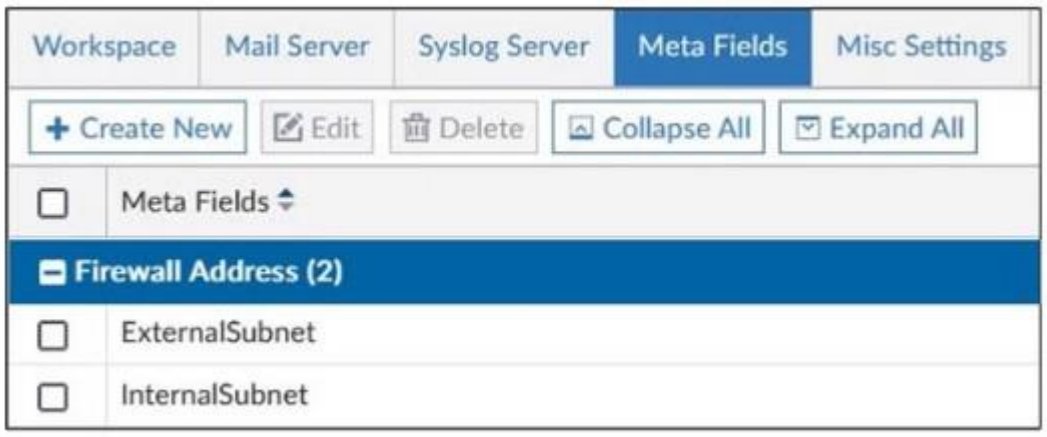
QUESTION 1
What is the purpose of ADOM revisions?

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.

QUESTION 2
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.

QUESTION 3
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:
What if FortiManager is behind a NAT device?
If FortiManager is behind a NAT device, sending its IP address for push updates causes push updates to fail because this is a non-routable IP address from the FDN. You must configure the following:
• On FortiManager, configure the NAT device IP address and port used for push updates.
• On the NAT device, configure the virtual IP and port that forwards to FortiManager.device.

QUESTION 4
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:
When you execute a script directly on a device, the changes are automatically applied on the device. You do not need to take any further action to apply the changes; however, you cannot preview the changes before they are applied.

QUESTION 5
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: C
Explanation:
An ADOM can work in device moces: Normal, which is the default mode, and Advanced.
In Normal mode, you cannot assign diferent FortiGate virtual domains (VDOMs) to different Fortitvlanager ADOMs.
In Advanced mode, you can assign different VDOMs from the sarne FortjGate device to diferent ADOMs. The system applies this setting globally to all ADOMs. This resutts in more complex management scenarios, and it is recommended for advanced users only.

QUESTION 6
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.

QUESTION 7
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            ADOM74   6.00741 (regular)  7.0 MR4 (2463)
                |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; conn: up
                |- vdom:[3]root flags:0 adom:ADOM74 pkg:[unknown]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            ADOM74   6.00741 (regular)  7.0 MR4 (2463)
                |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: autoupdated; conn: up
                |- vdom:[3]root flags:1 adom:ADOM74 pkg:[out-of-sync]ISFW
```

C.
```
FortiManager # 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            ADOM74   6.00741 (regular)  7.0 MR4 (2463)
                |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: installed; conn: up
                |- vdom:[3]root flags:0 adom:ADOM74 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            ADOM74   6.00741 (regular)  7.0 MR4 (2463)
                |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: installed; conn: up
                |- vdom:[3]root flags:0 adom:ADOM74 pkg:[imported]ISFW
```

Answer: C
Explanation:
Never Installed - The assigned policy package is not the result of an import for this device, and the package has not been installed since it has been assigned to this device.

QUESTION 8
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.

QUESTION 9
Refer to the exhibit. What can you conclude from the downloaded import report?

