Study HIGH Quality NSE5_FMG-7.0 Free Study Guides and Exams Tutorials [Q22-Q46

Study HIGH Quality NSE5_FMG-7.0 Free Study Guides and Exams Tutorials
Download Fortinet NSE5_FMG-7.0 Exam Dumps to Pass Exam Easily

Fortinet NSE5_FMG-7.0 Exam Syllabus Topics:

TopicDetailsTopic 1- Troubleshoot import and installation issues- Perform policy and object managementTopic 2- Troubleshoot policy and object management- Install configuration changes using scriptsTopic 3- Identify ADOM revisions and database versions- Implement and troubleshoot FortiManager HATopic 4- Troubleshoot device settings- Register devices in ADOMs - Configure FortiGuard servicesTopic 5- Configure various management panes and extensions- Configure administrative domains (ADOMs)

Q22. An administrator is replacing a device on FortiManager by running the following command:

execute device replace sn <devname> <serialnum>.

What device name and serial number must the administrator use?
* Device name and serial number of the original device.
* Device name and serial number of the replacement device.
* Device name of the replacement device and serial number of the original device.
* Device name of the original device and serial number of the replacement device.

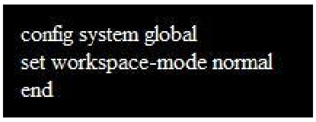
Q23. An administrator&#8217;s PC crashes before the administrator can submit a workflow session for approval. After the PC is restarted, the administrator notices that the ADOM was locked from the session before the crash.

How can the administrator unlock the ADOM?
* Restore the configuration from a previous backup.
* Log in as Super_User in order to unlock the ADOM.
* Log in using the same administrator account to unlock the ADOM.
* Delete the previous admin session manually through the FortiManager GUI or CLI.

Q24. An administrator has enabled Service Access on FortiManager.

What is the purpose of Service Access on the FortiManager interface?
* Allows FortiManager to download IPS packages
* Allows FortiManager to respond to request for FortiGuard services from FortiGate devices
* Allows FortiManager to run real-time debugs on the managed devices
* Allows FortiManager to automatically configure a default route

Q25. Refer to the following exhibit:



```
config system global
set workspace-mode normal
end
```

Which of the following statements are true based on this configuration? (Choose two.)
* The same administrator can lock more than one ADOM at the same time
* Ungraceful closed sessions will keep the ADOM in a locked state until the administrator session times out
* Unlocking an ADOM will submit configuration changes automatically to the approval administrator
* Unlocking an ADOM will install configuration automatically on managed devices

Q26. An administrator wants to delete an address object that is currently referenced in a firewall policy.

What can the administrator expect to happen?
* FortiManager will not allow the administrator to delete a referenced address object
* FortiManager will disable the status of the referenced firewall policy
* FortiManager will replace the deleted address object with the none address object in the referenced

firewall policy
* FortiManager will replace the deleted address object with all address object in the referenced firewall policy

Q27. Which two statements about the scheduled backup of FortiManager are true? (Choose two.)
* It does not back up firmware images saved on FortiManager.

* It can be configured using the CLI and GUI.
* It backs up all devices and the FortiGuard database.
* It supports FTP, SCP, and SFTP.

