NSE5_FMG-7.2 Dumps

Fortinet NSE 5 - FortiManager 7.2

https://www.certleader.com/NSE5_FMG-7.2-dumps.html

NEW QUESTION 1
- (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: C

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 2
- (Topic 1)
An administrator would like to create an SD-WAN using central management in theTrainingADOM.
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 theTrainingADOM
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)
Which two statements about the scheduled backup of FortiManager are true? (Choose two.)

A. It does not back up firmware images saved on FortiManager.
B. It can be configured using the CLI and GUI.
C. It backs up all devices and the FortiGuard database.
D. It supports FTP, SCP, and SFTP.

Answer: AD

Explanation:
Reference:https://docs.ansible.com/ansible/latest/collections/fortinet/fortimanager/fmgr_system_backup_allsettings_module.html

NEW QUESTION 4
- (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 5
- (Topic 1)
What are two outcomes of ADOM revisions? (Choose two.)

A. ADOM revisions can significantly increase the size of the configuration backups.
B. ADOM revisions can save the current size of the whole ADOM
C. ADOM revisions can create System Checkpoints for the FortiManager configuration
D. ADOM revisions can save the current state of all policy packages and objects for an ADOM

Answer: AD

Explanation:
Reference:https://docs2.fortinet.com/document/fortimanager/6.0.0/best- practices/101837/adom-revisions