```
Start to import config from device(Remote-FortiGate) vdom(root) to
adom(root), package(Remote-FortiGate_root)

"firewall address",SKIPPED,"(name=all, oid=2309, DUPLICATE)"

"firewall address",FAIL,"(name=REMOTE_SUBNET, oid=2311,
reason=interface((firewall address:REMOTE_SUBNET) any<-port6) binding
fail)"

"firewall policy",FAIL,"(name=1, oid=3070, reason=interface(interface binding
contradiction. detail: (firewall address:REMOTE_SUBNET) any<-port6) binding
fail)"
```

A. FortiManager does not support per-device mapping for firewall addresses.
B. The administrator will see a new policy package named Remote-FortiGate_root in the FortiManager ADOM database.
C. FortiManager will change the configuration of REMOTE_SUBNET to match the interface mapping coming in from Remote-FortiGate.
D. As a result of this policy import process, FortiManager will create a new firewall address called REMOTE_SUBNET in the ADOM database.

Answer: B
Explanation:
The import report shows that a new policy package named Remote-FortiGate_root will be created in the FortiManager ADOM database, but some firewall addresses and policies failed to import due to interface binding conflicts.

QUESTION 10
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.

QUESTION 11
Refer to the exhibit. What are two results from the configuration shown in the exhibit? (Choose two.)

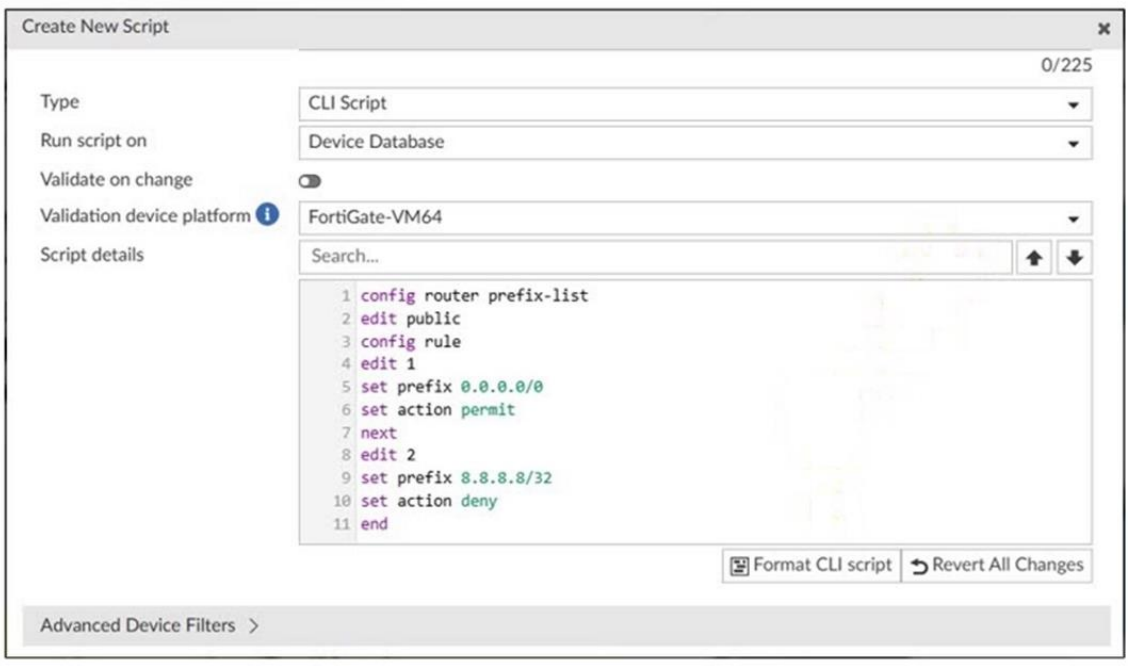
```
FortiManager # config system global
(global)# set workspace-mode normal
(global)# end
FortiManager #
```

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: AC
Explanation:
If an administrator locks an ADOM (checks it out) and then closes their session ungracefully (e.g., browser crash, network disconnect) without explicitly checking the configuration back in, the ADOM remains in a locked state. FortiManager relies on the configured session timeout to automatically release the lock. This prevents other administrators from editing the configuration until the lock expires.
The lock is applied on a per-ADOM basis. A single administrator can log into FortiManager and check out (lock) multiple different ADOMs simultaneously, provided those ADOMs are not currently locked by another administrator.

QUESTION 12
Refer to the exhibit. Which two results occur if you run the script using the Device Database option? (Choose two.)

FortiManager script



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.

QUESTION 13
Refer to the exhibits. An administrator runs the reload failure command diagnose test deploymanager reloadconf 262 on FortiManager.
Why does the administrator receive an error message?

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.
```

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.