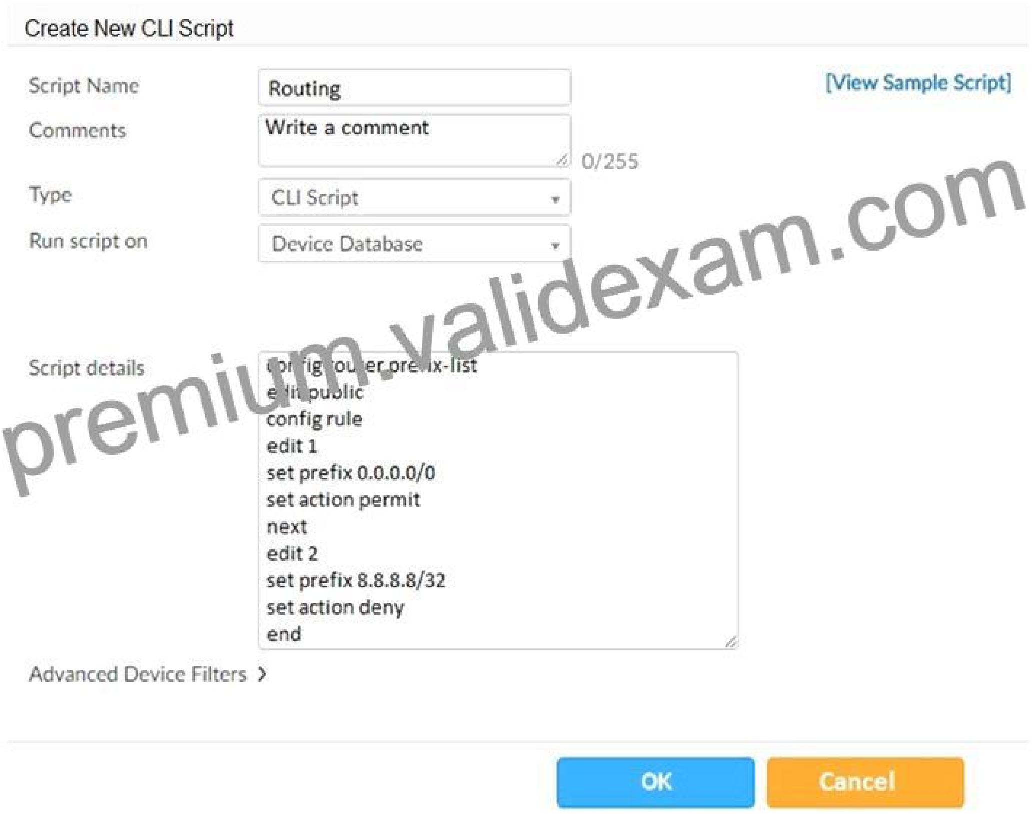
Q28. Which of the following statements are true regarding VPN Manager? (Choose three.)
* VPN Manager must be enabled on a per ADOM basis.
* VPN Manager automatically adds newly-registered devices to a VPN community.
* VPN Manager can install common IPsec VPN settings on multiple FortiGate devices at the same time.
* Common IPsec settings need to be configured only once in a VPN Community for all managed gateways.
* VPN Manager automatically creates all the necessary firewall policies for traffic to be tunneled by IPsec.

Q29. Which two items does an FGFM keepalive message include? (Choose two.)
* FortiGate uptime
* FortiGate license information
* FortiGate IPS version
* FortiGate configuration checksum

Q30. What is the purpose of the Policy Check feature on FortiManager?
* To find and provide recommendation to combine multiple separate policy packages into one common

policy package
* To find and merge duplicate policies in the policy package
* To find and provide recommendation for optimizing policies in a policy package
* To find and delete disabled firewall policies in the policy package

Q31. Refer to the exhibit.



Create New CLI Script

Script Name: Routing
Comments: Write a comment 0/255
Type: CLI Script
Run script on: Device Database
Script details:

```
config router prefix-list
edit public
config rule
edit 1
set prefix 0.0.0.0/0
set action permit
next
edit 2
set prefix 8.8.8.8/32
set action deny
end
```

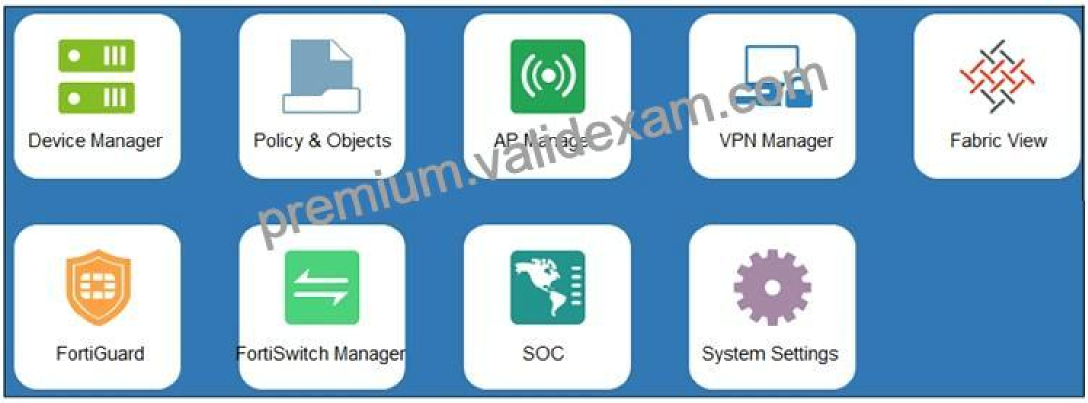
Which two statements are true if the script is executed using the Device Database option? (Choose two.)
* You must install these changes using the Install Wizard to a managed device
* The successful execution of a script on the Device Database will create a new revision history
* The script history will show successful installation of the script on the remote FortiGate
* The Device Settings Status will be tagged as Modified

