



Fortinet

Exam Questions NSE5_FMG-7.0

Fortinet NSE 5 - FortiManager 7.0

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)

View the following exhibit.

Import Device - Local-FortiGate [root]

Create a new policy package for import.

Policy Package Name

Folder

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?

- A. The unused objects that are not tied to the firewall policies will be installed on FortiGate
- B. The unused objects that are not tied to the firewall policies will remain as read-only locally on FortiGate
- C. The unused objects that are not tied to the firewall policies locally on FortiGate will be deleted
- D. The unused objects that are not tied to the firewall policies in policy package will be deleted from theFortiManager database

Answer: C

Explanation:

Reference: <https://community.fortinet.com/t5/FortiManager/Import-all-objects-Versus-Import-only-policy-dependent-objects/ta-p/193259?externalID=FD40392>

NEW QUESTION 3

- (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: D

NEW QUESTION 4

- (Topic 1)

Refer to the exhibit.

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

"firewall service category",SKIPPED,"(name=General, oid=697, DUPLICATE)"

"firewall address",SUCCESS,"(name=LOCAL_SUBNET, oid=684, new object)"

"firewall service custom",SUCCESS,"(name=ALL, oid=863, update previous
object)"

"firewall policy",SUCCESS,"(name=1, oid = 1090, new object)"
```

Which statement about the object named ALL is true?

- A. FortiManager updated the object ALL using the FortiGate value in its database.
- B. FortiManager installed the object ALL with the updated value.
- C. FortiManager created the object ALL as a unique entity in its database, which can be only used by this managed FortiGate.
- D. FortiManager updated the object ALL using the FortiManager value in its database.

Answer: A

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

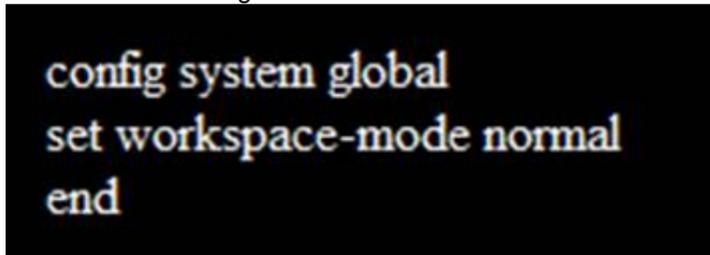
Explanation:

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

NEW QUESTION 6

- (Topic 1)

Refer to the following exhibit:



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

- A. The same administrator can lock more than one ADOM at the same time
- B. Ungraceful closed sessions will keep the ADOM in a locked state until the administrator session times out
- C. Unlocking an ADOM will submit configuration changes automatically to the approval administrator
- D. Unlocking an ADOM will install configuration automatically on managed devices

Answer: AB

Explanation:

Reference: http://help.fortinet.com/fmgr/cli/5-6-2/Document/0800_ADOMs/200_Configuring+.htm

NEW QUESTION 7

- (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 common policy 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 8

- (Topic 1)

An administrator run the reload failure command: diagnose test deploymanager reload config <deviceid> on FortiManager. What does this command do?

- A. It downloads the latest configuration from the specified FortiGate and performs a reload operation on the device database.
- B. It installs the latest configuration on the specified FortiGate and update the revision history database.
- C. It compares and provides differences in configuration on FortiManager with the current running configuration of the specified FortiGate.
- D. It installs the provisioning template configuration on the specified FortiGate.

Answer: A

Explanation:

Reference: <https://community.fortinet.com/t5/FortiManager/Technical-Note-Retrieve-configuration-file-using-CLI-from-a/ta-p/191000?externalID=FD36387>

NEW QUESTION 9

- (Topic 1)

View the following exhibit:

Create New CLI Script

[\[View Sample Script\]](#)

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

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 the Remote FortiGate Directly (via CLI) option? (Choose two.)

- A. You must install these changes using Install 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 10

- (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 server fds1.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 10

- (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 12

- (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 15

- (Topic 1)

Which two conditions trigger FortiManager to create a new revision history? (Choose two.)

- A. When configuration revision is reverted to previous revision in the revision history
- B. When FortiManager installs device-level changes to a managed device
- C. When FortiManager is auto-updated with configuration changes made directly on a managed device
- D. When changes to device-level database is made on FortiManager

Answer: BC

Explanation:

Reference: https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FortiManager_Admin_Guide/1000_Device%20Manager/1500_Manage_device_configs/600_Manage%20config%20rev%20history.htm

NEW QUESTION 18

- (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
fmfg/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-level database

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 21

- (Topic 2)