QUESTION 14
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?

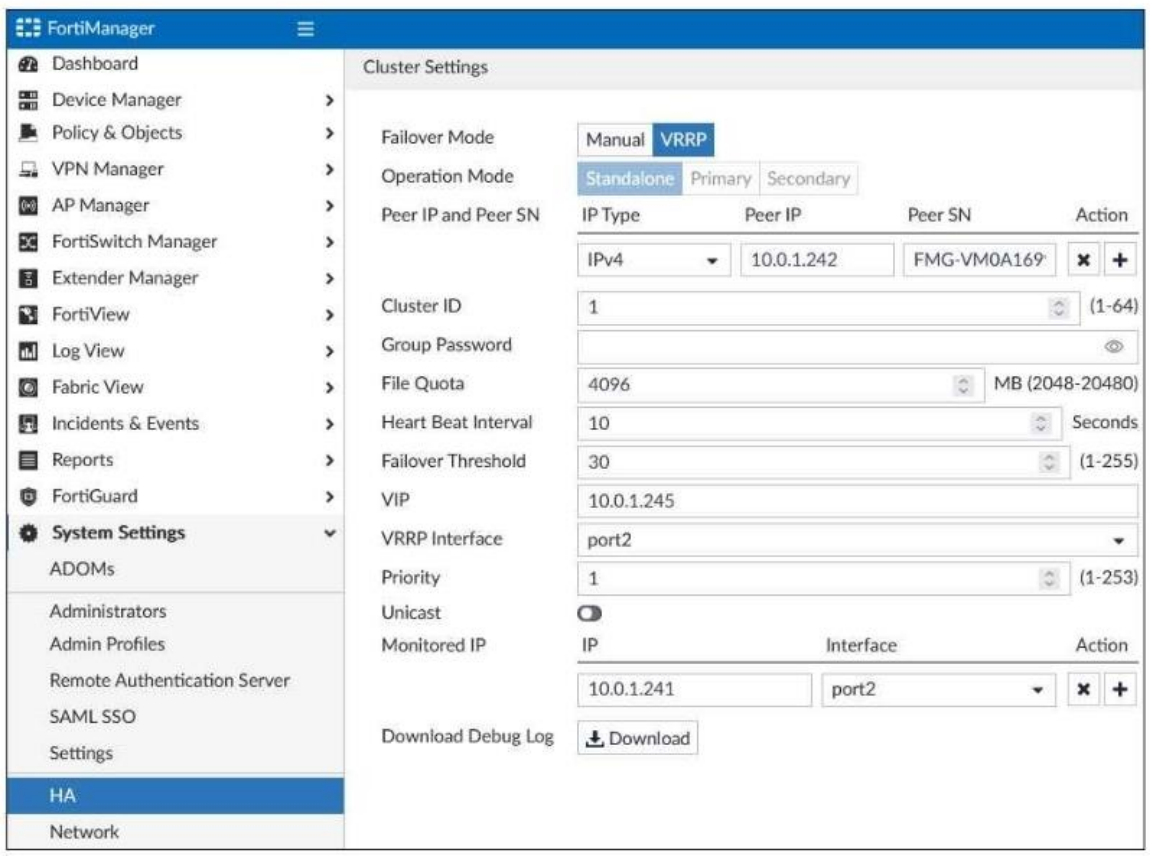
A. Configure RADIUS authentication to assign ADOM roles to each user.
B. Enable workflow mode, which is the only way to prevent concurrent configuration conflicts.

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 15
Refer to the exhibit. If the monitored interface for the primary FortiManager device fails, what must you do to maintain high availability (HA)?

