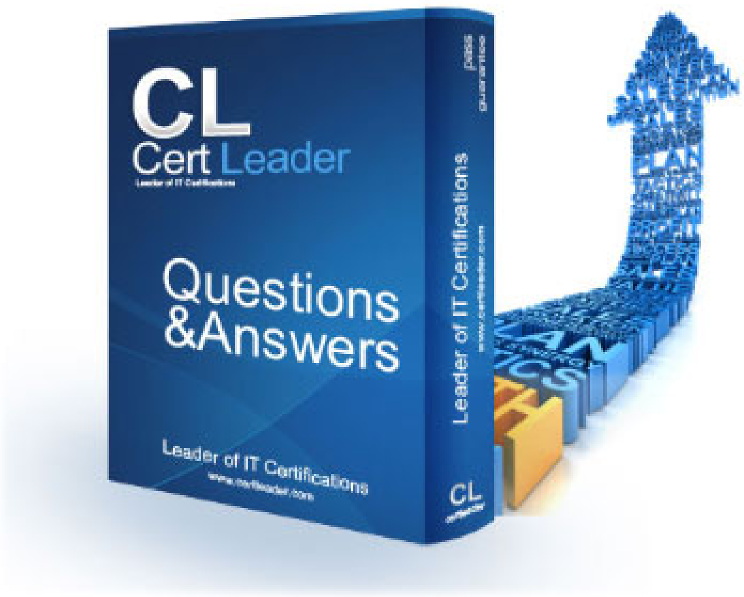
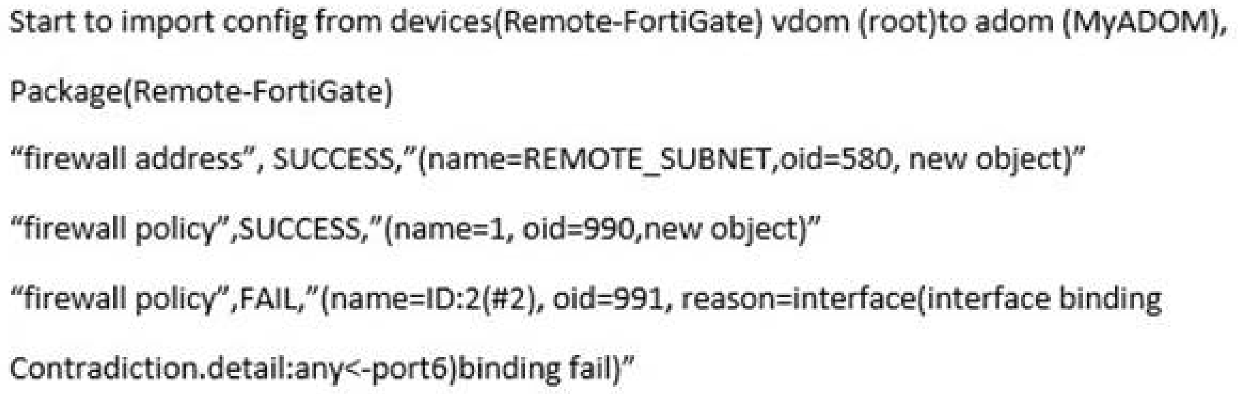
NSE5_FMG-7.0 Dumps

Fortinet NSE 5 - FortiManager 7.0

https://www.certleader.com/NSE5_FMG-7.0-dumps.html



NEW QUESTION 1
- (Topic 1)
View the following exhibit, which shows the Download Import Report:



```
Start to import config from devices(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)"
```

Why it is failing to import firewall policy ID 2?

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

Answer: A

Explanation:
FortiManager_6.4_Study_Guide-Online – page 331 & 332

NEW QUESTION 2
- (Topic 1)
An administrator would like to create an SD-WAN using central management in the Training ADOM.
To create an SD-WAN using central management, which two steps must be completed? (Choose two.)

A. Specify a gateway address when you create a default SD-WAN static route
B. Enable SD-WAN central management in the Training ADOM
C. Configure and install the SD-WAN firewall policy and SD-WAN static route before installing the SD-WANtemplate settings
D. Remove all the interface references such as routes or policies that will be a part of SD-WAN member interfaces

Answer: BD

Explanation:
Reference: https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/676493/removing-existing-configuration-references-to-interfaces

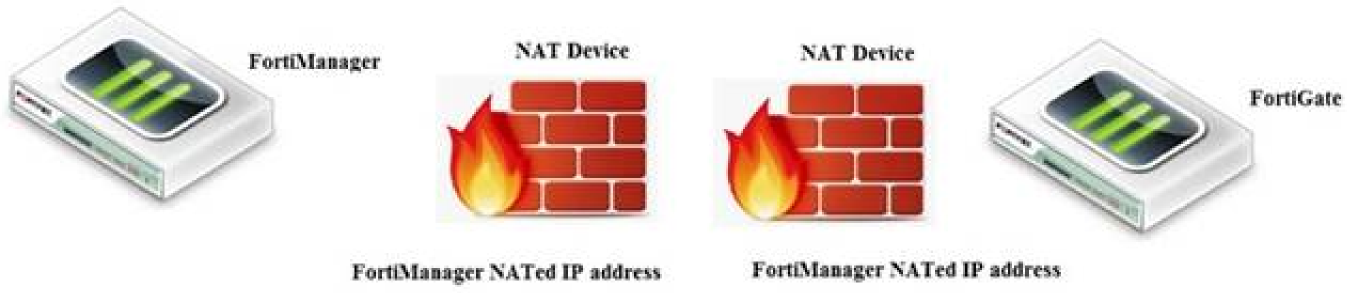
NEW QUESTION 3
- (Topic 1)
An administrator would like to review, approve, or reject all the firewall policy changes made by the junior
administrators.
How should the Workspace mode be configured on FortiManager?

A. Set to workflow and use the ADOM locking feature
B. Set to read/write and use the policy locking feature
C. Set to normal and use the policy locking feature
D. Set to disable and use the policy locking feature

Answer: A

Explanation:
Reference: https://help.fortinet.com/fmgr/50hlp/52/5-2-0/FMG_520_Online_Help/200_What's-New.03.03.html

NEW QUESTION 4
- (Topic 1)
View the following exhibit.



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

A. FortiGate is discovered by FortiManager through the FortiGate NATed IP address.
B. FortiGate can announce itself to FortiManager only if the FortiManager IP address is configured onFortiGate under central management.

C. During discovery, the FortiManager NATed IP address is not set by default on FortiGate.
D. If the FCFM tunnel is torn down, FortiManager will try to re-establish the FGFM tunnel.

Answer: AC

Explanation:
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.

NEW QUESTION 5
- (Topic 1)
What is the purpose of the Policy Check feature on FortiManager?

A. To find and provide recommendation to combine multiple separate policy packages into one commonpolicy package
B. To find and merge duplicate policies in the policy package
C. To find and provide recommendation for optimizing policies in a policy package
D. To find and delete disabled firewall policies in the policy package

Answer: C

Explanation:
Reference: https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FortiManager_Admin_Guide/1200_Policy%20and%20Objects/0800_Managing%20policy%20packages/2400_Perform%20a%20policy%20consistency%20check.htm

NEW QUESTION 6
- (Topic 1)
What will happen if FortiAnalyzer features are enabled on FortiManager?