Refer to the exhibit.

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

Given the configuration shown in the exhibit, which two statements are true? (Choose two.)

- A. It allows two or more administrators to make configuration changes at the same time, in the same ADOM.
- B. It disables concurrent read-write access to an ADOM.
- C. It allows the same administrator to lock more than one ADOM at the same time.
- D. It is used to validate administrator login attempts through external servers.

Answer: BC

Explanation:

Reference: <https://docs.fortinet.com/document/fortimanager/6.0.4/administration-guide/86456/concurrentadom-access>

NEW QUESTION 23

- (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 27

- (Topic 2)

Refer to the exhibit.

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 30

- (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

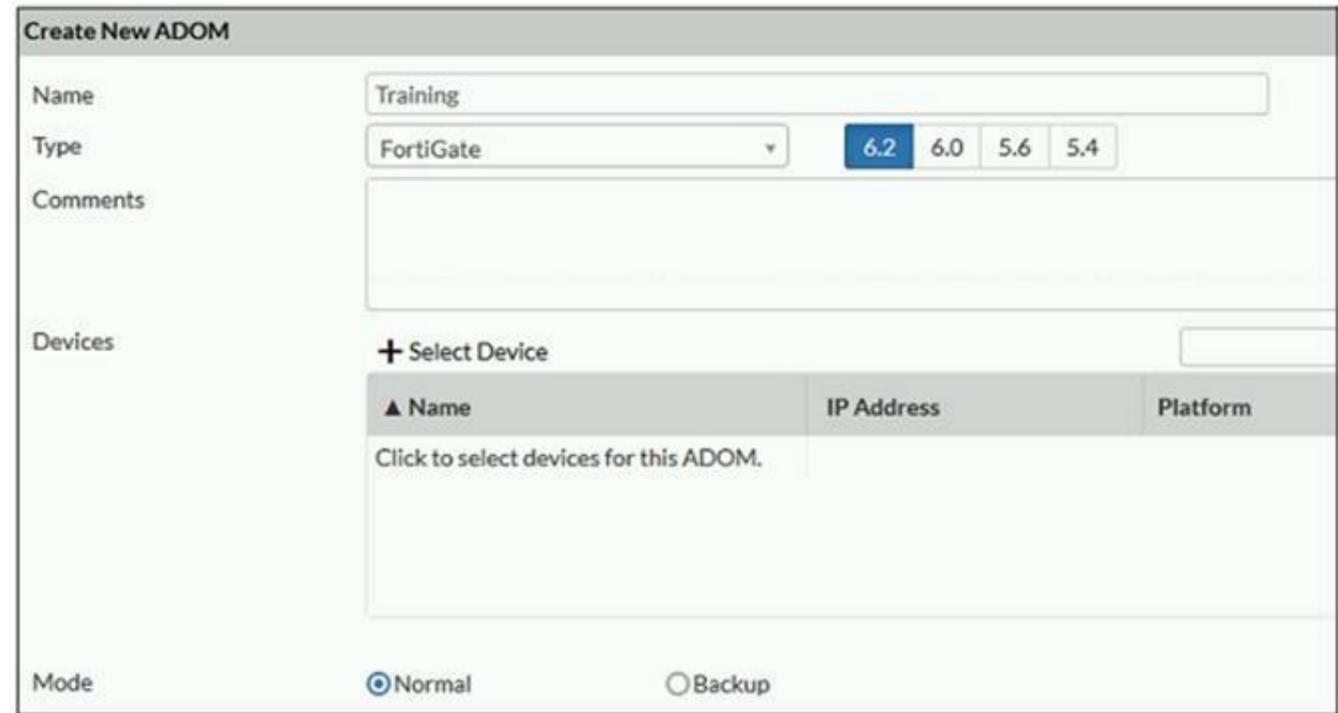
Explanation:

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

NEW QUESTION 32

- (Topic 2)

Refer to the exhibit.



Which two statements about an ADOM set in Normal mode 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 33

- (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 38

- (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 device independently.
- D. The policy configuration has never been imported after a device was registered on FortiManager.

Answer: C

NEW QUESTION 42

- (Topic 2)

An administrator'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?

- A. Restore the configuration from a previous backup.
- B. Log in as Super_User in order to unlock the ADOM.
- C. Log in using the same administrator account to unlock the ADOM.
- D. Delete the previous admin session manually through the FortiManager GUI or CLI.

Answer: D

NEW QUESTION 43

- (Topic 2)

What is the purpose of ADOM revisions?

- A. To create System Checkpoints for the FortiManager configuration.
- B. To save the current state of the whole ADOM.
- C. To save the current state of all policy packages and objects for an ADOM.
- D. To revert individual policy packages and device-level settings for a managed FortiGate by reverting to a specific ADOM revision

Answer: C

Explanation:

Fortimanager 6.4 Study guide page 198

NEW QUESTION 46

- (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 50

- (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?

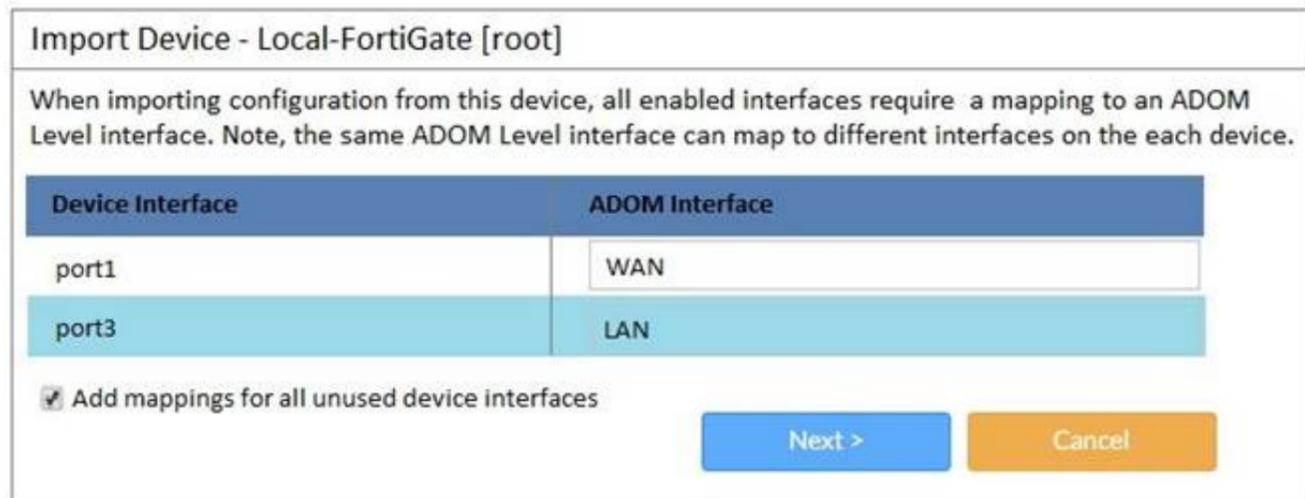
- A. You need to assign the global policy package from the global ADOM
- B. You need to reapply the global poky package to the ADOM