FortiManager cluster settings

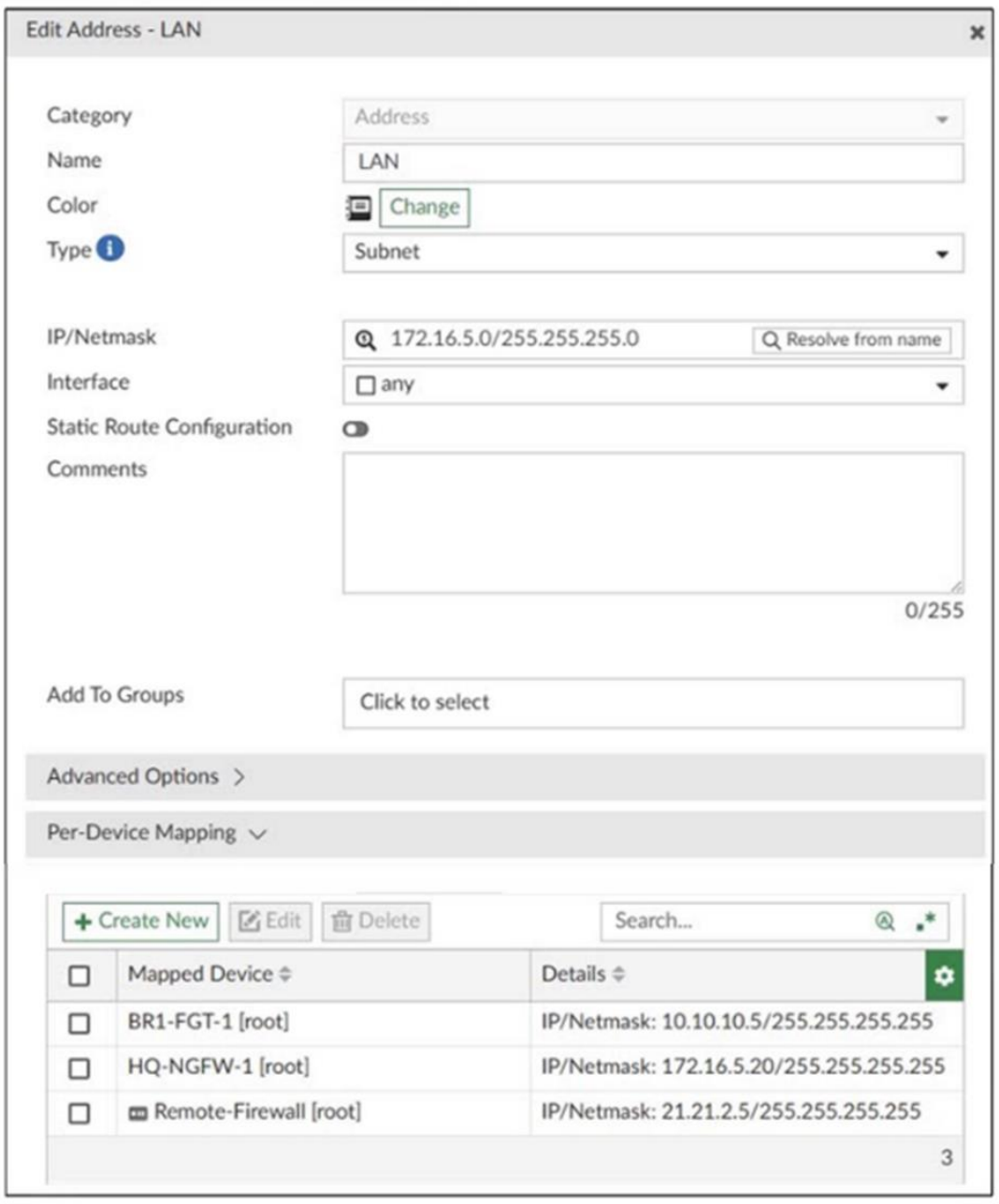


A. The FortiManager HA failover is transparent to administrators and does not require any additional action.
B. Manually promote one of the working secondary devices to the primary role: and reboot the original primary device to remove the peer IP address of the failed device.
C. Reconfigure the primary 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 16
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.