A. FortiManager will reboot
B. FortiManager will send the logging configuration to the managed devices so the managed devices will start sending logs to FortiManager
C. FortiManager will enable ADOMs automatically to collect logs from non-FortiGate devices
D. FortiManager can be used only as a logging device.

Answer: A

Explanation:
Reference: https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FortiManager_Admin_Guide/1800_FAZ%20Features/0200_Enable%20FAZ%20Features.htm

NEW QUESTION 7
- (Topic 1)
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 FortiManager Access is enabled in the administrator profile
B. Make sure Offline Mode is disabled
C. Make sure the administrator IP address is part of the trusted hosts.
D. Make sure ADOMs are enabled and the administrator has access to the Global ADOM

Answer: C

Explanation:
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.
Reference: https://docs.fortinet.com/document/fortimanager/6.0.3/administration-guide/107347/trusted-hosts

NEW QUESTION 8
- (Topic 1)
Which configuration setting for FortiGate is part of a device-level database on FortiManager?

A. VIP and IP Pools
B. Firewall policies
C. Security profiles
D. Routing

Answer: D

Explanation:
The FortiManager stores the FortiGate configuration details in two distinct databases. The device-level database includes configuration details related to device-level settings, such as interfaces, DNS, routing, and more. The ADOM-level database includes configuration details related to firewall policies, objects, and security profiles.

NEW QUESTION 9
- (Topic 1)
In the event that the primary FortiManager fails, which of the following actions must be performed to return the FortiManager HA to a working state?

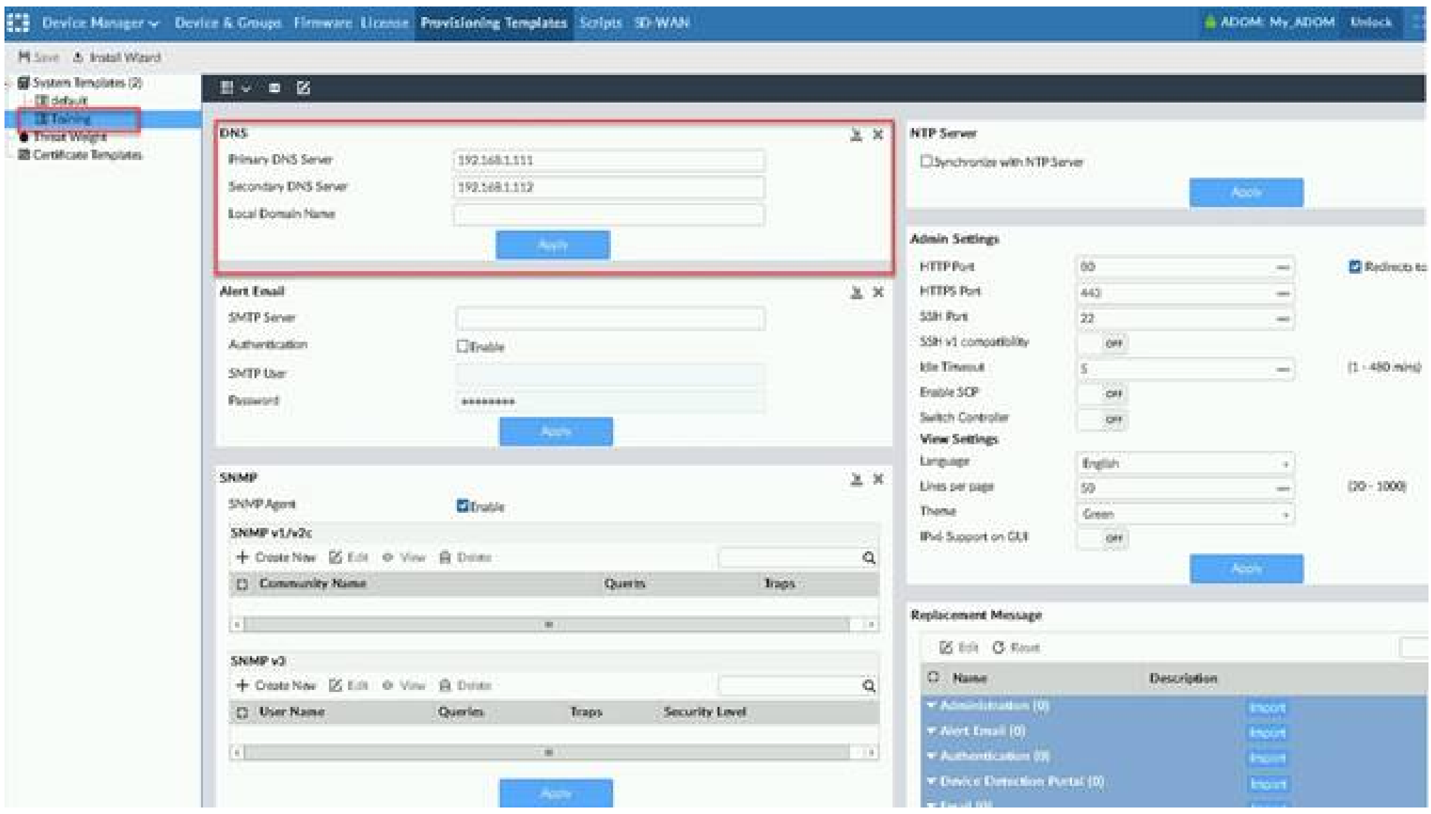
A. Secondary device with highest priority will automatically be promoted to the primary role, and manuallyreconfigure all other secondary devices to point to the

new primary device
B. 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.
C. Manually promote one of the secondary devices 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.

Answer: C

Explanation:
FortiManager_6.4_Study_Guide-Online – page 346
FortiManager HA doesn’t support IP takeover where an HA state transition is transparent to administrators. If a failure of the primary occurs, the administrator must take corrective action to resolve the problem that may include invoking the state transition. If the primary device fails, the administrator must do the following in order to return the FortiManager HA to a working state:
* 1. Manually reconfigure one of the secondary devices to become the primary device
* 2. Reconfigure all other secondary devices to point to the new primary device

NEW QUESTION 10
- (Topic 1)
Refer to the exhibits. Exhibit one.



