- **Vendor: Fortinet**
- **Exam Code: NSE5_FMG-6.2**
- **Exam Name: Fortinet NSE 5 - FortiManager 6.2**
- **New Updated Questions from Braindump2go (Updated in Nov./2020)**

QUESTION 23
An administrator has assigned a global policy package to custom ADOM1. Then the administrator creates a new policy package, **Fortinet**, in the custom ADOM1.

Which statement about the global policy package assignment to the newly-created policy package **Fortinet** is true?

A. When a new policy package is created, it automatically assigns the global policies to the new package.
B. When a new policy package is created, you need to assign the global policy package from the global ADOM.
C. When a new policy package is created, you need to reapply the global policy package to the ADOM.
D. When a new policy package is created, you can select the option to assign the global policies to the new package.

Correct Answer: A

QUESTION 24
Refer to the exhibit.

```
Start to import config from device(Remote-FortiGate)vdom(root)to adom(MyADOM),
package(Remote-FortiGate)
"firewall address",SUCCESS,"(name=REMOTE_SUBNET,oid=580,new object)"
"firewall policy",SUCCESS,"(name=1,oid=990, new object)"
"firewall policy",FAIL,"(name=ID:2(#2),oid=991,reason=interface(interface binding
contradiction.detail:any<-port6)binding fail)"
```

Review the **Download Import Report**.

Why is it failing to import firewall policy ID 2?

A. Policy ID 2 does not have **ADOM Interface** mapping configured on FortiManager.
B. Policy ID 2 for this managed FortiGate already exists on FortiManager in policy package named **Remote-FortiGate**.
C. The address object used in policy ID 2 already exists in the ADOM database with **any** as the interface association, and conflicts with the address object interface association locally on FortiGate.
D. Policy ID 2 is configured from the interface **any** to **port6**. FortiManager rejects to import this policy because the **any** interface does not exist on FortiManager.

Correct Answer: C

QUESTION 25
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?

A. Make sure the administrator IP address is part of the trusted hosts
B. Make sure ADOMs are enabled and the administrator has access to the **Global ADOM**
C. Make sure **FortiManager Access** is enabled in the administrator profile
D. Make sure **Offline Mode** is disabled

Correct Answer: A

QUESTION 26
In the event that the primary FortiManager fails, which action must be performed to return the FortiManager HA to a working state?

A. The secondary device with highest priority will automatically be promoted to the primary role, and you must manually reconfigure all other secondary devices to point to the new primary device.
B. Manually promote one of the secondary devices to the primary role, and reconfigure all other secondary devices to point to the new primary device.
C. Reboot one of the secondary devices to promote it automatically to the primary role, and reconfigure all other secondary devices to point to the new primary device.
D. FortiManager HA state transition is transparent to administrators and does not require any reconfiguration.