- C. it automatically assigns the global policies
- D. You can select the option to assign the global polices

Answer: C

NEW QUESTION 53

- (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 55

- (Topic 3)

An administrator has added all the devices in a Security Fabric group to FortiManager. How does the administrator identify the root FortiGate?

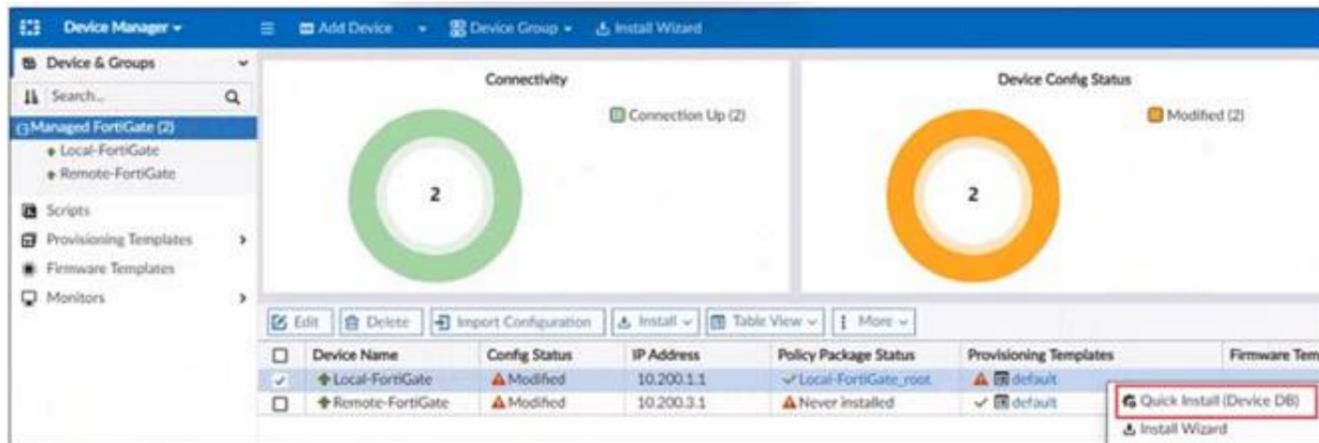
- A. By a dollar symbol (\$) at the end of the device name
- B. By an at symbol (@) at the end of the device name
- C. By a QUESTION NO: mark(?) at the end of the device name
- D. By an Asterisk (*) at the end of the device name

Answer: D

NEW QUESTION 60

- (Topic 3)

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 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 FortiGate 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 64

- (Topic 3)

Which two settings are required for FortiManager Management Extension Applications (MEA)? (Choose two.)

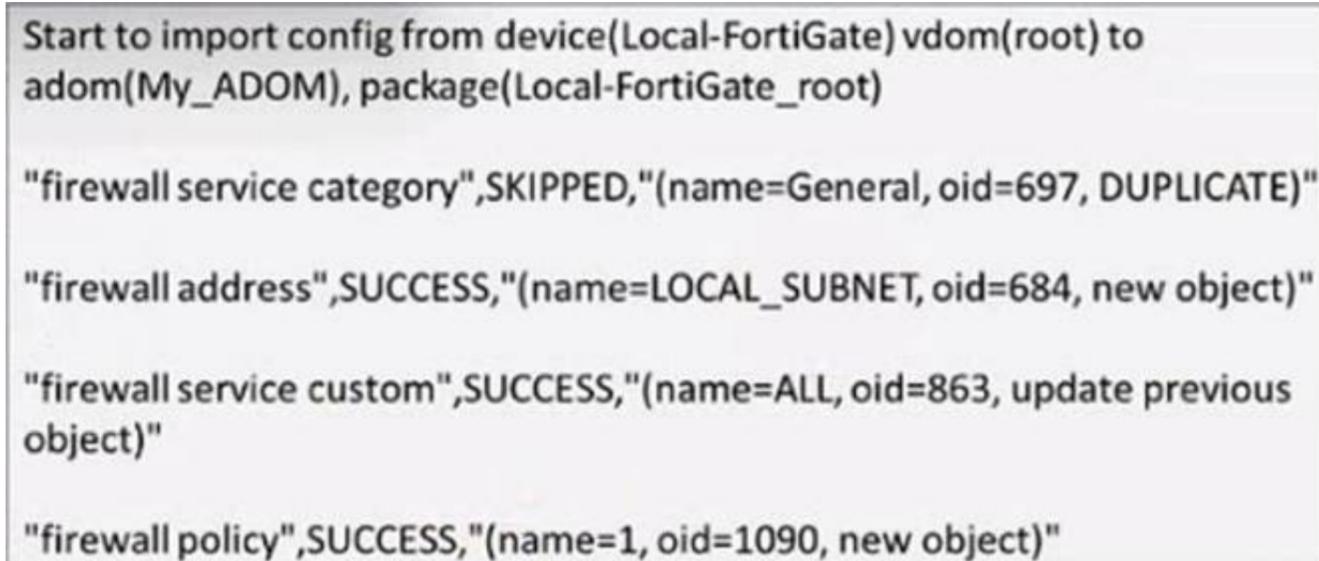
- A. When you configure MEA, you must open TCP or UDP port 540.
- B. You must open the ports to the Fortinet registry
- C. You must create a MEA special policy on FortiManager using the super user profile
- D. The administrator must have the super user profile.

Answer: CD

NEW QUESTION 67

- (Topic 3)

Refer to the exhibit.



Given the configuration shown in the exhibit, how did FortiManager handle the service category named General?

- A. FortiManager ignored the firewall service category General but created a new service category in its database.
- B. FortiManager ignored the firewall service category general and deleted the duplicate value in its database
- C. FortiManager ignored the firewall service category General and updated the FortiGate duplicate value in the FortiGate database.
- D. FortiManager ignored the firewall service category General and did not update its database with the value

Answer: C

NEW QUESTION 68

- (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 71

- (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 72

- (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 77

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

NSE5_FMG-7.0 Practice Exam Features:

- * NSE5_FMG-7.0 Questions and Answers Updated Frequently
- * NSE5_FMG-7.0 Practice Questions Verified by Expert Senior Certified Staff
- * NSE5_FMG-7.0 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * NSE5_FMG-7.0 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE5_FMG-7.0 Practice Test Here](#)