DNS
Primary DNS Server: 192.168.1.111
Secondary DNS Server: 192.168.1.112
Local Domain Name:

Alert Email
SMTP Server:
Authentication: □Enable
SMTP User:
Password: ********

SNMP
SNMP Agent: ☑Enable
SNMP v1/v2c

□ Community Name	Queries	Traps

SNMP v3

□ User Name	Queries	Traps	Security Level

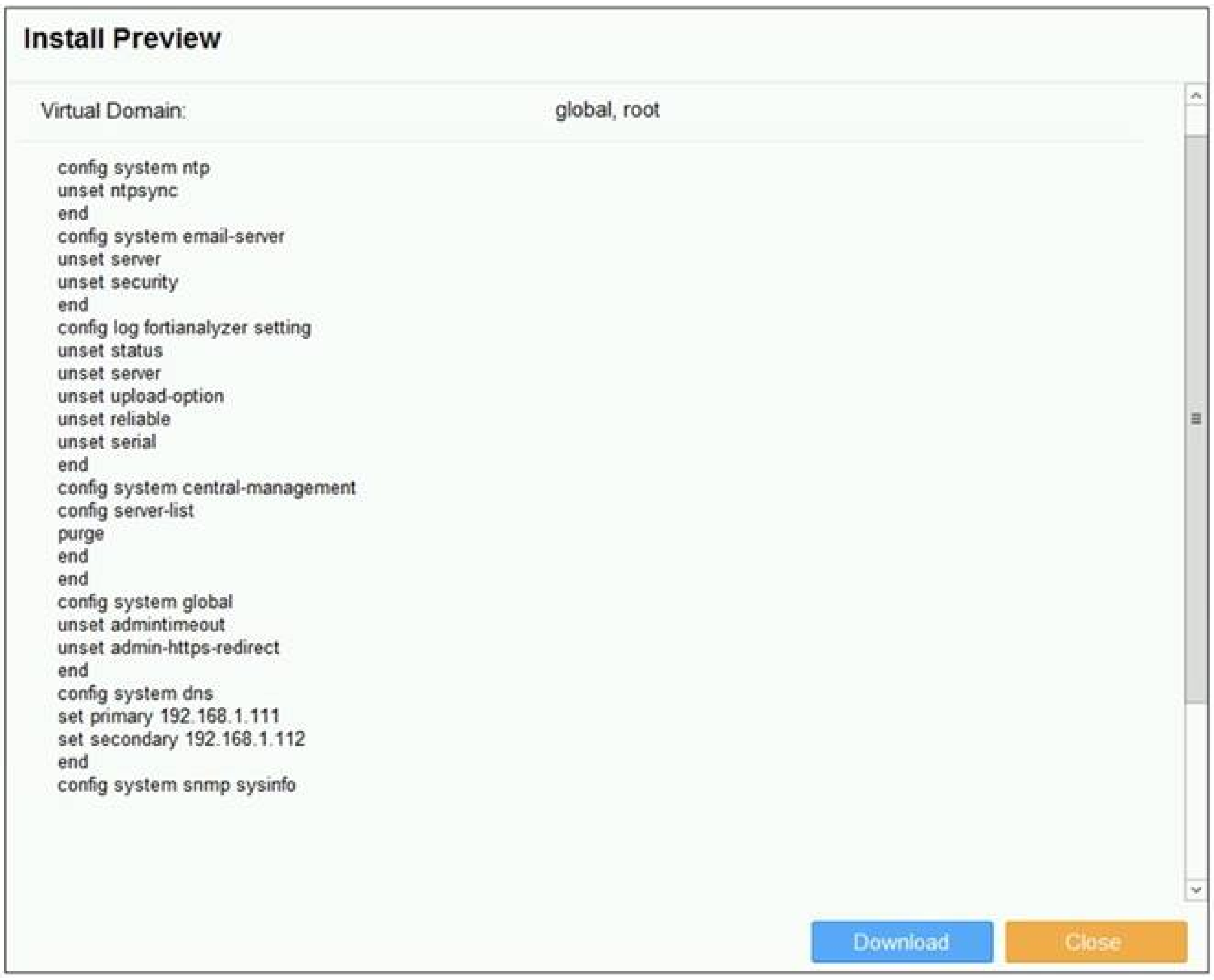
NTP Server
□Synchronize with NTP Server

Admin Settings
HTTP Port: 80 ☑ Redirects to
HTTPS Port: 443
SSH Port: 22
SSH v1 compatibility: OFF
Idle Timeout: 5 (1 - 480 mins)
Enable SCP: OFF
Switch Controller: OFF
View Settings
Language: English
Lines per page: 50 (20 - 1000)
Theme: Green
IPv6 Support on GUI: OFF

Replacement Message

□ Name	Description
▾ Administration (0)	
▾ Alert Email (0)	
▾ Authentication (0)	
▾ Device Detection Portal (0)	
▾ Email (0)	

Exhibit two.



Install Preview

Virtual Domain: global, root

```
config system ntp
unset ntpsync
end
config system email-server
unset server
unset security
end
config log fortianalyzer setting
unset status
unset server
unset upload-option
unset reliable
unset serial
end
config system central-management
config server-list
purge
end
end
config system global
unset admintimeout
unset admin-https-redirect
end
config system dns
set primary 192.168.1.111
set secondary 192.168.1.112
end
config system snmp sysinfo
```

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

Answer: B

NEW QUESTION 10
- (Topic 1)
Which two settings must be configured for SD-WAN Central Management? (Choose two.)

A. SD-WAN must be enabled on per-ADOM basis
B. You can create multiple SD-WAN interfaces per VDOM
C. When you configure an SD-WAN, you must specify at least two member interfaces.
D. The first step in creating an SD-WAN using FortiManager is to create two SD-WAN firewall policies.

Answer: AC

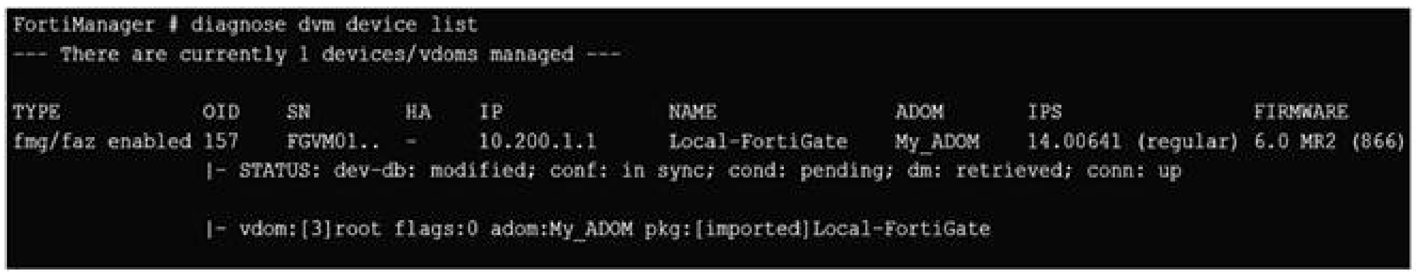
NEW QUESTION 15
- (Topic 1)
You are moving managed FortiGate devices from one ADOM to a new ADOM. Which statement correctly describes the expected result?

