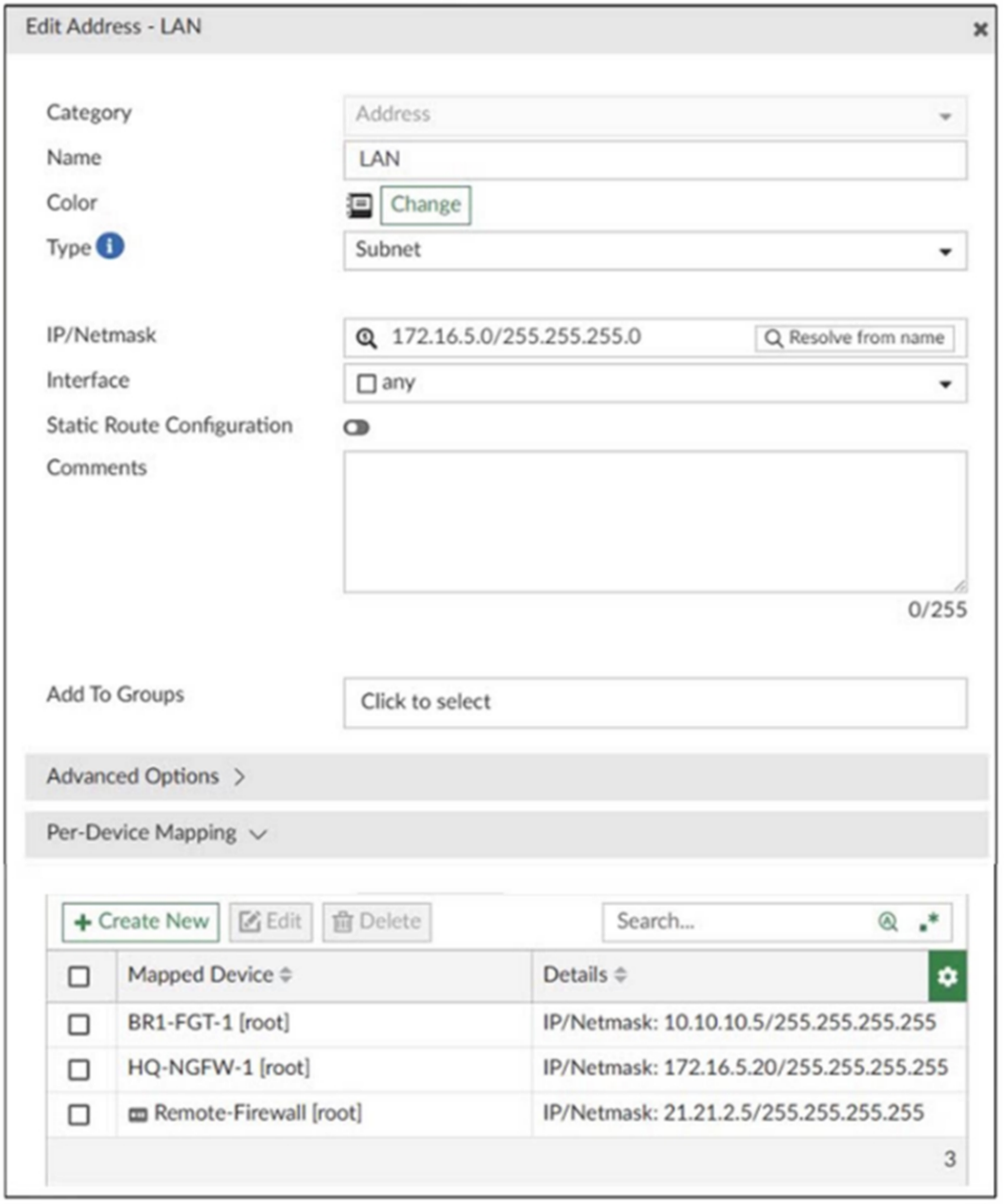
A. When FortiManager installs device-level changes on a managed device
B. When changes to the device-level database are made on FortiManager
C. When FortiManager is auto-updated with configuration changes made directly on a managed device
D. When a provisioning template is assigned to a managed device 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 14
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].