NEW QUESTION 6
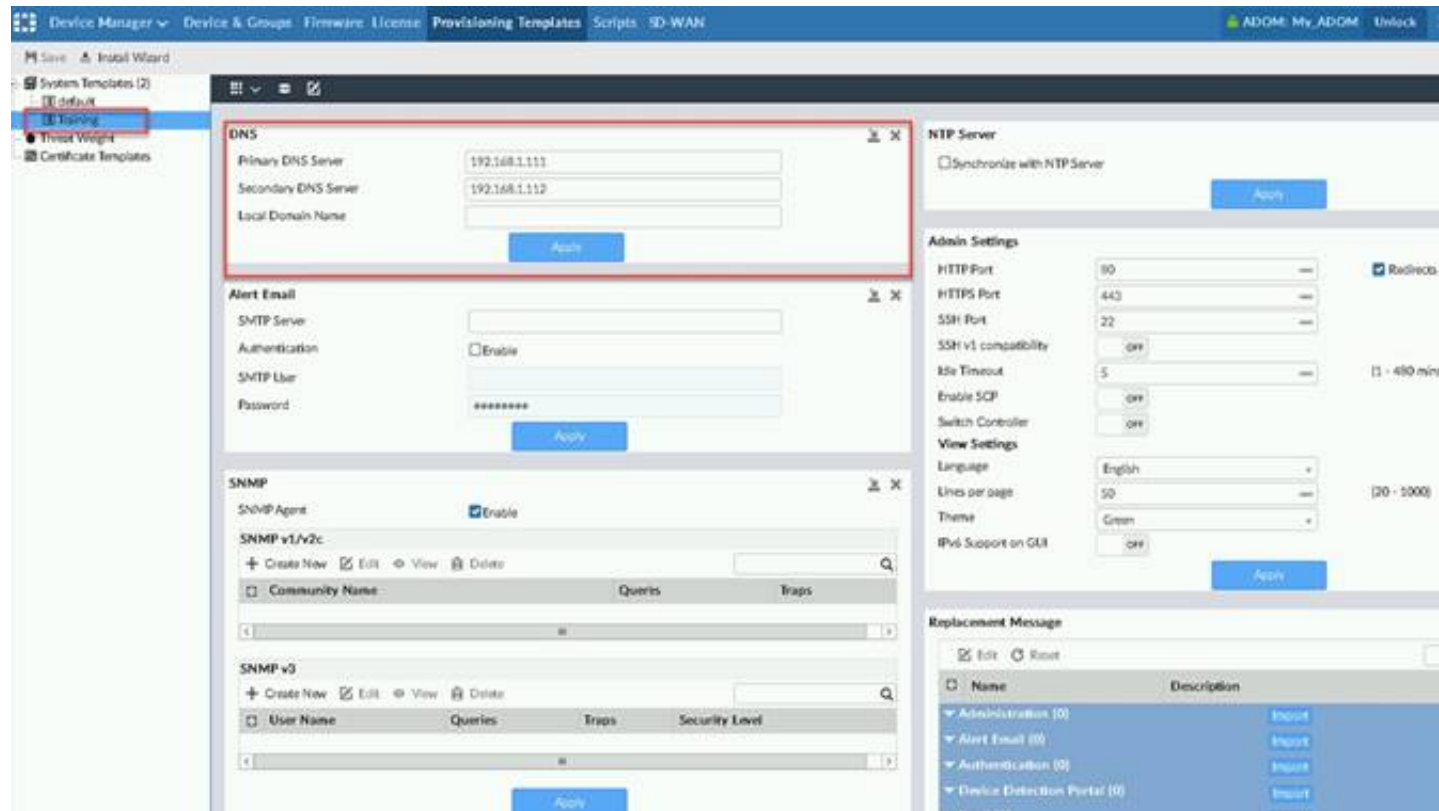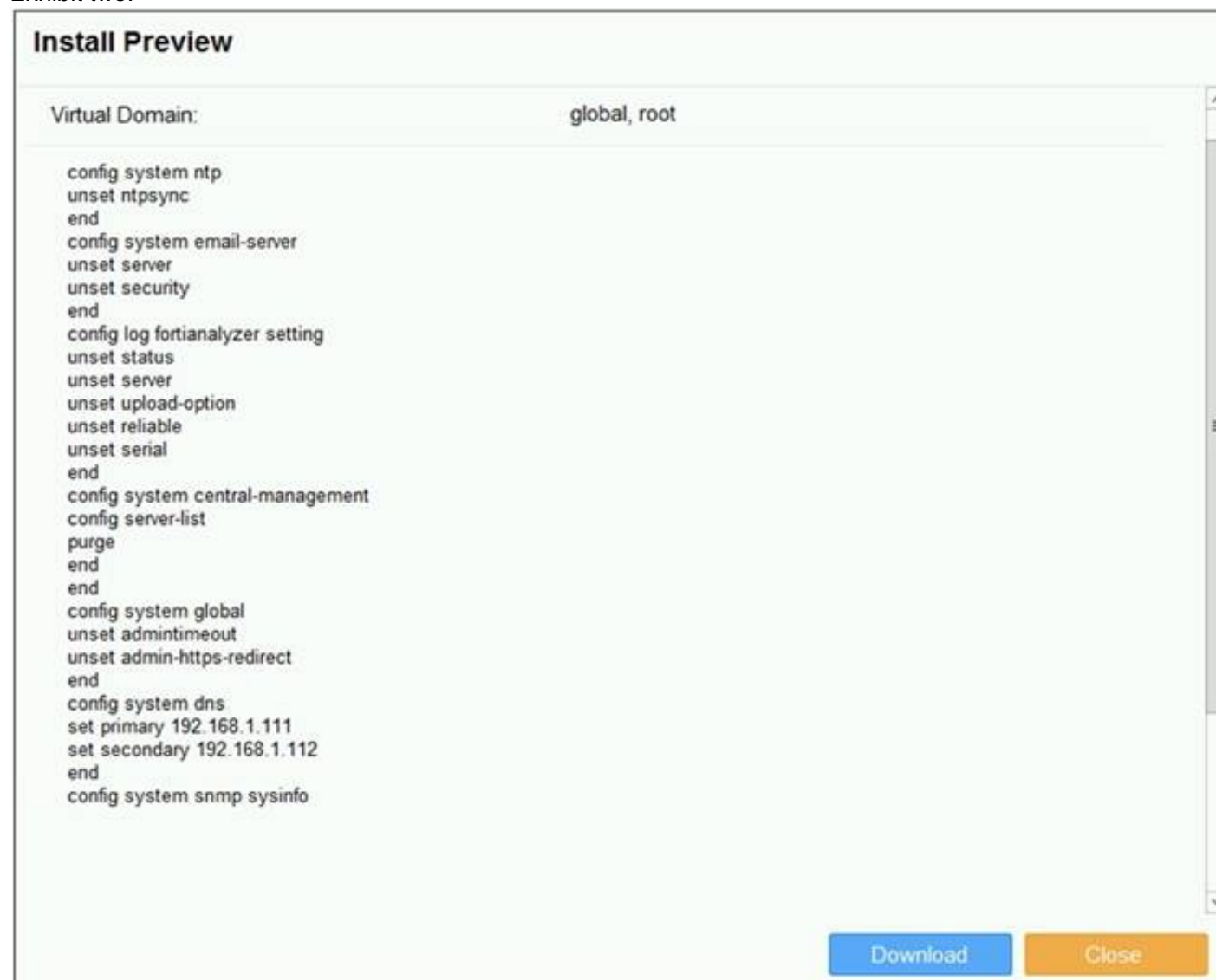- (Topic 1)

Refer to the exhibits. Exhibit one.

Exhibit two.

An administrator created a new system template namedTrainingwith 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 theTrainingsystem template
B. TheTrainingsystem template has other default settings
C. The ADOM is locked by another administrator
D. TheTrainingsystem template does not have assigned devices

Answer: B

NEW QUESTION 7
- (Topic 1)
View the following exhibit, which shows theDownload 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 8
- (Topic 1)
View the following exhibit:


```
#diagnose fmupdate view-serverlist fds
Fortiguard Server Comm: Enabled
Server Override Mode: Loose
FDS server list :
Index Address          Port    TimeZone   Distance   Source
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
*0   10.0.1.50         8890    -5         0          CLI
1    96.45.33.89       443     -5         0          FDNI
2    96.45.32.81       443     -5         0          FDNI
....
38 fds1.fortinet.com   443     -5         0          DEFAULT
```

How will FortiManager try to get updates for antivirus and IPS?