A. Any pending device settings will be installed automatically
B. Any unused objects from a previous ADOM are moved to the new ADOM automatically
C. The shared policy package will not be moved to the new ADOM
D. Policy packages will be imported into the new ADOM automaticallyD

Answer: C

Explanation:
Reference: https://community.fortinet.com/t5/FortiManager/Technical-Note-How-to-move-objects-to-new-ADOM-on-FortiManager/ta-p/198342

NEW QUESTION 19
- (Topic 1)
Refer to the exhibit.



```
FortiManager # diagnose dvm device list
--- There are currently 1 devices/vdoms managed ---

TYPE            OID    SN        HA    IP              NAME              ADOM      IPS                FIRMWARE
fmg/faz enabled 157    FGVM01..  -     10.200.1.1      Local-FortiGate   My_ADOM   14.00641 (regular) 6.0 MR2 (866)
                |- STATUS: dev-db: modified; conf: in sync; cond: pending; dm: retrieved; conn: up

                |- vdom:[3]root flags:0 adom:My_ADOM pkg:[imported]Local-FortiGate
```

Which two statements about the output are true? (Choose two.)

A. The latest revision history for the managed FortiGate does match with the FortiGate running configuration
B. Configuration changes have been installed to FortiGate and represents FortiGate configuration has been changed
C. The latest history for the managed FortiGate does not match with the device-level database
D. Configuration changes directly made on the FortiGate have been automatically updated to device-leveldatabase

Answer: AC

Explanation:
STATUS: dev-db: modified; conf: in sync; cond: pending; dm: retrieved; conn: up– dev-db: modified – This is the device setting status which indicates that configuration changes were made on FortiManager.– conf: in sync – This is the sync status which shows that the latest revision history is in sync with Fortigate's configuration.– cond: pending – This is the configuration status which says that configuration changes need to be installed.
Most probably a retrieve was done in the past (dm: retrieved) updating the revision history DB (conf: in sync) and FortiManager device level DB, now there is a new modification on FortiManager device level DB (dev-db: modified) which wasn't installed to FortiGate (cond: pending), hence; revision history DB is not aware of that modification and doesn't match device DB.
Conclusion:– Revision DB does match FortiGate.– No changes were installed to FortiGate yet.– Device DB doesn't match Revision DB.– No changes were done on FortiGate (auto-update) but configuration was retrieved instead
After an Auto-Update or Retrieve:device database = latest revision = FGT
Then after a manual change on FMG end (but no install yet):latest revision = FGT (still) but now device database has been modified (is different).
After reverting to a previous revision in revision history:device database = reverted revision != FGT

NEW QUESTION 24
- (Topic 2)
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?

A. Device name and serial number of the original device.
B. Device name and serial number of the replacement device.
C. Device name of the replacement device and serial number of the original device.
D. Device name of the original device and serial number of the replacement device.

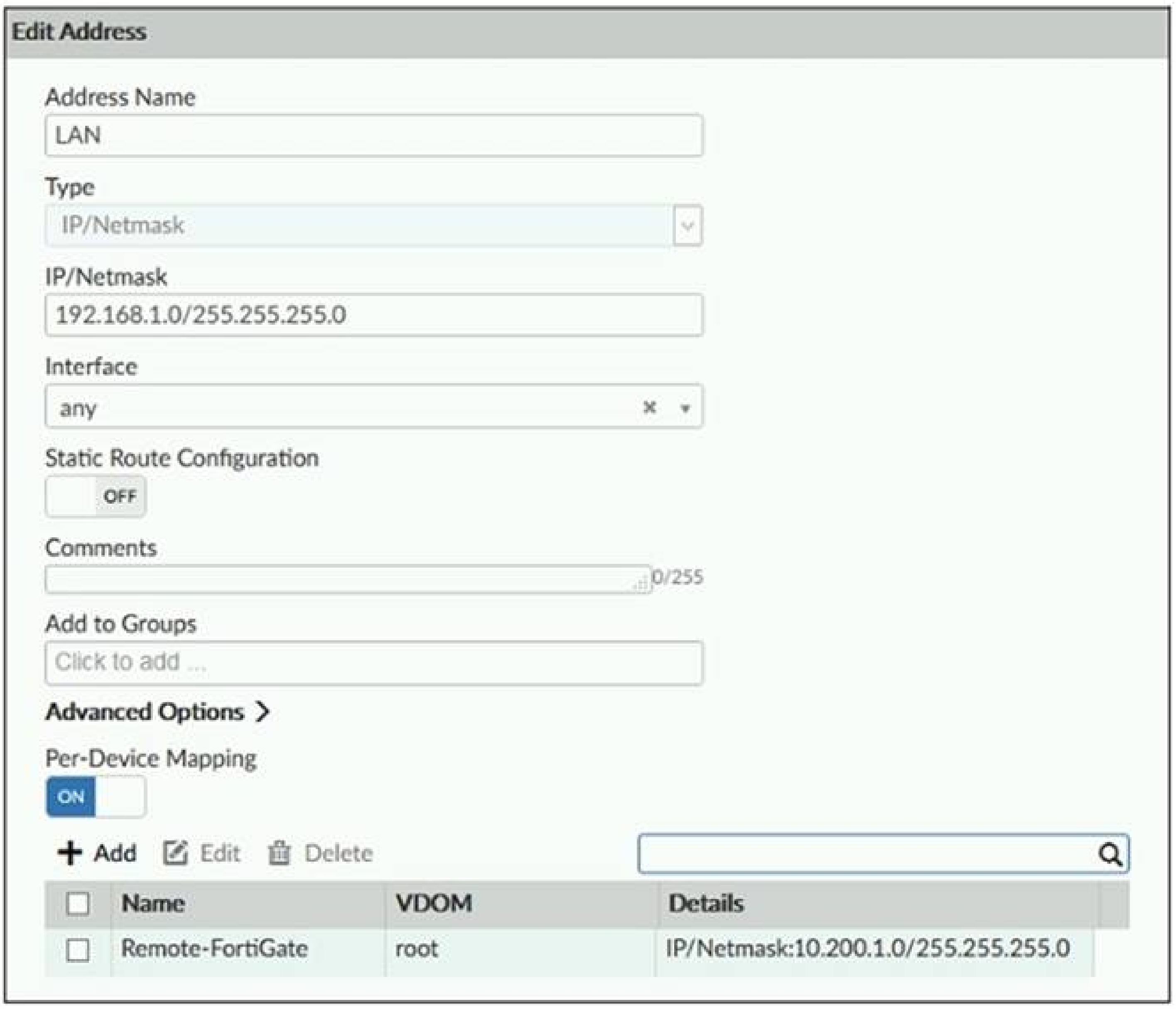
Answer: D

NEW QUESTION 25
- (Topic 2)
Which two statements regarding device management on FortiManager are true? (Choose two.)

A. FortiGate devices in HA cluster devices are counted as a single device.
B. FortiGate in transparent mode configurations are not counted toward the device count on FortiManager.
C. FortiGate devices in an HA cluster that has five VDOMs are counted as five separate devices.
D. The maximum number of managed devices for each ADOM is 500.

Answer: AC

NEW QUESTION 28
- (Topic 2)
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?

A. 192.168.0.1/24
B. 10.200.1.0/24
C. It will create a firewall address group on Local-FortiGate with 192.168.0.1/24 and 10.0.1.0/24 object values.
D. Local-FortiGate will automatically choose an IP/Netmask based on its network interface settings.

