Fortinet

Exam Questions NSE5_FMG-7.2

Fortinet NSE 5 - FortiManager 7.2

NEW QUESTION 1
- (Topic 1)
When an installation is performed from FortiManager, what is the recovery logic used between FortiManager and FortiGate for an FGFM tunnel?

A. After 15 minutes, FortiGate will unset all CLI commands that were part of the installation that caused the tunnel to go down.
B. FortiManager will revert and install a previous configuration revision on the managed FortiGate.
C. FortiGate will reject the CLI commands that will cause the tunnel to go down.
D. FortiManager will not push the CLI commands as a part of the installation that will cause the tunnel to go down.

Answer: A

Explanation:
The configuration change will break the fgfm connection, causing the FortiGate unit to attempt to reconnect for 900 seconds. If the FortiGate cannot reconnect, it will rollback to its previous configuration.

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)
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
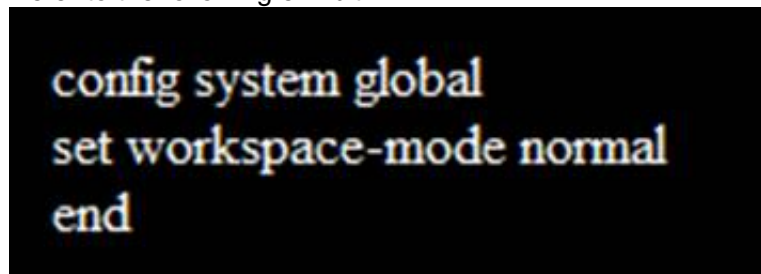D. When changes to device-level database is made on FortiManager

Answer: BC

Explanation:
Reference:https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FortiManager_Admin_Guide/1000_Device%20Manager/1500_Manage_device_configs/0600_Manage%20config%20rev%20history.htm

NEW QUESTION 5
- (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_AD0Ms/200_Configuring+.htm