Correct Answer: B

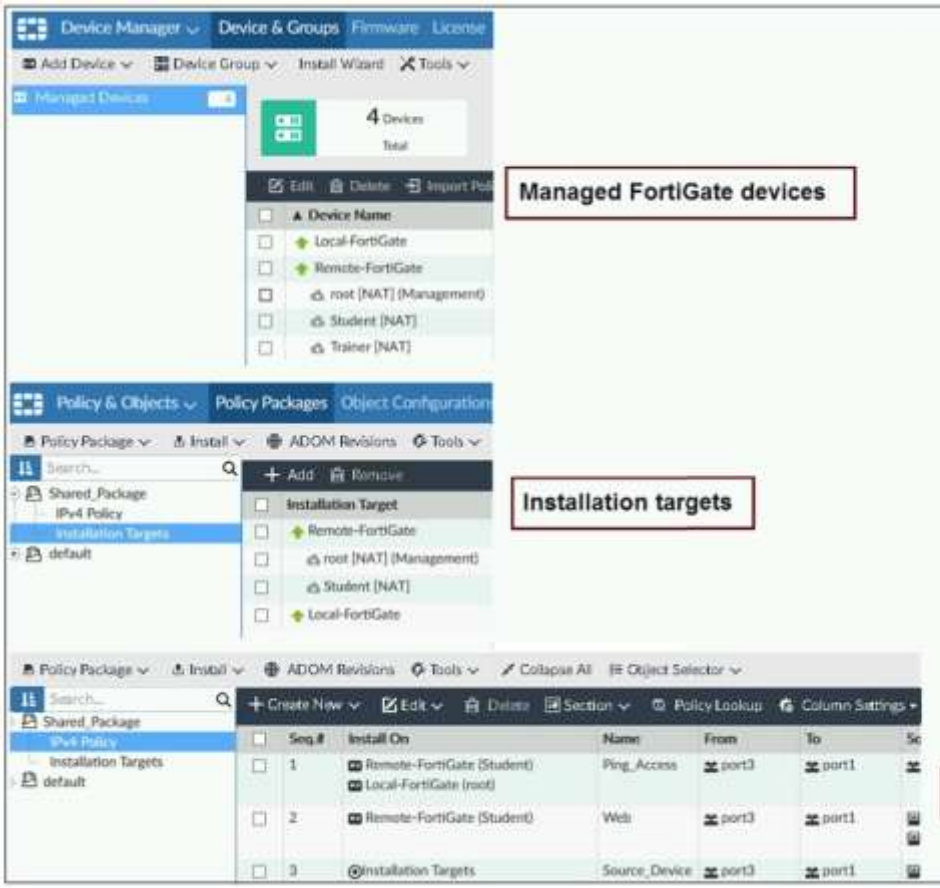
QUESTION 27
Refer to the exhibit.

If both FortiManager and FortiGate are behind the NAT devices, what are the two expected results? (Choose two.)

A. During discovery, the FortiManager NATed IP address is not set by default on FortiGate.
B. FortiGate can announce itself to FortiManager only if the FortiManager non-NATed IP address is configured on FortiGate under central management.
C. FortiGate is discovered by FortiManager through the FortiGate NATed IP address.
D. If the FGFM tunnel is torn down, FortiManager will try to re-establish the FGFM tunnel.

Correct Answer: AC

QUESTION 28
Refer to the exhibit.



Given the configurations shown in the exhibit, what can you conclude from the installation targets in the **Install On** column?

A. Policy seq.# 3 will not be installed on any managed device.
B. Policy seq.# 3 will be installed on the **Trainer[NAT]** VDOM only.
C. Policy seq.# 3 will be installed on all managed devices and VDOMs that are listed under **Installation Targets**.
D. The **Install On** column value represents successful installations on the managed devices.

Correct Answer: C

QUESTION 29
What will be the result of reverting to a previous revision version in the revision history?

A. It will install configuration changes to managed device automatically
B. It will tag the device settings status as **Auto-Update**
C. It will generate a new version **ID** and remove all other revision history versions
D. It will modify the device-level database

Correct Answer: D

QUESTION 30
What does a policy package status of **Conflict** indicate?

A. The policy package reports inconsistencies and conflicts during a **Policy Consistency Check**.
B. The policy package does not have a FortiGate as the installation target.
C. The policy package configuration has been changed on both FortiManager and the managed device independently.
D. The policy configuration has never been imported after a device was registered on FortiManager.