Answer: A

NEW QUESTION 33
- (Topic 2)
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

Answer: D

NEW QUESTION 37
- (Topic 2)
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

Answer: B

Explanation:
FortiManager 6.2 Study guide page 350

NEW QUESTION 41
- (Topic 2)
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 deviceindependently.
D. The policy configuration has never been imported after a device was registered on FortiManager.

Answer: C

NEW QUESTION 44
- (Topic 2)
Which two statements about Security Fabric integration with FortiManager are true? (Choose two.)

A. The Security Fabric license, group name and password are required for the FortiManager Security Fabricintegration
B. The Fabric View module enables you to generate the Security Fabric ratings for Security Fabric devices
C. The Security Fabric settings are part of the device level settings
D. The Fabric View module enables you to view the Security Fabric ratings for Security Fabric devices

Answer: CD

NEW QUESTION 49
- (Topic 2)
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 globalADOM.
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.

Answer: A

Explanation:
Global Policy Package is applied at the ADOM level and you have the option to choose which ADOM policy packages you want to exclude (there is no option to choose Policy Packages to include).

NEW QUESTION 51
- (Topic 2)
Which two items are included in the FortiManager backup? (Choose two.)

A. FortiGuard database
B. Global database
C. Logs
D. All devices

Answer: BD

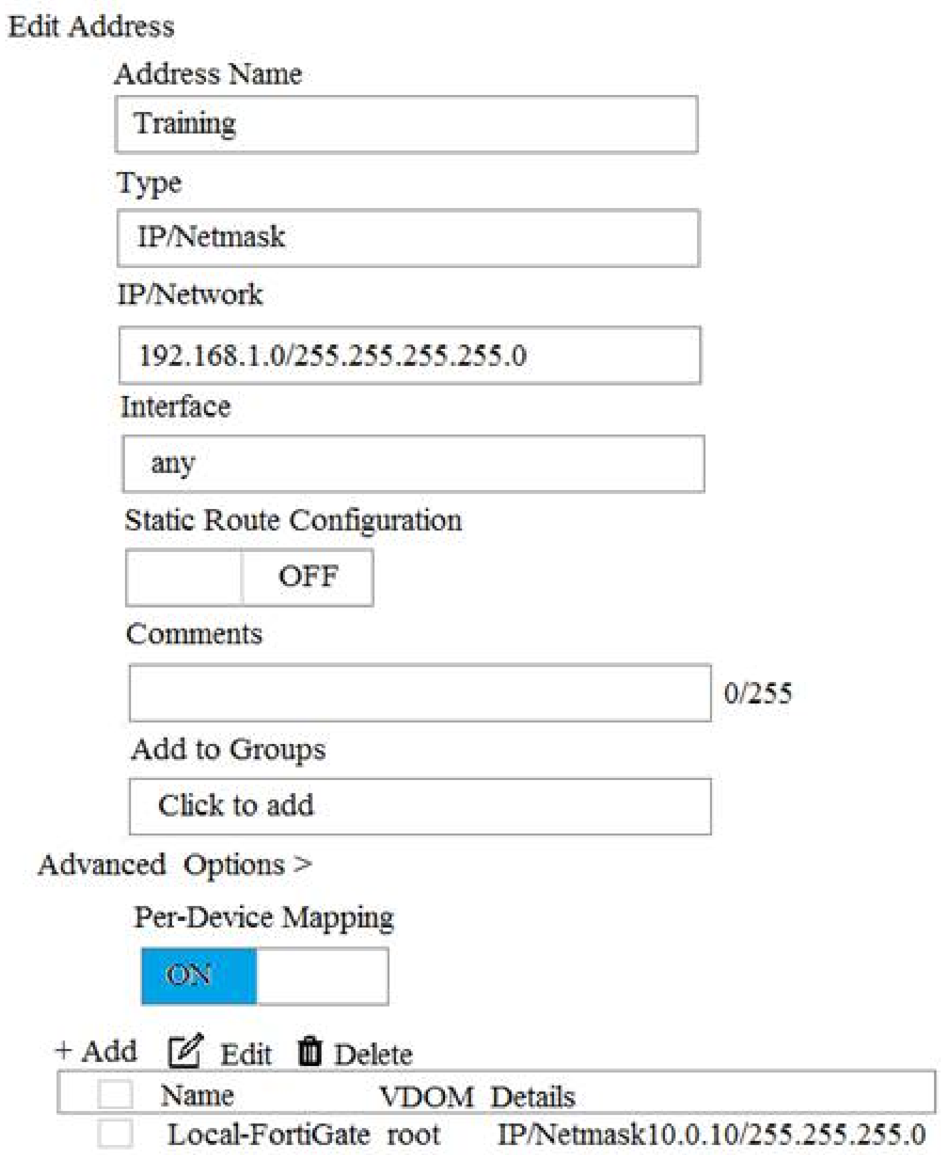
Explanation:
Reference: https://kb.fortinet.com/kb/viewContent.do?externalId=FD34549

NEW QUESTION 52
- (Topic 3)
Which of the following statements are true regarding reverting to previous revision version from the revision history? (Choose two.)

A. To push these changes to a managed device, it required an install operation to the managed FortiGate.
B. Reverting to a previous revision history will generate a new version ID and remove all other historyversions.
C. Reverting to a previous revision history will tag the device settings status as Auto- Update.
D. It will modify device-level database

Answer: AD

NEW QUESTION 54
- (Topic 3)
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?

A. 10.0.1.0/24
B. It will create firewall address group on Local-FortiGate with 192.168.0.1/24 and 10.0.1.0/24 object values
C. 192.168.0.1/24
D. Local-FortiGate will automatically choose an IP Network based on its network interface settings.