NEW QUESTION 6
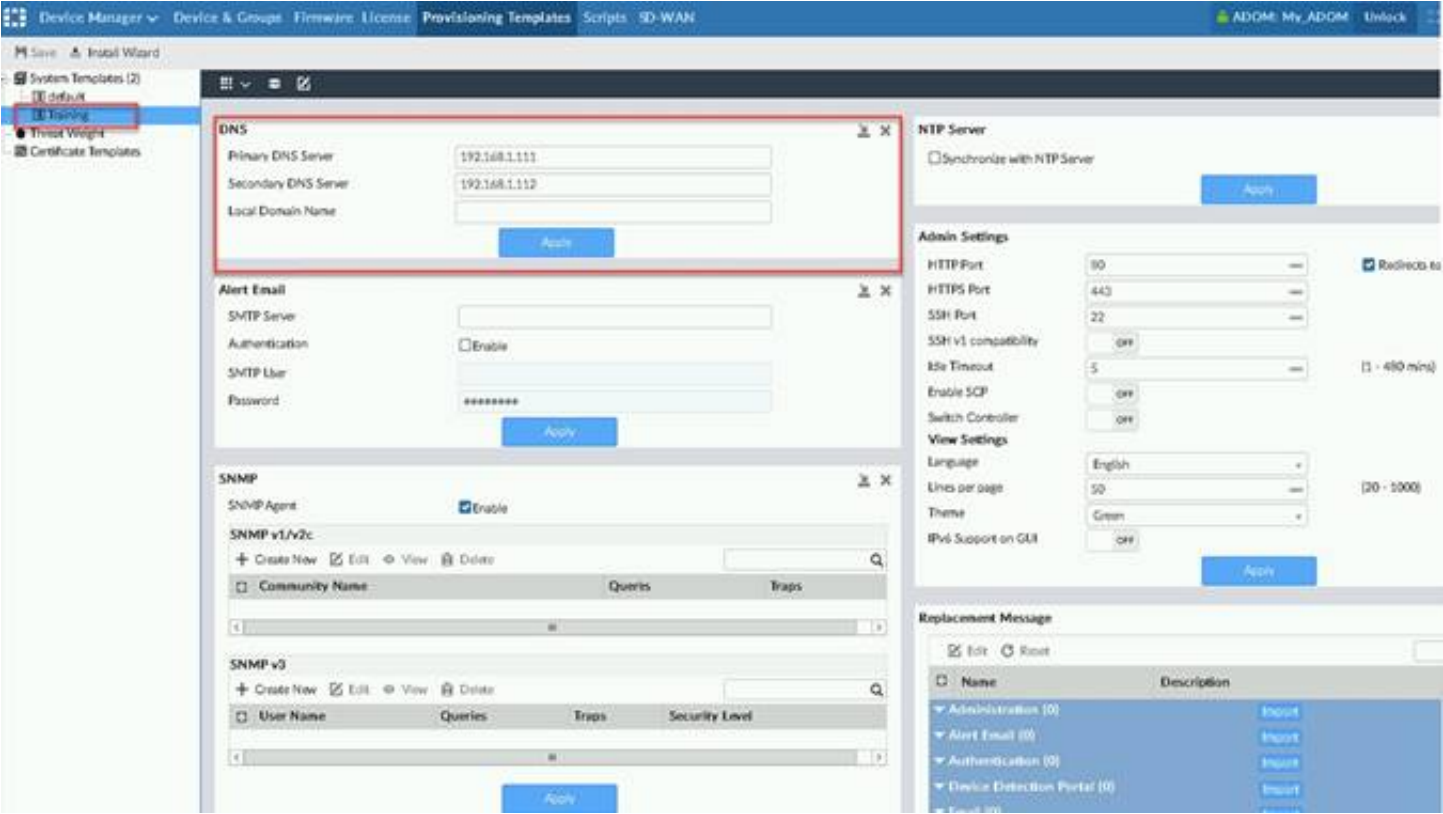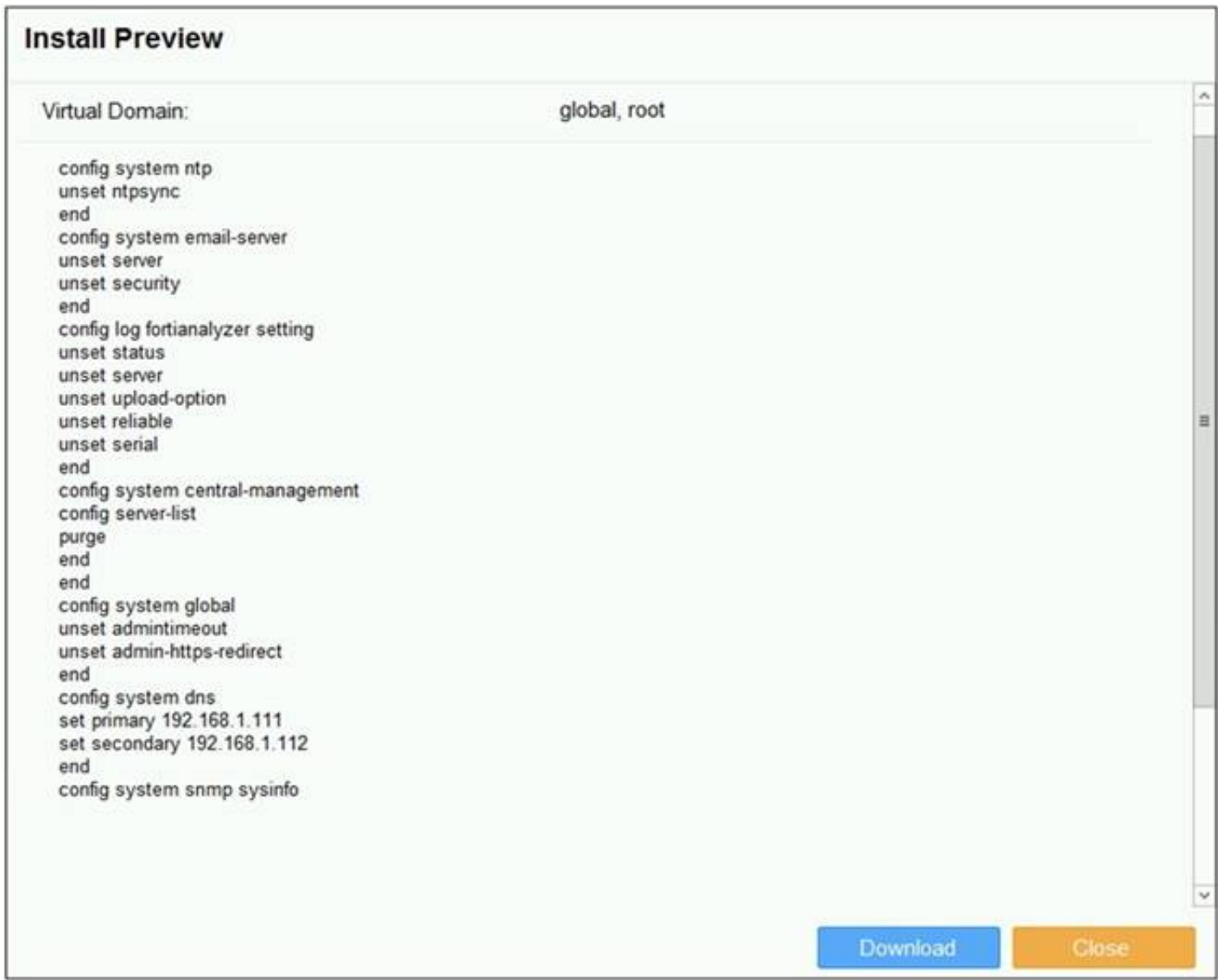- (Topic 1)
Refer to the exhibits. Exhibit one.