A. From the list of configured override servers with ability to fall back to public FDN servers
B. From the configured override server list only
C. From the default serverfdsl.fortinet.com
D. From public FDNI server with highest index number only

Answer: A

Explanation:
Reference:https://community.fortinet.com/t5/Fortinet-Forum/Clarification-of-FortiManager-s-quot-Server-Override-Mode-quot/td-p/89973

NEW QUESTION 9
- (Topic 1)
Which three settings are the factory default settings on FortiManager? (Choose three.)

A. Username is admin
B. Password is fortinet
C. FortiAnalyzer features are disabled
D. Reports and Event Monitor panes are enabled
E. port1 interface IP address is 192.168.1.99/24

Answer: ACE

NEW QUESTION 10
- (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
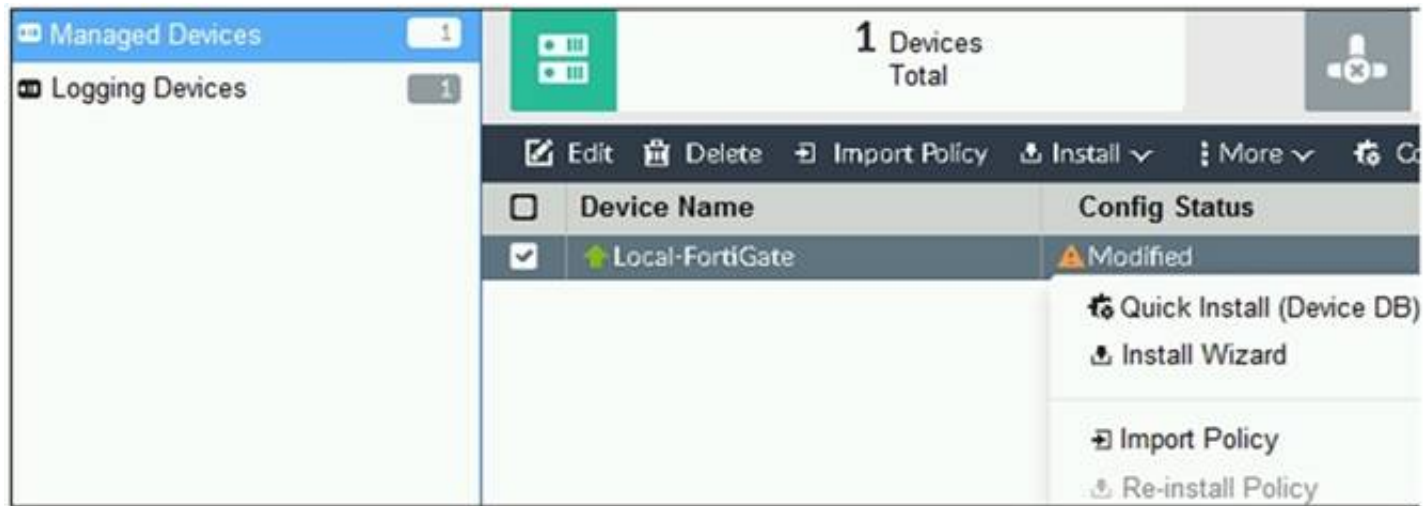D. FortiManager can be used only as a logging device.

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 10
- (Topic 1)
Refer to the exhibit.

You are using theQuick Installoption 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 theInstall 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

Answer: BC

Explanation:
FortiManager_6.4_Study_Guide-Online – page 164
The Install Config option allows you to perform a quick installation of device-level settings without launching the Install Wizard. When you use this option, you cannot preview the changes prior to committing. Administrator should be certain of the changes before using this install option, because the install can't be cancelled after the process is initiated.

NEW QUESTION 11
- (Topic 1)
View the following exhibit.

Starting Log (Run the device)

Start installing
Local-FortiGate $ config user device
Local-FortiGate (device) $ edit "mydevice"
new entry 'mydevice' added
Local-FortiGate (mydevice) $ next
MAC address can not be 0
Node_check_object fail!for mac 00:00:00:00:00:00
Attribute 'mac' value '00:00:00:00:00:00' checkingfail -33
Command fail. Return code 1
Local-FortiGate (device) $ end
...
Local-FortiGate $ config firewall policy
Local-FortiGate (policy) $ edit 2
New entry '2' added
Local-FortiGate (2) $ set name "Device_policy"
Local-FortiGate (2) $ set uuid 64...
Local-FortiGate (2) $ set srcintf "port3"
Local-FortiGate (2) $ set dstintf "port1"
Local-FortiGate (2) $ set srcaddr "all"
Local-FortiGate (2) $ set dstaddr "all"
Local-FortiGate (2) $ set action accept
Local-FortiGate (2) $ set schedule "always"
Local-FortiGate (2) $ set service "ALL"
Local-FortiGate (2) $ set devices "mydevice"
Entry not found in datasource
Value parse error before 'mydevice'
Command fail. Return code -3
Local-FortiGate (2) $ set nat enable
Local-FortiGate (2) $ next
Local-FortiGate (policy) $ end
...