Answer: A

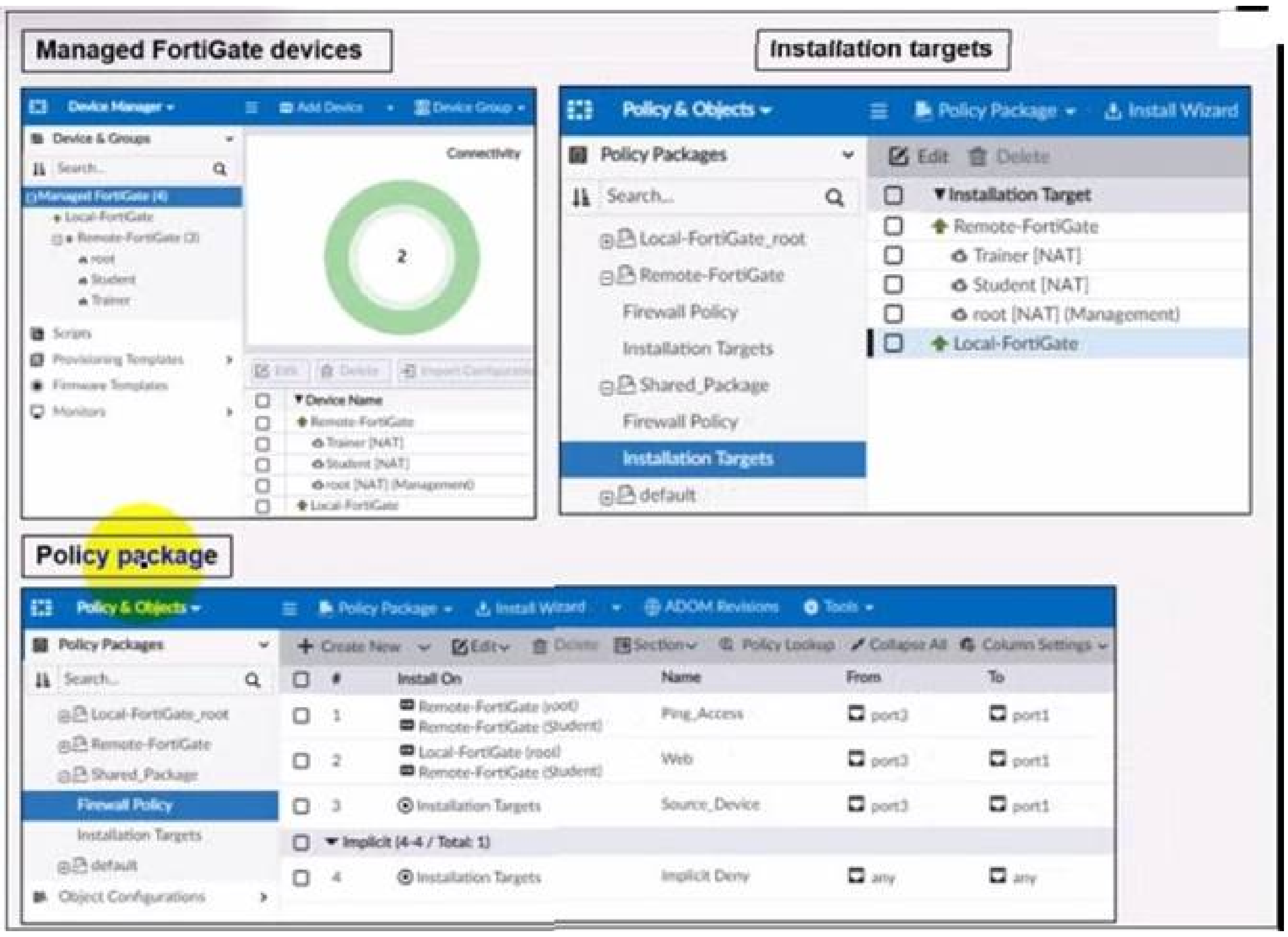
NEW QUESTION 57
- (Topic 3)
What does a policy package status of Modified indicate?

A. FortiManager is unable to determine the policy package status
B. The policy package was never imported after a device was registered on FortiManager
C. The Policy configuration has been changed on a managed device and changes have not yet been imported into FortiManager
D. The Policy package configuration has been changed on FortiManager and changes have not yet been installed on the managed device.

Answer: D

Explanation:
Reference: http://help.fortinet.com/fmgr/50hlp/56/5-6-1/FortiManager_Admin_Guide/1200_Policy%20and%20Objects/0800_Managing%20policy%20packages/2200_Policy%20Package%20Installation%20targets.htm

NEW QUESTION 61
- (Topic 3)
Refer to the exhibit.



☐	Installation Target
☐	Remote-FortiGate
☐	Trainer [NAT]
☐	Student [NAT]
☐	root [NAT] (Management)
☐	Local-FortiGate

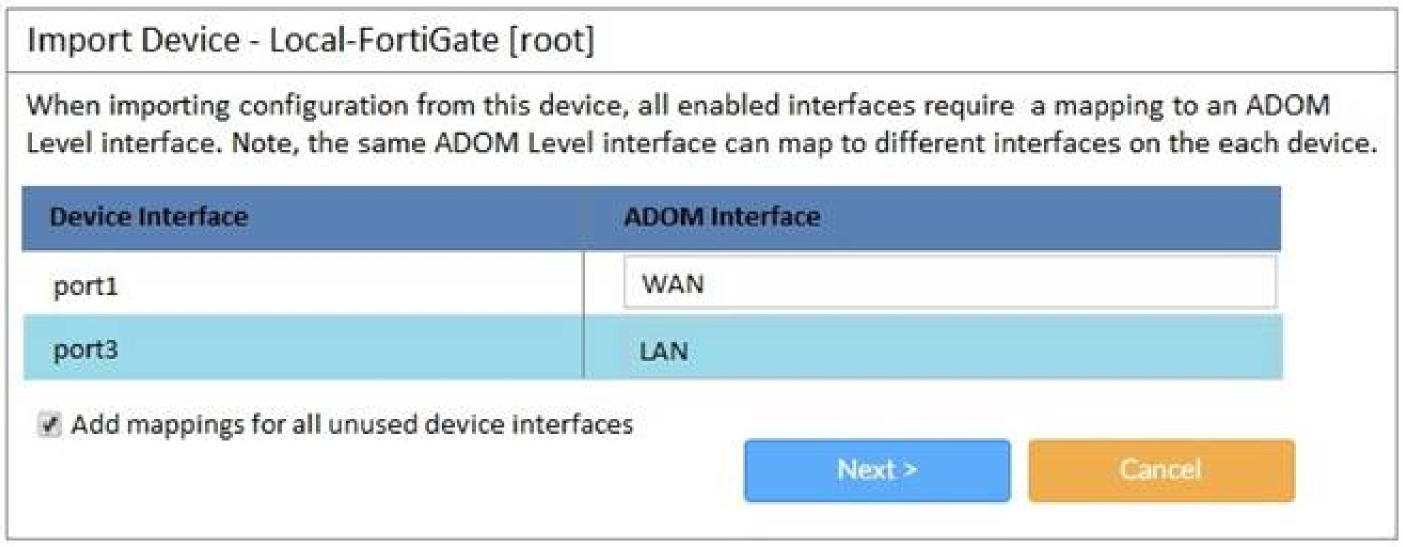
☐	#	Install On	Name	From	To
☐	1	Remote-FortiGate (root) Remote-FortiGate (Student)	Ping_Access	port3	port1
☐	2	Local-FortiGate (root) Remote-FortiGate (Student)	Web	port3	port1
☐	3	Installation Targets	Source_Device	port3	port1
☐	Implicit (4-4 / Total: 1)				
☐	4	Installation Targets	Implicit Deny	any	any

Given the configuration shown in the exhibit, what can you conclude from the installation targets m the Install On column? (Choose two)

A. Policy seq # 2 will not be installed on the Local-FortiGate root VDOM because there is no root VDOM in the Installation Target
B. Policy seq # 3 will be installed on all managed devices and VDOMs that are listed under Installation Targets
C. Policy seq # 1 will be installed on the Remoto-FortiGate root[NAT] and Student[NAT] VDOMs only
D. Policy 3 will be installed on all FortiGate devices and vdom belongs to the ADOM
E. Policy seq # 3 will be skipped because no installation targets are specified

Answer: BC

NEW QUESTION 65
- (Topic 3)
View the following exhibit:



Import Device - Local-FortiGate [root]

When importing configuration from this device, all enabled interfaces require a mapping to an ADOM Level interface. Note, the same ADOM Level interface can map to different interfaces on the the each device.