Q32. An administrator run the reload failure command: diagnose test deploymanager reload config

<deviceid> on FortiManager. What does this command do?
* It downloads the latest configuration from the specified FortiGate and performs a reload operation on the device database.
* It installs the latest configuration on the specified FortiGate and update the revision history database.
* It compares and provides differences in configuration on FortiManager with the current running

configuration of the specified FortiGate.
* It installs the provisioning template configuration on the specified FortiGate.

Q33. Refer to the exhibit.



An administrator logs into the FortiManager GUI and sees the panes shown in the exhibit.

Which two reasons can explain why the FortiAnalyzer feature panes do not appear? (Choose two.)
* The administrator logged in using the unsecure protocol HTTP, so the view is restricted.
* The administrator profile does not have full access privileges like the Super_User profile.
* The administrator IP address is not a part of the trusted hosts configured on FortiManager interfaces.
* FortiAnalyzer features are not enabled on FortiManager.

Q34. An administrator would like to create an SD-WAN default static route for a newly created SD-WAN using the FortiManager GUI. Both port1 and port2 are part of the SD-WAN member interfaces.

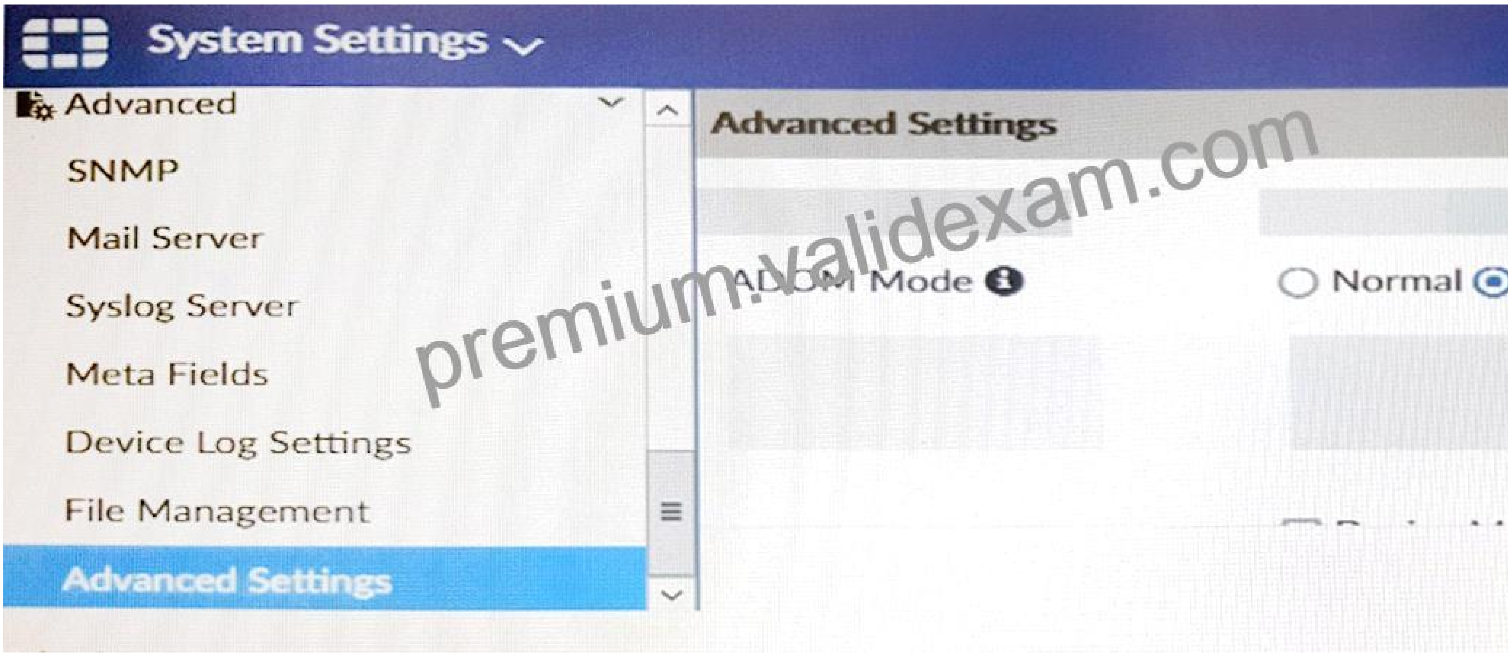
Which interface must the administrator select in the static route device drop-down list?
* port2
* virtual-wan-link
* port1
* auto-discovery