Correct Answer: A

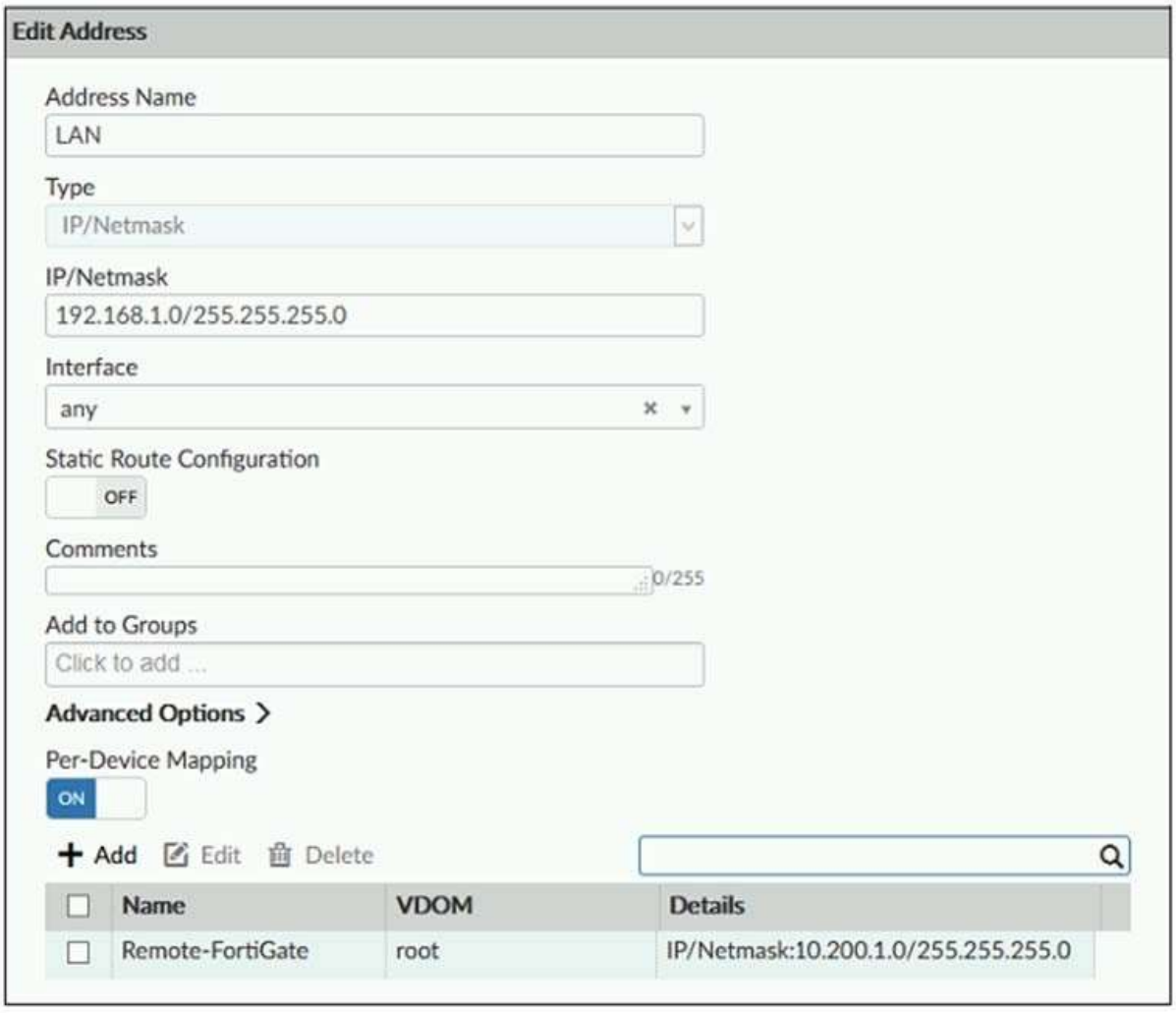
QUESTION 31
An administrator configures a new firewall policy on FortiManager and has not yet pushed the changes to the managed FortiGate.

In which database will the configuration be saved?

A. Device-level database
B. Revision history database
C. ADOM-level database
D. Configuration-level database

Correct Answer: C

QUESTION 32
Refer to the exhibit.



An administrator has created a firewall address object which is used in multiple policy packages for multiple FortiGate devices in an ADOM.

When the installation operation is performed, which IP/Netmask will be installed on managed devices for this firewall address object?