Device Interface	ADOM Interface
port1	WAN
port3	LAN

☑ Add mappings for all unused device interfaces

An administrator used the value shown in the exhibit when importing a Local-FortiGate into FortiManager. What name will be used to display the firewall policy for port1?

A. port1 on FortiGate and WAN on FortiManager
B. port1 on both FortiGate and FortiManager
C. WAN zone on FortiGate and WAN zone on FortiManager
D. WAN zone on FortiGate and WAN interface on FortiManager

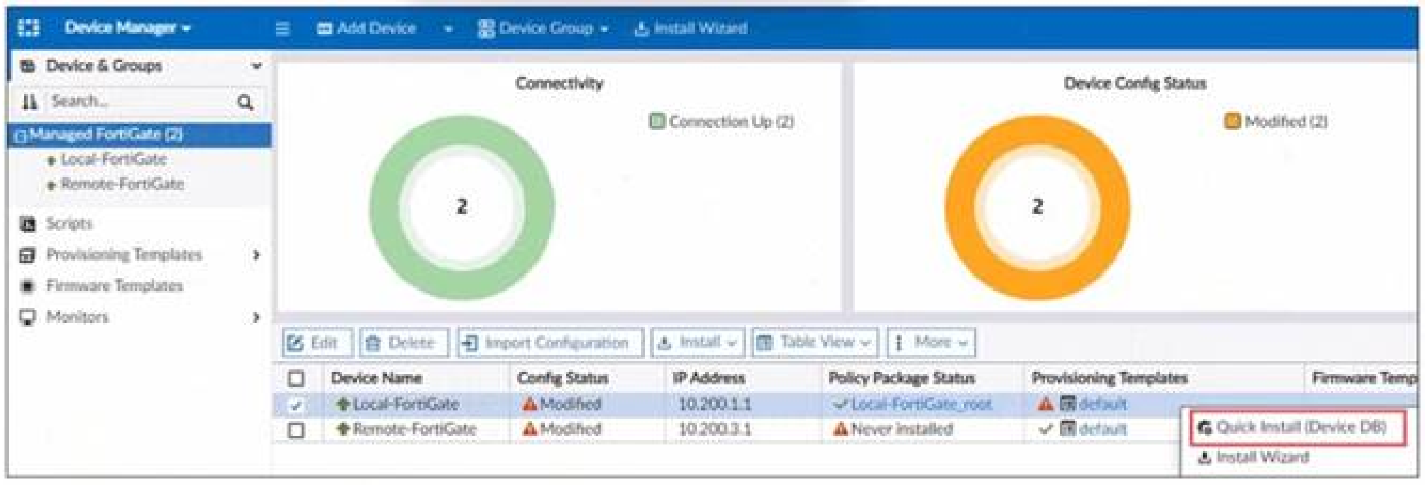
Answer: A

NEW QUESTION 69
- (Topic 3)
Which configuration setting for FortiGate is part of an ADOM-level database on FortiManager?

A. NSX-T Service Template
B. Security profiles
C. SNMP
D. Routing

Answer: D

NEW QUESTION 73
- (Topic 3)
Refer to the exhibit.



☐	Device Name	Config Status	IP Address	Policy Package Status	Provisioning Templates	Firmware Temp
✓	Local-FortiGate	Modified	10.200.1.1	✓Local-FortiGate_root	default	
☐	Remote-FortiGate	Modified	10.200.3.1	Never installed	✓ default	

You ate using the Quick install option to install configuration changes on the managed FortiGate
Which two statements correctly describe the result? (Choose two)

A. It installs device-level changes on the FortiGate device without launching the Install Wizard
B. It installs all the changes in the device database first and the administrator must reinstall the changes on the FodiGate device
C. It provides the option to preview only the policy package changes before installing them
D. It install provisioning template changes on the FortiGate device

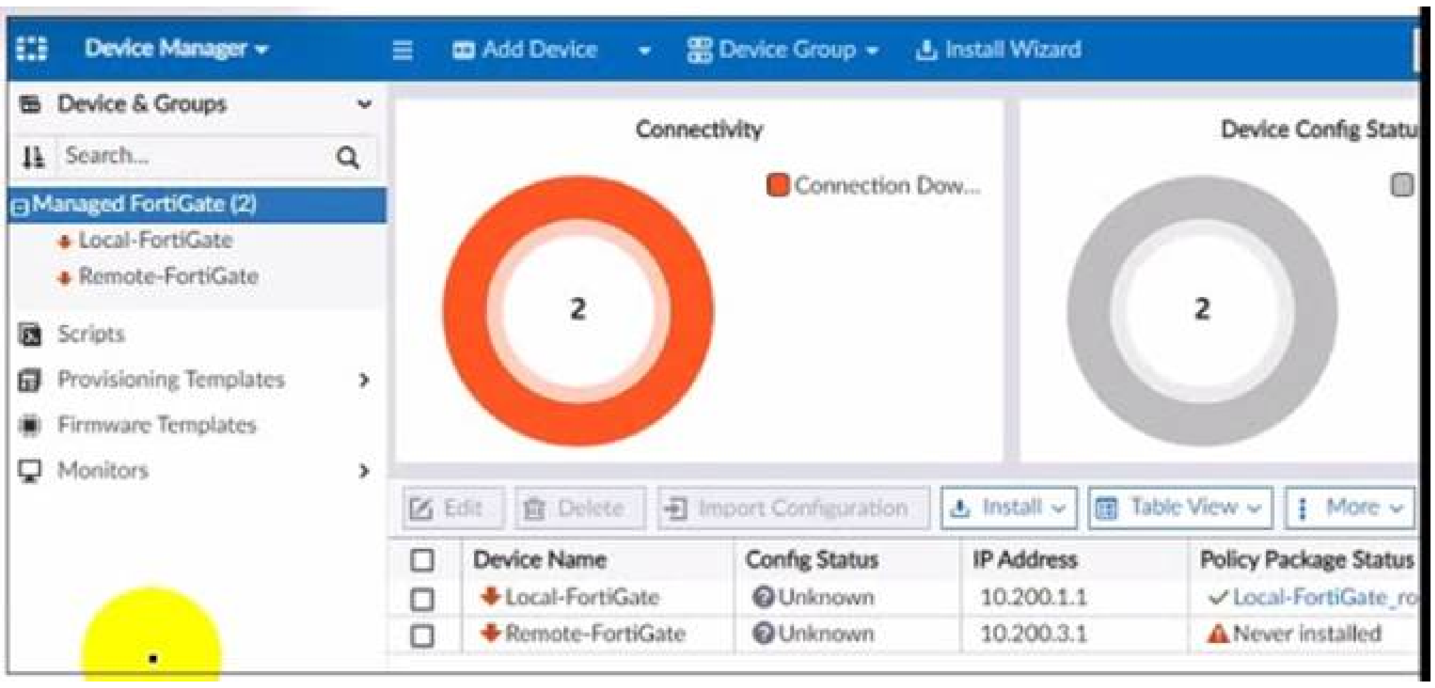
Answer: AD

NEW QUESTION 76
- (Topic 3)
Which two settings are required for FortiManager Management Extension Applications (MEA)? (Choose two.)