Q35. An administrator has assigned a global policy package to a new ADOM called ADOM1. What will happen if the administrator tries to create a new policy package in ADOM1?
* When creating a new policy package, the administrator can select the option to assign the global policy

package to the new policy package
* When a new policy package is created, the administrator needs to reapply the global policy package to

ADOM1.
* When a new policy package is created, the administrator must assign the global policy package from the global ADOM.
* When the new policy package is created, FortiManager automatically assigns the global policy package to the new policy package.

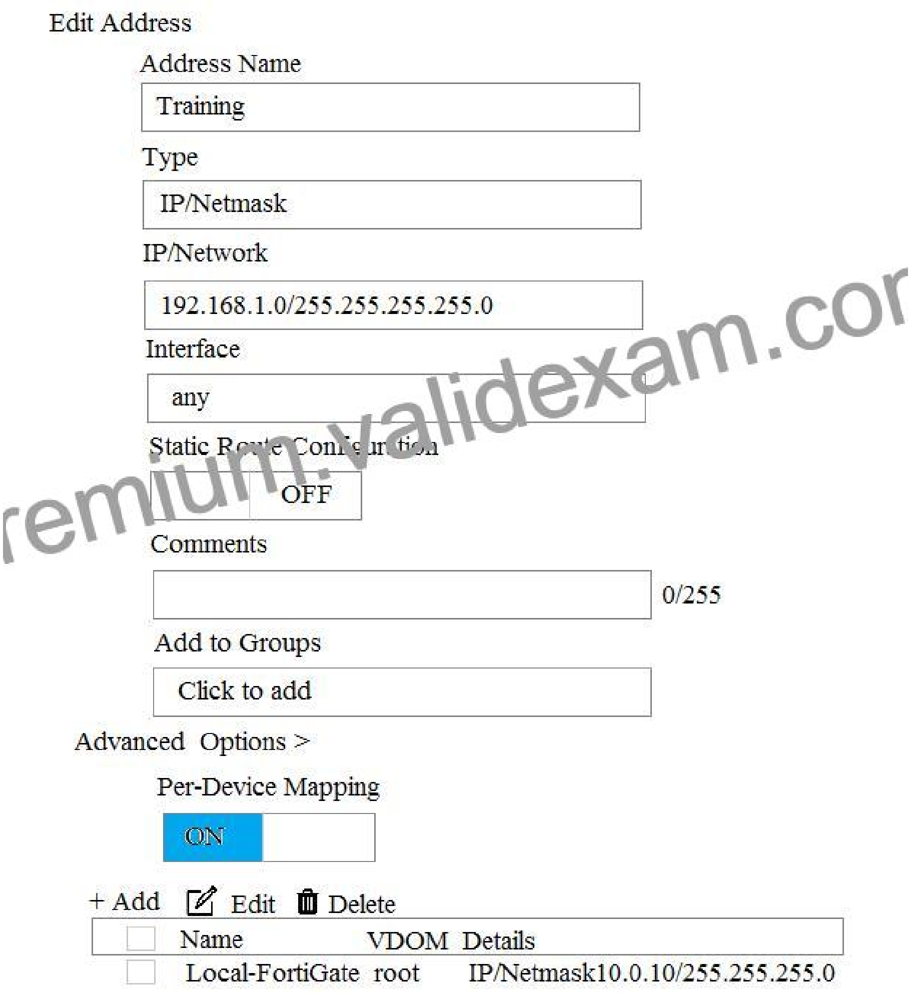
Q36. View the following exhibit.



ADOM Mode ○ Normal ●

Which of the following statements are true based on this configuration setting? (Choose two.)
* This setting will enable the ADOMs feature on FortiManager.
* This setting is applied globally to all ADOMs.
* This setting will allow assigning different VDOMs from the same FortiGate to different ADOMs.
* This setting will allow automatic updates to the policy package configuration for a managed device.