Which statement is true regarding this failed installation log?

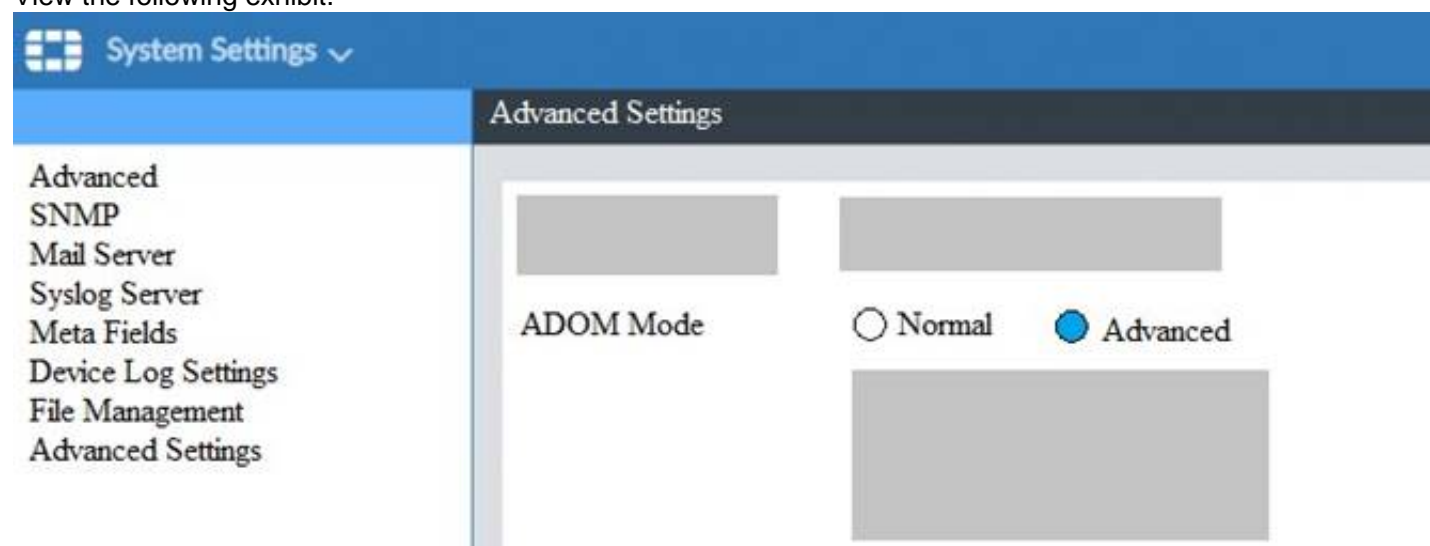A. Policy ID 2 is installed without a source address
B. Policy ID 2 will not be installed
C. Policy ID 2 is installed in disabled state
D. Policy ID 2 is installed without a source device

Answer: B

NEW QUESTION 15
- (Topic 1)
View the following exhibit.

What is the purpose of settingADOM ModetoAdvanced?

A. The setting allows automatic updates to the policy package configuration for a managed device
B. The setting enables the ADOMs feature on FortiManager
C. This setting allows you to assign different VDOMs from the same FortiGate to different ADOMs.
D. The setting disables concurrent ADOM access and adds ADOM locking

Answer: C

Explanation:
Reference:https://docs.fortinet.com/document/fortianalyzer/7.0.0/administration-guide/66530/adom-device-modes

NEW QUESTION 20
- (Topic 1)
View the following exhibit:

Create New CLI Script

Script Name	Config	
Comments	Write a comment	0/255
Type	CLI Script	
Run Script on	Remote FortiGate Directly(via CLI)	

[View Sample Script]

Script Detail

```
config vpn ipsec phase1-interface
edit "H25_0"
set auto-discovery-sender enable
next
end
config system interface
edit "H25_0"
set vdom "root"
set ip 172.16.1.1 255.255.255.255
set remote-ip 172.16.1.254
next
end
config router bgp
set as 65100
set router-id 172.16.1.1
config neighbor-group
```

Advanced Device Filters

Which two statements are true if the script is executed using theRemote FortiGate Directly (via CLI)option? (Choose two.)

A. You must install these changes usingInstall Wizard
B. FortiGate will auto-update the FortiManager's device-level database.
C. FortiManager will create a new revision history.
D. FortiManager provides a preview of CLI commands before executing this script on a managed FortiGate.