A. When you configure MEA, you must open TCP or UDP port 540.
B. You must open the ports to the Fortinet registry
C. You must create a MEA special policy on FortiManager using the super user profile
D. The administrator must have the super user profile.

Answer: CD

NEW QUESTION 79
- (Topic 3)
Refer to the exhibit.



☐	Device Name	Config Status	IP Address	Policy Package Status
☐	Local-FortiGate	Unknown	10.200.1.1	✓Local-FortiGate_ro
☐	Remote-FortiGate	Unknown	10.200.3.1	Never installed

A junior administrator is troubleshooting a FortiManager connectivity issue that rs occurring with managed FortiGate devices
Given the FortiManager device manager settings shown in the exhibit what can you conclude from the exhibit?

A. The administrator had restored the FortiManager configuration file
B. The administrator must refresh both devices to restore connectivity
C. FortiManager test internet connectivity therefore, both devices appear to be down
D. The administrator can reclaim the FGFM tunnel to get both devices online

Answer: C

NEW QUESTION 83
- (Topic 3)
An administrator is in the process of moving the system template profile between ADOMs by running the following command: execute improfile import-profile ADOM2 3547 /tmp/myfile Where does the administrator import the file from?

A. File system
B. ADOM1
C. ADOM2 object database
D. ADOM2

Answer: C

NEW QUESTION 84
- (Topic 3)
In addition to the default ADOMs, an administrator has created a new ADOM named Training for FortiGate devices. The administrator authorized the FortiGate device on FortiManager using the Fortinet Security Fabric.
Given the administrator's actions, which statement correctly describes the expected result?

A. The FortiManager administrator must add the authorized device to the Training ADOM using the Add Device wizard only.
B. The authorized FortiGate will be automatically added to the Training ADOM.
C. The authorized FortiGate will appear in the root ADOM.
D. The authorized FortiGate can be added to the Training ADOM using FortiGate Fabric Connectors.

Answer: C

NEW QUESTION 86
- (Topic 3)
Which of the following statements are true regarding VPN Manager? (Choose three.)

A. VPN Manager must be enabled on a per ADOM basis.
B. VPN Manager automatically adds newly-registered devices to a VPN community.
C. VPN Manager can install common IPsec VPN settings on multiple FortiGate devices at the same time.
D. Common IPsec settings need to be configured only once in a VPN Community for all managed gateways.
E. VPN Manager automatically creates all the necessary firewall policies for traffic to be tunneled by IPsec.

Answer: ACD

NEW QUESTION 88
- (Topic 3)
Push updates are failing on a FortiGate device that is located behind a NAT device Which two settings should the administrator check? (Choose two.)

A. That the virtual IP address and correct ports are set on the NAT device
B. That the NAT device IP address and correct ports are configured on FortiManager
C. That the external IP address on the NAT device is set to DHCP and configured with the virtual IP
D. That the override server IP address is set on FortiManager and the NAT device

Answer: BC

NEW QUESTION 90
- (Topic 3)
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?

A. port2
B. virtual-wan-link
C. port1
D. auto-discovery

Answer: B

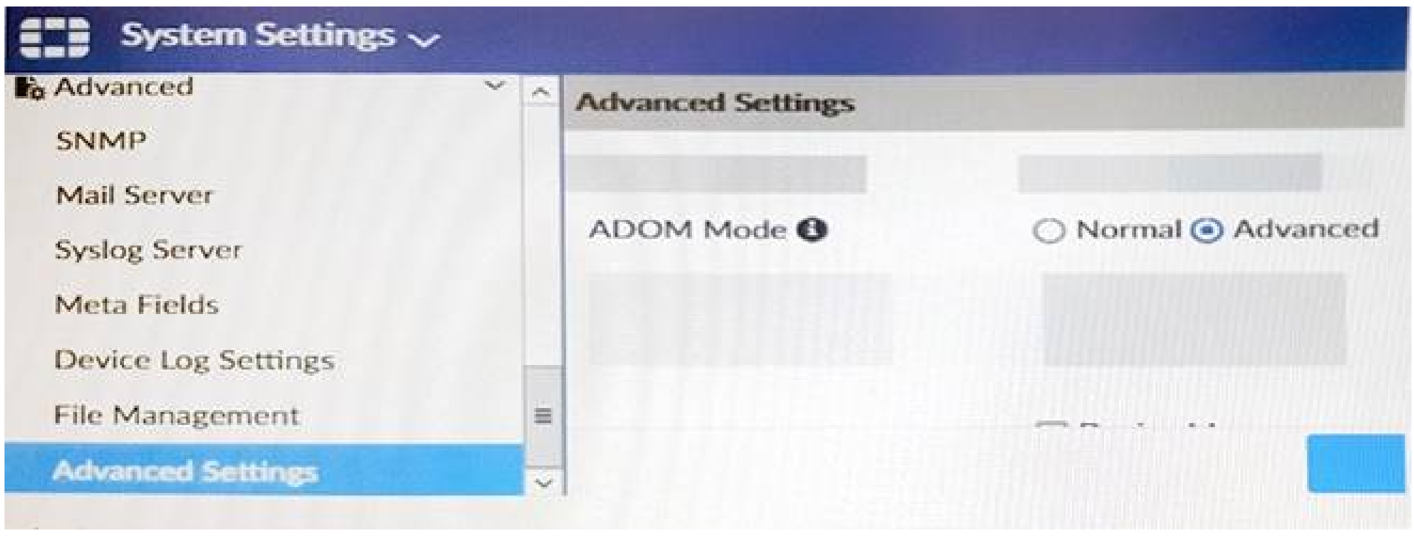
NEW QUESTION 94
- (Topic 3)
Which of the following statements are true regarding VPN Gateway configuration in VPN Manager? (Choose two.)

A. Managed gateways are devices managed by FortiManager in the same ADOM
B. External gateways are third-party VPN gateway devices only
C. Protected subnets are the subnets behind the device that you don’t want to allow access to over the IPsecVPN
D. Managed devices in other ADOMs must be treated as external gateways

Answer: AD

Explanation:
Reference: http://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMG-FAZ/1300_VPN_Manager/0800_IPsec_VPN_Gateway/0400_Create_mngd_gateway.htm

NEW QUESTION 97
- (Topic 3)
View the following exhibit.



Advanced Settings

ADOM Mode ○ Normal ● Advanced

Which of the following statements are true based on this configuration setting? (Choose two.)

A. This setting will enable the ADOMs feature on FortiManager.
B. This setting is applied globally to all ADOMs.
C. This setting will allow assigning different VDOMs from the same FortiGate to different ADOMs.
D. This setting will allow automatic updates to the policy package configuration for a managed device.

Answer: BC

NEW QUESTION 101

......