A. `192.168.0.1/24` on Remote-FortiGate`10.200.1.0/24` on Remote-FortiGate
B. If no dynamic mapping is defined for other FortiGate devices, the object will not be installed

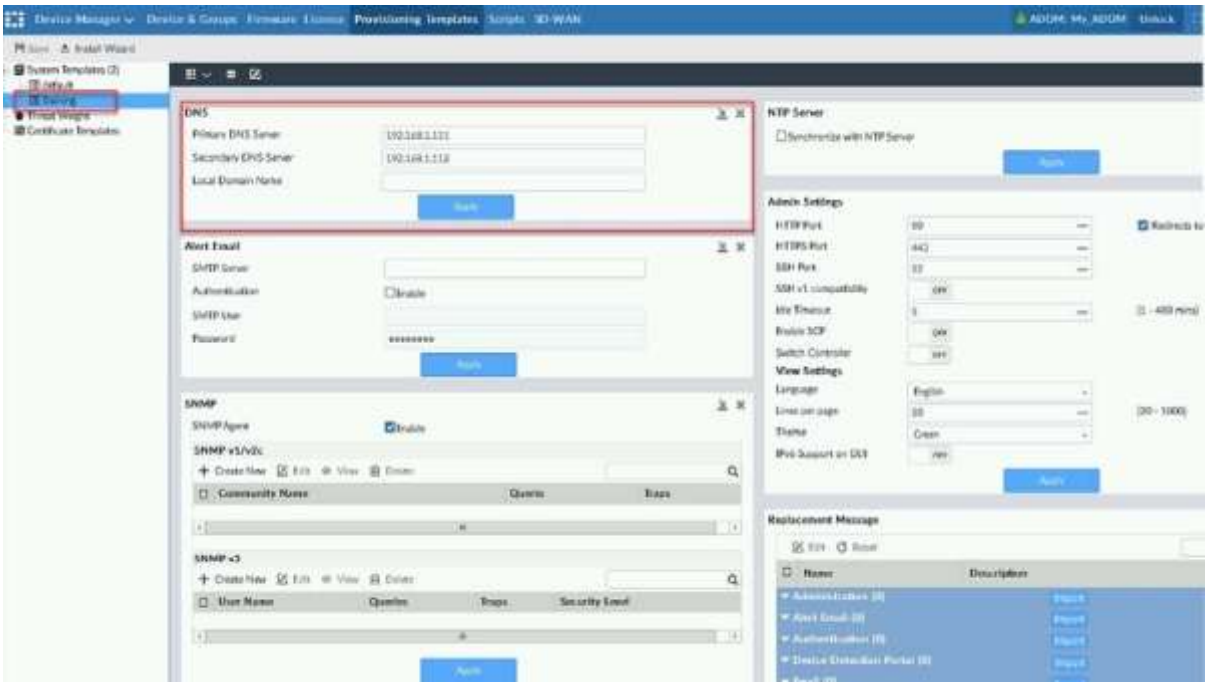
C. The FortiManager administrator can choose the value for the firewall address object in the **Install Wizard** for Remote-FortiGate