Q37. View the following exhibit.



Edit Address

Address Name: Training

Type: IP/Netmask

IP/Network: 192.168.1.0/255.255.255.255.0

Interface: any

Static Route Configuration: OFF

Comments: 0/255

Add to Groups: Click to add

Advanced Options >

Per-Device Mapping: ON

	Name	VDOM	Details
□	Local-FortiGate	root	IP/Netmask10.0.10/255.255.255.0

An administrator has created a firewall address object, Training, which is used in the Local-FortiGate policy package. When the install operation is performed, which IP Netmask will be installed on the Local-FortiGate, for the Training firewall address object?
* 10.0.1.0/24
* It will create firewall address group on Local-FortiGate with 192.168.0.1/24 and 10.0.1.0/24 object values
* 192.168.0.1/24
* Local-FortiGate will automatically choose an IP Network based on its network interface settings.

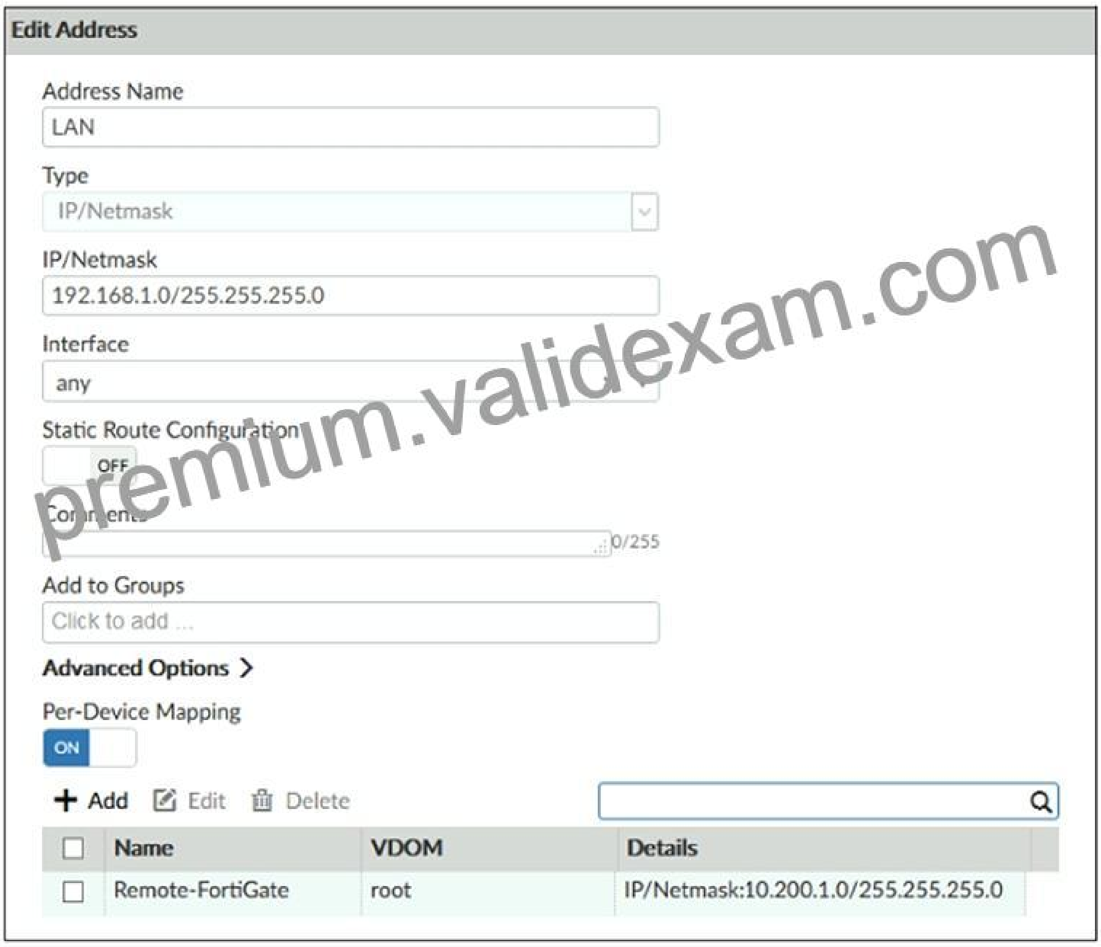
Q38. Which two statements about Security Fabric integration with FortiManager are true? (Choose two.)
* The Security Fabric license, group name and password are required for the FortiManager Security Fabric

integration
* The Fabric View module enables you to generate the Security Fabric ratings for Security Fabric devices
* The Security Fabric settings are part of the device level settings
* The Fabric View module enables you to view the Security Fabric ratings for Security Fabric devices