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)
Which three settings are the factory default settings on FortiManager? (Choose three.)
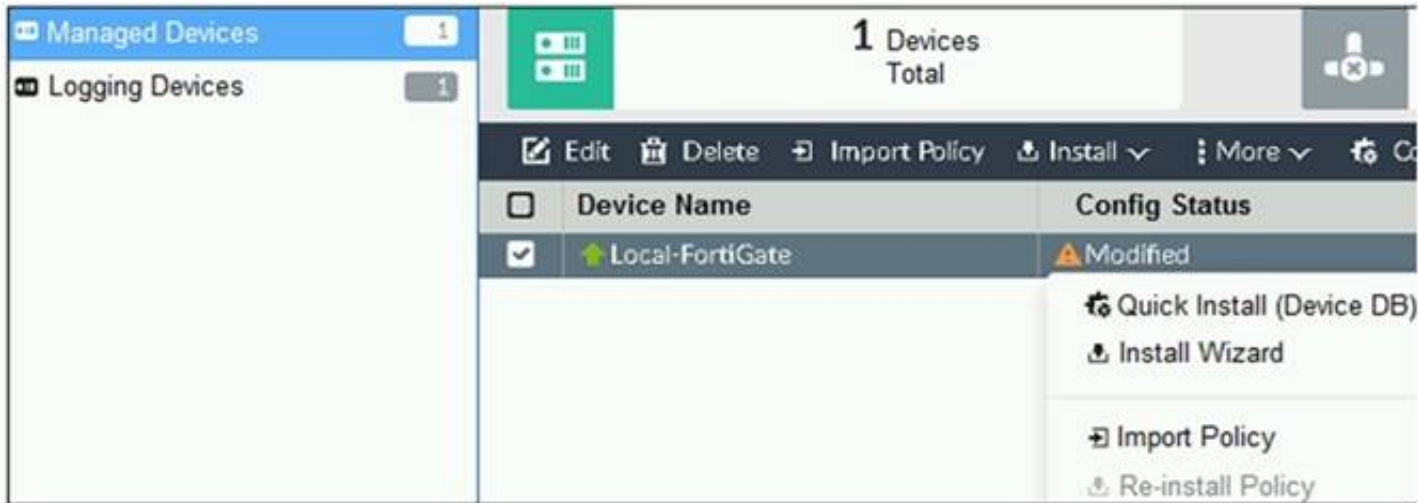
A. Username is admin

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 8
- (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 9
- (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 10
- (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 thismanaged FortiGate.
D. FortiManager updated the object ALL using the FortiManager value in its database.

Answer: A

NEW QUESTION 10

- (Topic 1)

An administrator, Trainer, who is assigned theSuper_Userprofile, is trying to approve a workflow session that was submitted by another administrator, Student. However, Trainer is unable to approve the workflow session.

What can prevent an admin account that hasSuper_Userrights over the device from approving a workflow session?

Session List

	ID	Name	User	Date Submitt...	Approved/To...	Comments
☑	1	Firewall p..	Student	2017-06-01...	0/1	firewall policies

View Diff

+ Add Comment

[Student] - 2017-06-01
13:31:35
firewall policies
[Student] - 2017-06-01
16:29:27