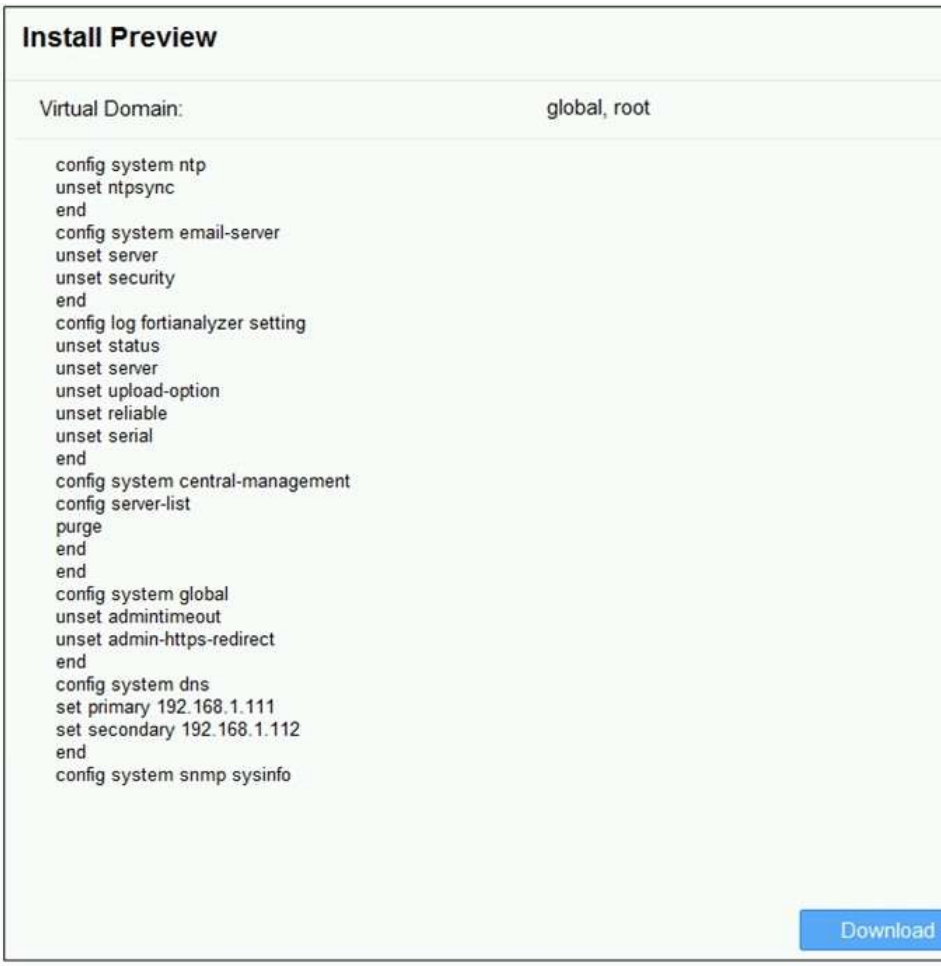
Correct Answer: B

QUESTION 33
Refer to the exhibits.

Exhibit one.

Exhibit two.





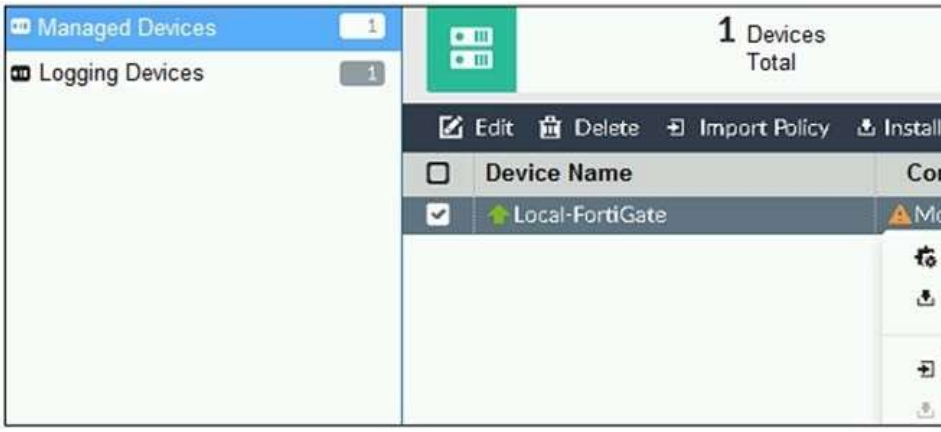
An administrator created a new system template named `Training` with two new DNS addresses on FortiManager. During the installation preview stage, the administrator notices that many unset commands need to be pushed.

What can be the main reason for these unset commands?

A. The DNS addresses in the default system settings are the same as the `Training` system template
B. The `Training` system template has other default settings
C. The ADOM is locked by another administrator
D. The `Training` system template does not have assigned devices

Correct Answer: B

QUESTION 34
Refer to the exhibit.



You are using the **Quick Install** option to install configuration changes on the managed FortiGate.

Which two statements correctly describe the result? (Choose two.)

A. It will not create a new revision in the revision history
B. It installs device-level changes to FortiGate without launching the **Install Wizard**
C. It cannot be canceled once initiated and changes will be installed on the managed device
D. It provides the option to preview configuration changes prior to installing them

Correct Answer: BC

QUESTION 35
An administrator has enabled **Service Access** on FortiManager.

What is the purpose of **Service Access** on the FortiManager interface?

A. Allows FortiManager to download IPS packages
B. Allows FortiManager to respond to request for FortiGuard services from FortiGate devices
C. Allows FortiManager to run real-time debugs on the managed devices
D. Allows FortiManager to automatically configure a default route

Correct Answer: B