Q39. Which two conditions trigger FortiManager to create a new revision history? (Choose two.)
* When configuration revision is reverted to previous revision in the revision history
* When FortiManager installs device-level changes to a managed device
* When FortiManager is auto-updated with configuration changes made directly on a managed device
* When changes to device-level database is made on FortiManager

Q40. Which of the following statements are true regarding schedule backup of FortiManager? (Choose two.)
* Backs up all devices and the FortiGuard database.
* Does not back up firmware images saved on FortiManager
* Supports FTP, SCP, and SFTP
* Can be configured from the CLI and GUI

Q41. Refer to the exhibit.



Edit Address

Address Name: LAN

Type: IP/Netmask

IP/Netmask: 192.168.1.0/255.255.255.0

Interface: any

Static Route Configuration: OFF

Comments: 0/255

Add to Groups: Click to add ...

Advanced Options >

Per-Device Mapping: ON

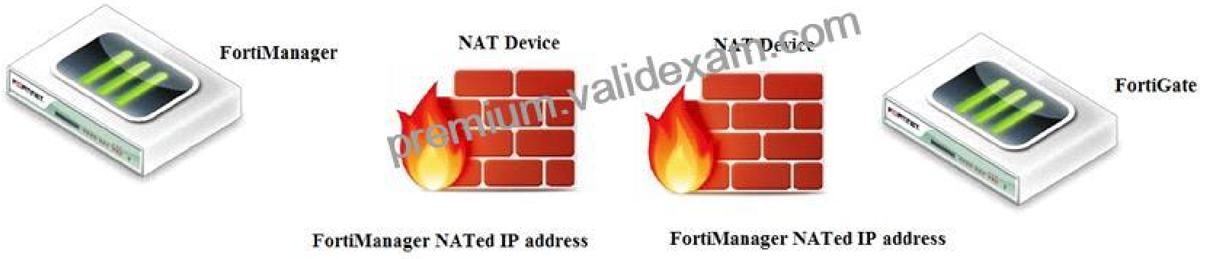
☐	Name	VDOM	Details
☐	Remote-FortiGate	root	IP/Netmask:10.200.1.0/255.255.255.0

An administrator has created a firewall address object, Training which is used in the Local-FortiGate policy package.

When the installation operation is performed, which IP/Netmask will be installed on the Local-FortiGate, for the Training firewall address object?
* 192.168.0.1/24
* 10.200.1.0/24
* It will create a firewall address group on Local-FortiGate with 192.168.0.1/24 and 10.0.1.0/24 object values.
* Local-FortiGate will automatically choose an IP/Netmask based on its network interface settings.
FortiManager_6.4_Study_Guide-Online &#8211; page 209

In the example, the dynamic address object LocalLan refers to the internal network address of the managed firewalls. The object has a default value of 192.168.1.0/24. The mapping rules are defined per device. For Remote-FortiGate, the address object LocalLan referes to 10.10.11.0/24. The devices in the ADOM that do not have dynamic mapping for LocalLan have a default value of 192.168.1.0/2.