Answer: BC

NEW QUESTION 22
- (Topic 1)
View the following exhibit.

Given the configurations shown in the exhibit, what can you conclude from the installation targets in theInstall Oncolumn?

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

Answer: B

NEW QUESTION 27
- (Topic 1)
Refer to the exhibit.

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 32
- (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 asAuto-Update
C. It will generate a new versionIDand remove all other revision history versions

D. It will modify the device-level database

Answer: D

NEW QUESTION 35
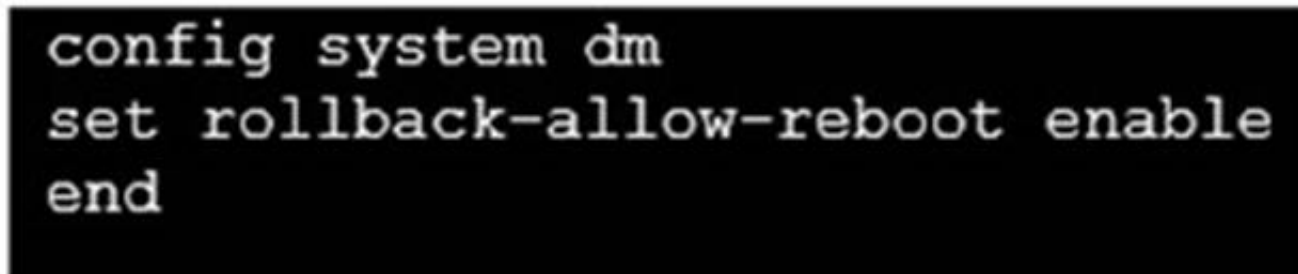- (Topic 2)
What does a policy package status ofConflictindicate?

A. The policy package reports inconsistencies and conflicts during aPolicy 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 36
- (Topic 2)
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?

A. It allows FortiGate to unset central management settings.
B. It allows FortiGate to reboot and recover the previous configuration from its configuration file.
C. It allows the FortiManager to revert and install a previous configuration revision on the managed FortiGate.
D. It allows FortiGate to reboot and restore a previously working firmware image.

Answer: B

Explanation:
Reference:https://docs.fortinet.com/document/fortimanager/6.2.0/fortigate-fortimanager-communicationsprotocol-guide/141304/fgfm-recovery-logic

NEW QUESTION 41
- (Topic 2)
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

Answer: C

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD47942

NEW QUESTION 42
- (Topic 2)
Refer to the exhibit.

Which two statements about an ADOM set inNormalmode on FortiManager are true? (Choose two.)

A. It supports the FortiManager script feature
B. It allows making configuration changes for managed devices on FortiManager panes
C. FortiManager automatically installs the configuration difference in revisions on the managed FortiGate
D. You cannot assign the same ADOM to multiple administrators

Answer: AB

Explanation:
"FortiGate units in the ADOM will query their own configuration every 5 seconds. If there has been a configuration change, the FortiGate unit will send a diff revision on the change to the FortiManager using the FGFM protocol."

NEW QUESTION 44
- (Topic 2)
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 panesdo notappear? (Choose two.)

A. The administrator logged in using the unsecure protocol HTTP, so the view is restricted.
B. The administrator profile does not have full access privileges like theSuper_Userprofile.
C. The administrator IP address is not a part of the trusted hosts configured on FortiManager interfaces.
D. FortiAnalyzer features are not enabled on FortiManager.

Answer: BD

NEW QUESTION 46
- (Topic 2)
Refer to the exhibit.

Which two statements are true if the script is executed using the Device Database option? (Choose two.)

A. You must install these changes using the Install Wizard to a managed device
B. The successful execution of a script on the Device Database will create a new revision history
C. The script history will show successful installation of the script on the remote FortiGate
D. The Device Settings Status will be tagged as Modified