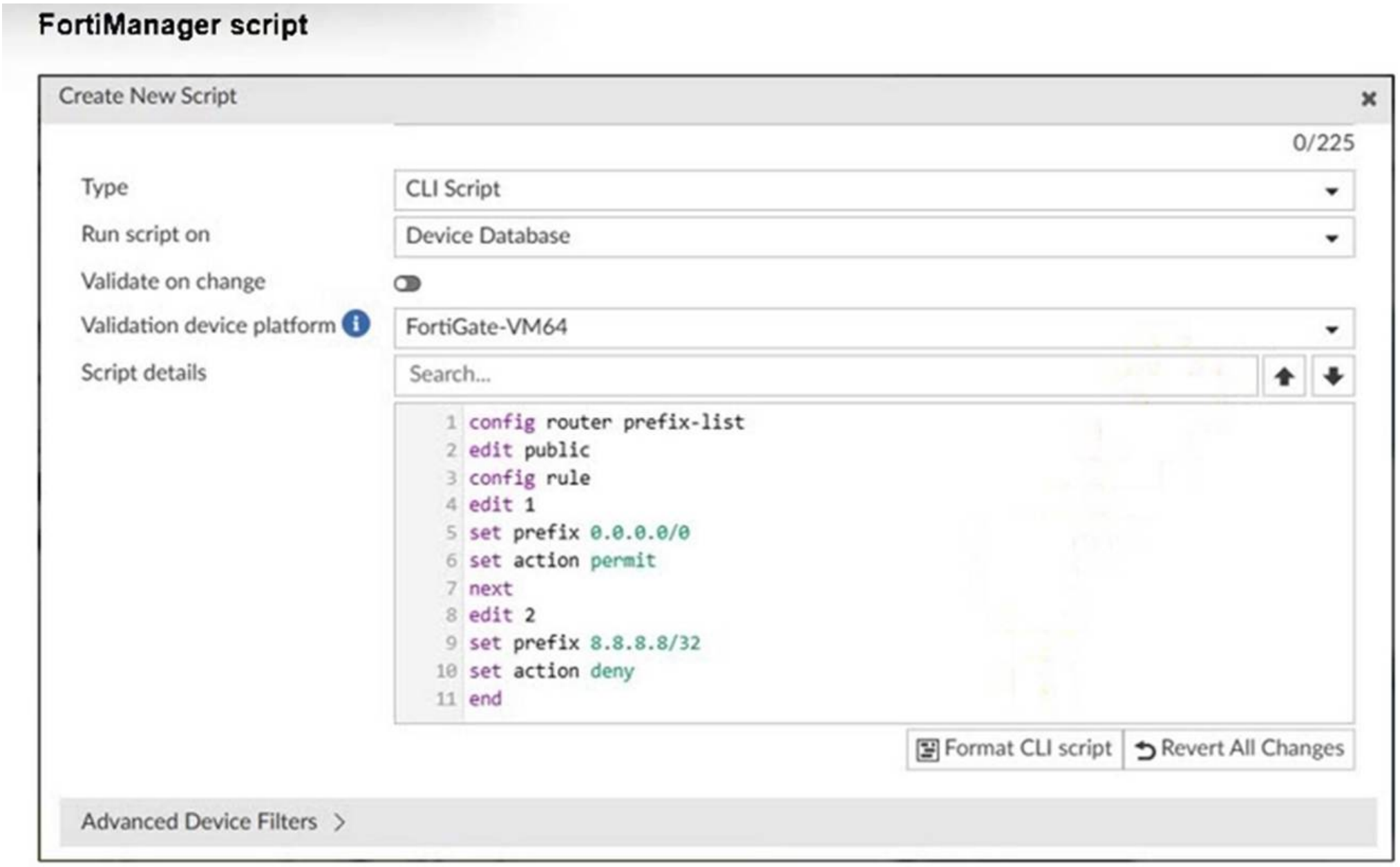
NEW QUESTION 19
A service provider administrator has assigned a global policy package to a managed customer ADOM named My_ADOM. The customer administrator has access only to My_ADOM.
How can the customer administrator edit the global header policy of the global policy package?

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 24
Refer to the exhibit.



Which two results occur if you run the script using theDevice Databaseoption? (Choose two.)

A. The device Config Status is tagged as Modified.
B. The script history shows the successful installation of the script on the remote FortiGate.
C. The successful execution of a script on the Device Database creates a new revision history.
D. The administrator must install these changes on a managed device using the Install Wizard.

Answer: AD

Explanation:
Running a script on the Device Database marks the configuration as modified but does not immediately apply changes to the device.
The administrator must use the Install Wizard to push and install these changes from the Device Database onto the managed device.

NEW QUESTION 29
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 33
.....

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