FortiManager address object



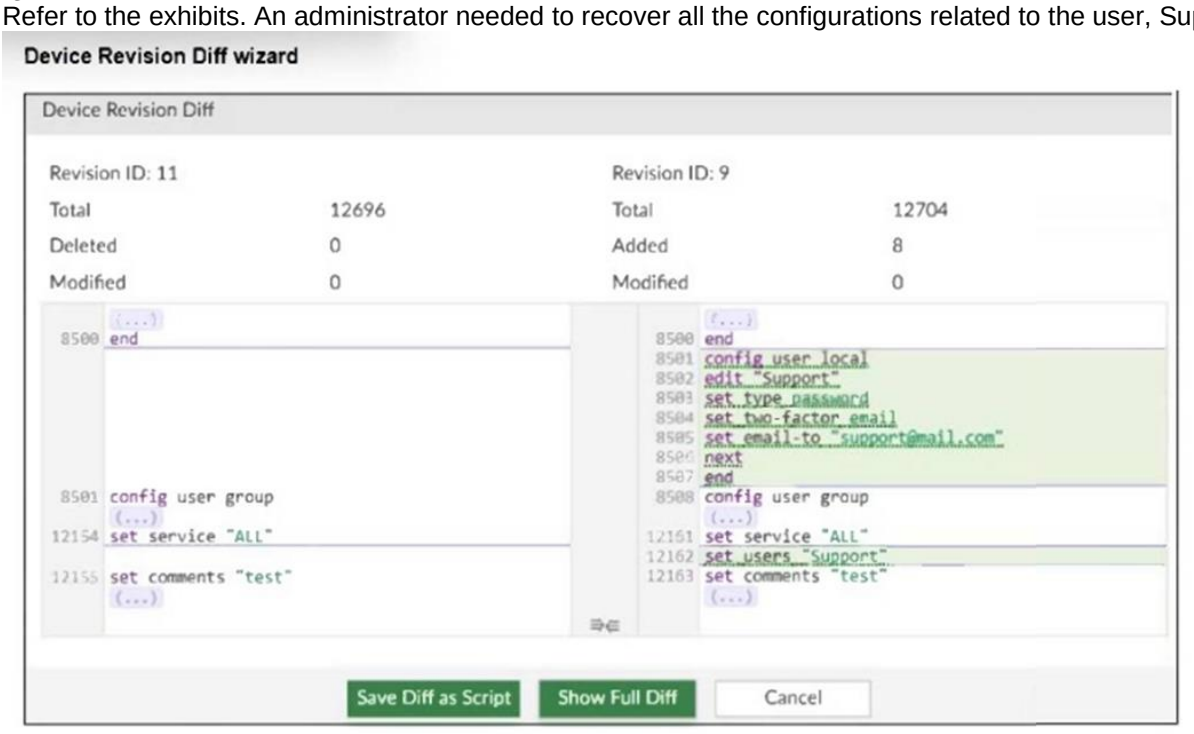
After the installation operation is performed, which IP/netmask will be installed on Remote-Firewall [VDOM1] for the LAN firewall address object?

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:
Remote-firewall(VDOM1) is different on the Remote-firewall(root) and it doesn't included within per-device mapping.

QUESTION 17
Refer to the exhibits. An administrator needed to recover all the configurations related to the user, Support. The configurations were saved in configuration revision ID 9.

Device Revision Diff wizard



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
```

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:
Fortimanager will show the policy package as unknown when you do a retrieve or a revert revisions. The dev db is in sync, so the config was reverted and device settings installed.

QUESTION 18
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.

QUESTION 19
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: AC
Explanation:
Conditions for Revision History and Troubleshooting
FortiManager creates a revision history when:
1- FortiGate is added to FortiManager
2- Device changes are installed
3- FortiGate configuration is retrieved from FortiManager
4- A local change on FortiGate causes an automatic update
Scripts run directly on remote devices also cause automatic updates and create a revision history
5- You revert to a previous revision and install the changes
How to check managed FortiGate configuration issues:
1- View and download FortiGate configuration revision
Compare differences between revisions
2- View who made the changes
3- View what has been installed on the managed device

QUESTION 20
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: B
Explanation:
In FortiManager, when a global policy package is assigned to an ADOM, any new policy package created within that ADOM will automatically inherit and include the assigned global policy package. This is designed to ensure consistency and centralized control over shared policies across multiple ADOMs.
……