Answer: AD

NEW QUESTION 50
- (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.
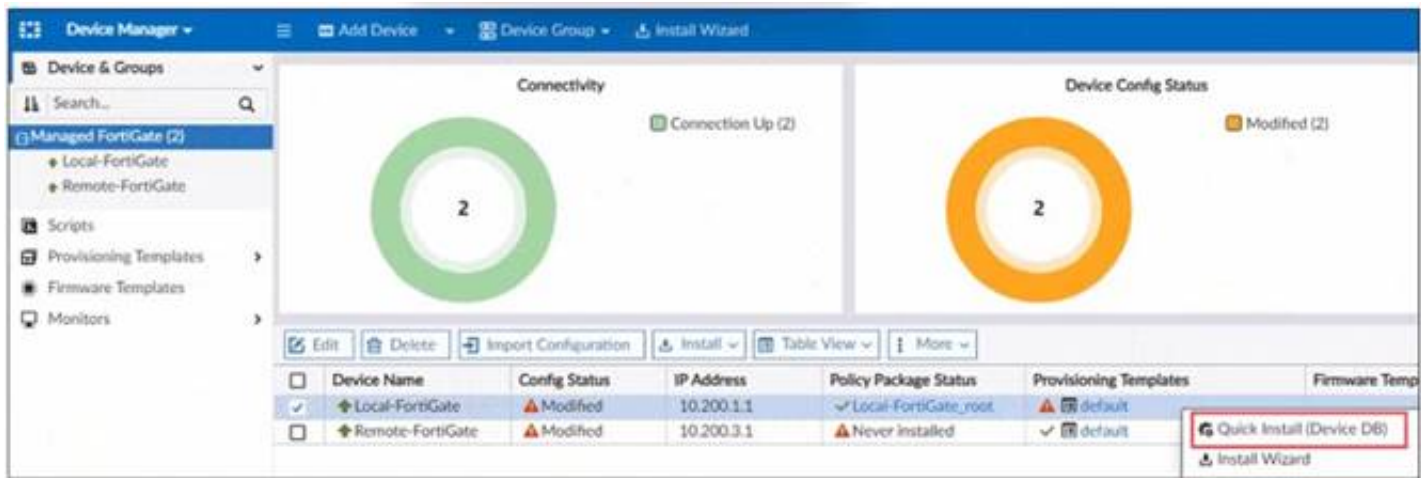
Answer: B

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 52
- (Topic 3)
Refer to the exhibit.

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 53
- (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 57
- (Topic 3)
Refer to the exhibit.
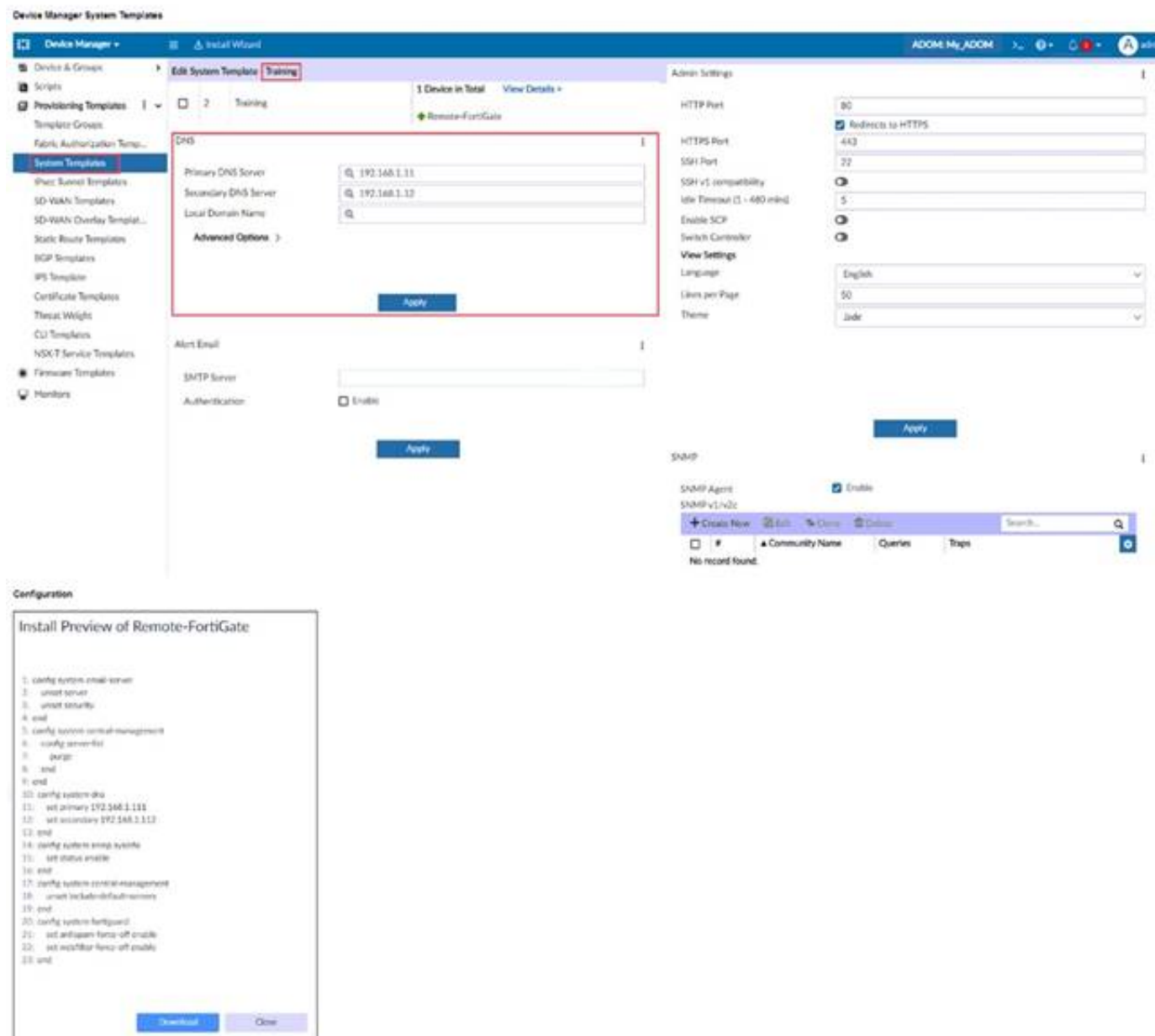
On FortiManager, an administrator created a new system template named Training with two new DNS addresses. During the installation preview stage, the administrator notices that central-management settings need to be purged.
What can be the main reason for the central-management purge command?