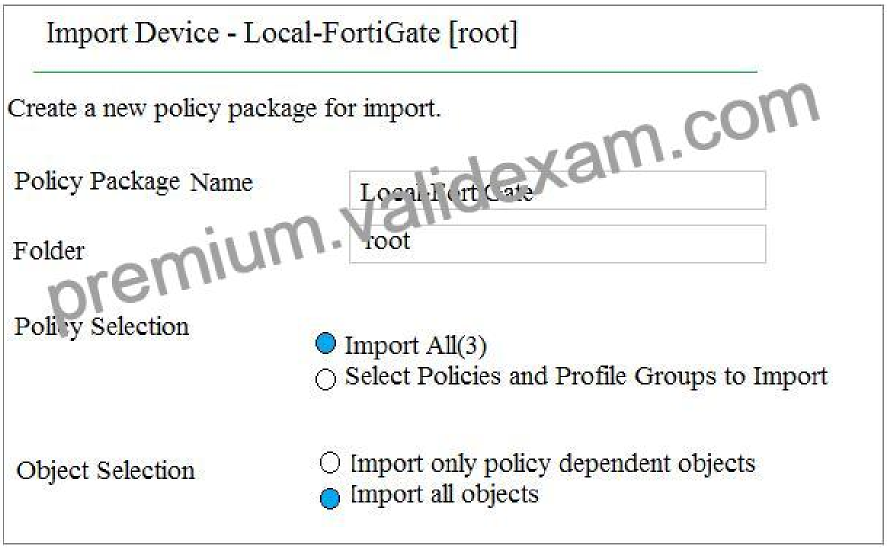
Q42. View the following exhibit.



If both FortiManager and FortiGate are behind the NAT devices, what are the two expected results? (Choose two.)
* FortiGate is discovered by FortiManager through the FortiGate NATed IP address.
* FortiGate can announce itself to FortiManager only if the FortiManager IP address is configured on

FortiGate under central management.
* During discovery, the FortiManager NATed IP address is not set by default on FortiGate.
* If the FCFM tunnel is torn down, FortiManager will try to re-establish the FGFM tunnel.
Fortimanager can discover FortiGate through a NATed FortiGate IP address. If a FortiManager NATed IP address is configured on FortiGate, then FortiGate can announce itself to FortiManager. FortiManager will not attempt to re-establish the FGFM tunnel to the FortiGate NATed IP address, if the FGFM tunnel is interrupted. Just like it was in the NATed FortiManager scenario, the FortiManager NATed IP address in this scenario is not configured under FortiGate central management configuration.

Q43. View the following exhibit.



Import Device - Local-FortiGate [root]

Create a new policy package for import.

Policy Package Name: Local-FortiGate
Folder: root

Policy Selection
● Import All(3)
○ Select Policies and Profile Groups to Import

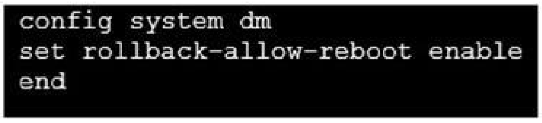
Object Selection
○ Import only policy dependent objects
● Import all objects

An administrator is importing a new device to FortiManager and has selected the shown options. What will happen if the

administrator makes the changes and installs the modified policy package on this managed FortiGate?
* The unused objects that are not tied to the firewall policies will be installed on FortiGate
* The unused objects that are not tied to the firewall policies will remain as read-only locally on FortiGate
* The unused objects that are not tied to the firewall policies locally on FortiGate will be deleted
* The unused objects that are not tied to the firewall policies in policy package will be deleted from the FortiManager database

Q44. Which two statements regarding device management on FortiManager are true? (Choose two.)
* FortiGate devices in HA cluster devices are counted as a single device.
* FortiGate in transparent mode configurations are not counted toward the device count on FortiManager.
* FortiGate devices in an HA cluster that has five VDOMs are counted as five separate devices.
* The maximum number of managed devices for each ADOM is 500.

Q45. Refer to the exhibit.



```
config system dm
set rollback-allow-reboot enable
end
```

An administrator has configured the command shown in the exhibit on FortiManager. A configuration change has been installed from FortiManager to the managed FortiGate that causes the FGFM tunnel to go down for more than 15 minutes.

What is the purpose of this command?
* It allows FortiGate to unset central management settings.
* It allows FortiGate to reboot and recover the previous configuration from its configuration file.
* It allows the FortiManager to revert and install a previous configuration revision on the managed FortiGate.
* It allows FortiGate to reboot and restore a previously working firmware image.

Q46. An administrator with the Super_User profile is unable to log in to FortiManager because of an authentication failure message.

Which troubleshooting step should you take to resolve the issue?
* Make sure FortiManager Access is enabled in the administrator profile
* Make sure Offline Mode is disabled
* Make sure the administrator IP address is part of the trusted hosts.
* Make sure ADOMs are enabled and the administrator has access to the Global ADOM
Even if a user entered the correct userid/password, the FMG denies access if a user is logging in from an untrusted source IP subnets.

Topic 1, Main Questions Pool B