A. The Remote-FortiGate device does not have any DNS server-list configured in the central-management settings.
B. The DNS addresses in the default system settings are the same as the Training system template.
C. The ADOM is locked by another administrator.
D. The Training system template has a default FortiGuard widget.

Answer: A

NEW QUESTION 59
- (Topic 3)
Refer to the exhibit.

An administrator is about to add the FortiGate device to FortiManager using the discovery process FortiManager is operating behind a NAT device, and the administrator configured the FortiManager NATed IP address under the FortiManager system administration settings
What is the expected result?

A. During discovery FortiManager sets trie FortiManager NATed IP address on FortiGate

B. During discovery FortiManager sets both tie FortiManager NATed IP address and NAT device IP address on FortiGate
C. During discovery FortiManager sets the NATed device IP address on FortiGate
D. During discovery FortiManager uses only the FortiGate serial number to establish the connection

Answer: C

NEW QUESTION 60
- (Topic 3)
An administrator would like to create an SD-WAN using central management. What steps does the
administrator need to perform to create an SD-WAN using central management?

A. First create an SD-WAN firewall policy, add member interfaces to the SD-WAN template and create a static route
B. You must specify a gateway address when you create a default static route
C. Remove all the interface references such as routes or policies
D. Enable SD-WAN central management in the ADOM, add member interfaces, create a static route and SDWAN firewall policies.

Answer: D

NEW QUESTION 62
- (Topic 3)
An administrator created a header and footer global policy package and assigned it to an ADOM.
What are two outcomes from this action? (Choose two.)

A. You must manually move the header and footer policies after the policy assignment.
B. After you assign the global policy package to an ADOM, the policy package is hiddenfrom the ADOM and cannot be viewed.
C. If you assign an additional global policy package to the same ADOM, FortiManaqer removes previously assigned policies.
D. You can edit or delete all the global objects in the global ADOM.

Answer: AD

NEW QUESTION 64
- (Topic 3)
An administrator has assigned a global policy package to custom ADOM1. Then the administrator creates a new policy package Fortinet in the custom ADOM1.
What will happen to the Fortinet policy package when it is created?
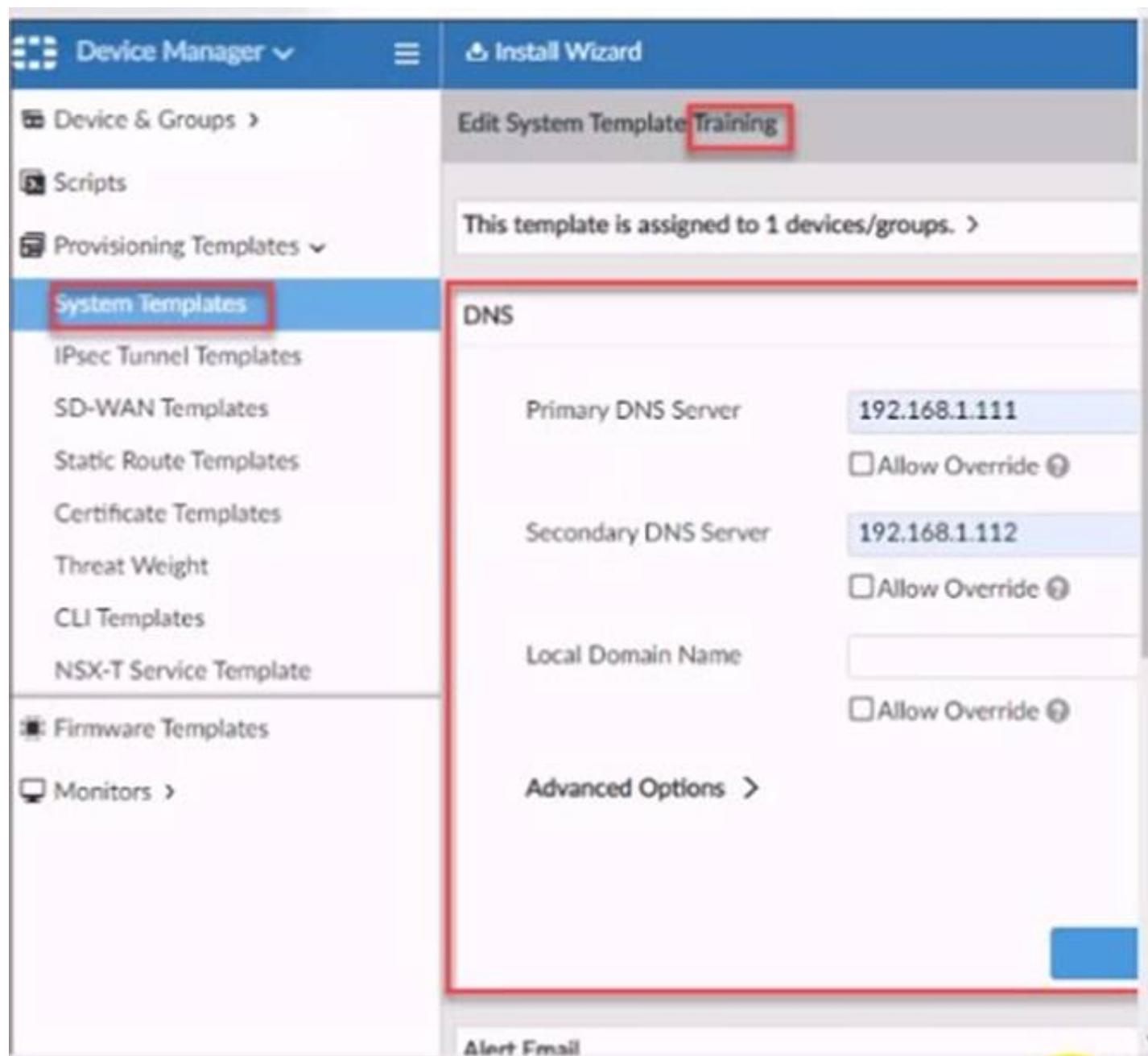
A. You need to assign the global policy package from the global ADOM
B. You need to reapply the global poky package to the ADOM
C. it automatically assigns the global policies
D. You can select the option to assign the global polices

Answer: C

NEW QUESTION 65
- (Topic 3)
Refer to the exhibit.

According to the error message why is FortiManager failing to add the FortiAnalyzer device?

A. The administrator must turn off the Use Legacy Device login and add the FortiAnalyzer device to the same network as Forti-Manager
B. The administrator must select the Forti-Manager administrative access checkbox on the FortiAnalyzer management interface
C. The administrator must use the Add Model Device section and discover the FortiAnalyzer device
D. The administrator must use the correct user name and password of the FortiAnalyzer device

Answer: A

NEW QUESTION 67
- (Topic 3)
Which three settings are the factory default settings on FortiManager? (Choose three.)

A. The administrative domain is disabled.
B. The Port1 interface IP address is 192.168.1.99/24.
C. Management Extension applications are enabled.
D. The FortiManager setup wizard is disabled.
E. FortiAnalvzer features are disabled.

Answer: ABE

NEW QUESTION 70
- (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 versionIDand remove all other historyversions.
C. Reverting to a previous revision history will tag the device settings status asAuto- Update.
D. It will modify device-level database

Answer: AD

NEW QUESTION 75
- (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

+ Add ☑ Edit 🗑 Delete

	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 78
- (Topic 3)
Refer to the exhibit.

```
Request
POST http://localhost:8080/fpc/api/customers/1/policytabs
Headers
accept: application/json
content-type: application/json
fpc-sid: $FPCSID
Cookie: JSESSIONID=$FPCSID
Payload
{
"centralNat": true,
"interfacePolicy6": false,
"dosPolicy6": false,
"policy64": false,
"interfacePolicy": true,
"policy6": false,
"dosPolicy": false,
"policy46": false,
"id": 1,
"customerId": 1
}
Response
Status 200 OK
```

Which statement is true about the FortiManager ADOM policy tab based on the API request?

A. The API command has enabled both central NAT and interface policy on the policy tab.
B. The API command has requested the policy tab permissions information only.
C. The API command has failed when requesting policy tab permissions information.
D. The API command has applied to customer with ID: 200.

Answer: A

NEW QUESTION 83
- (Topic 3)
Refer to the exhibit.

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 86
- (Topic 3)
View the following exhibit:

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 87
- (Topic 3)
An administrator would like to authorize a newly-installed AP using AP Manager. What steps does the administrator need to perform to authorize an AP?

A. Authorize the new AP using AP Manager and wait until the change is updated on the FortiA
B. Changes to the AP's state do not require installation.
C. Changes to the AP's state must be performed directly on the managed FortiGate.
D. Authorize the new AP using AP Manager and install the policy package changes on the managed FortiGate.
E. Authorize the new AP using AP Manager and install the device level settings on the managed FortiGate.

Answer: D

NEW QUESTION 88
- (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: B

NEW QUESTION 92
- (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 IPsec VPN
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 95
......

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your NSE5_FMG-7.2 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE5_FMG-7.2-dumps.html