A. Trainer is not a part of workflow approval group
B. Trainer does not have full rights over this ADOM
C. Trainer must close Student's workflow session before approving the request
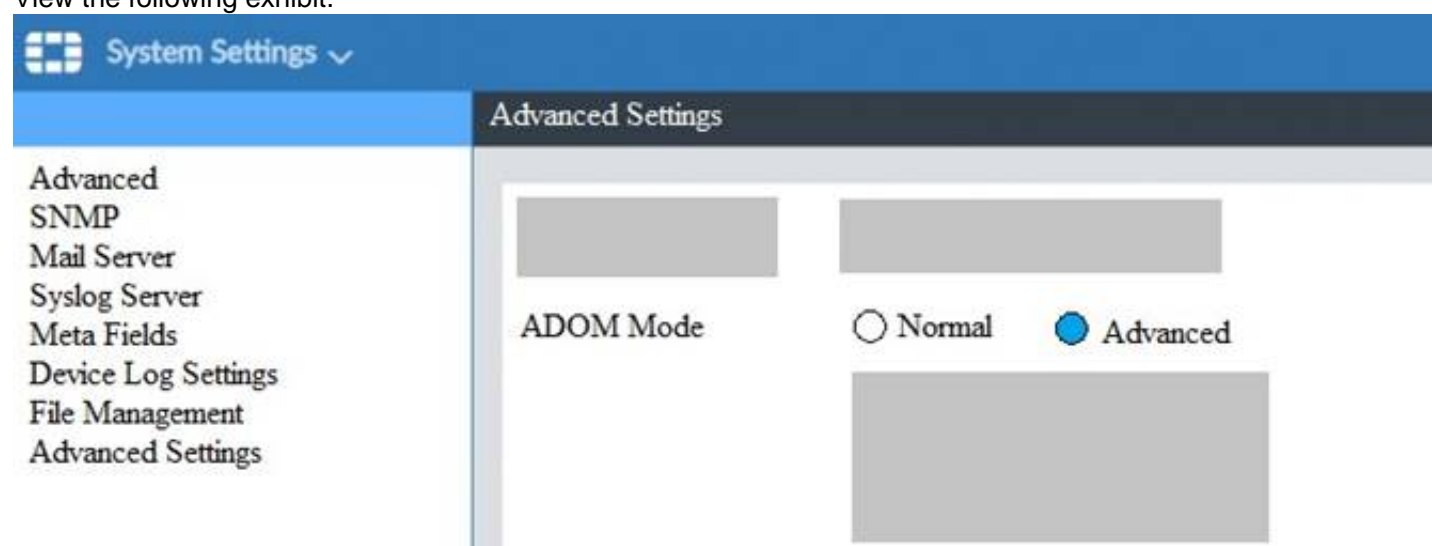D. Student, who submitted the workflow session, must first self-approve the request

Answer: A

Explanation:
Reference:https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMG-FAZ/0800_ADOMs/1800_Workflow/0600_Workflow%20sessions.htm

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

System Settings ⌄

Advanced Settings

Advanced
SNMP
Mail Server
Syslog Server
Meta Fields
Device Log Settings
File Management
Advanced Settings

ADOM Mode   ○ Normal   ● Advanced

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 13
- (Topic 1)
In addition to the default ADOMs, an administrator has created a new ADOM namedTrainingfor FortiGate devices. The administrator sent a device registration to FortiManager from a remote FortiGate. Which one of the following statements is true?

A. The FortiGate will be added automatically to the default ADOM named FortiGate.
B. The FortiGate will be automatically added to the Training ADOM.
C. By default, the unregistered FortiGate will appear in the root ADOM.
D. The FortiManager administrator must add the unregistered device manually to the unregistered devicemanually to the Training ADOM using the Add Device wizard

Answer: C

Explanation:
Reference:https://docs.fortinet.com/document/fortimanager/7.0.0/administration- guide/718923/root-adom

NEW QUESTION 15
- (Topic 1)
An administrator wants to delete an address object that is currently referenced in a firewall policy.
What can the administrator expect to happen?

A. FortiManager will not allow the administrator to delete a referenced address object
B. FortiManager will disable the status of the referenced firewall policy
C. FortiManager will replace the deleted address object with thenoneaddress object in the referencedfirewall policy
D. FortiManager will replace the deleted address object withalladdress object in the referenced firewall policy

Answer: C

Explanation:
Reference:https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FortiManager_Admin_Guide/1200_Policy%20and%20Objects/1200_Managing%20object
s/0800_Remove%20an%20object.htm

NEW QUESTION 17
- (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 20
- (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 22
- (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 23
- (Topic 2)
An administrator has enabledService Accesson FortiManager.
What is the purpose ofService Accesson 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 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 30
- (Topic 2)
Refer to the exhibit.

Which two statements are true if the script is executed using theDevice Databaseoption? (Choose two.)

A. You must install these changes using theInstall Wizardto a managed device
B. The successful execution of a script on theDevice Databasewill create a new revision history
C. The script history will show successful installation of the script on the remote FortiGate
D. TheDevice Settings Statuswill be tagged asModified

Answer: AD

NEW QUESTION 33
- (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 35
- (Topic 3)
What will happen if FortiAnalyzer features are enabled on FortiManager?

A. FortiManager will keep all the logs and reports on the FortiManager.
B. FortiManager will enable ADOMs to collect logs automatically from non-FortiGate devices.
C. FortiManager will install the logging configuration to the managed devices
D. FortiManager can be used only as a logging device.

Answer: C

NEW QUESTION 38
- (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 43
- (Topic 3)
View the following exhibit.
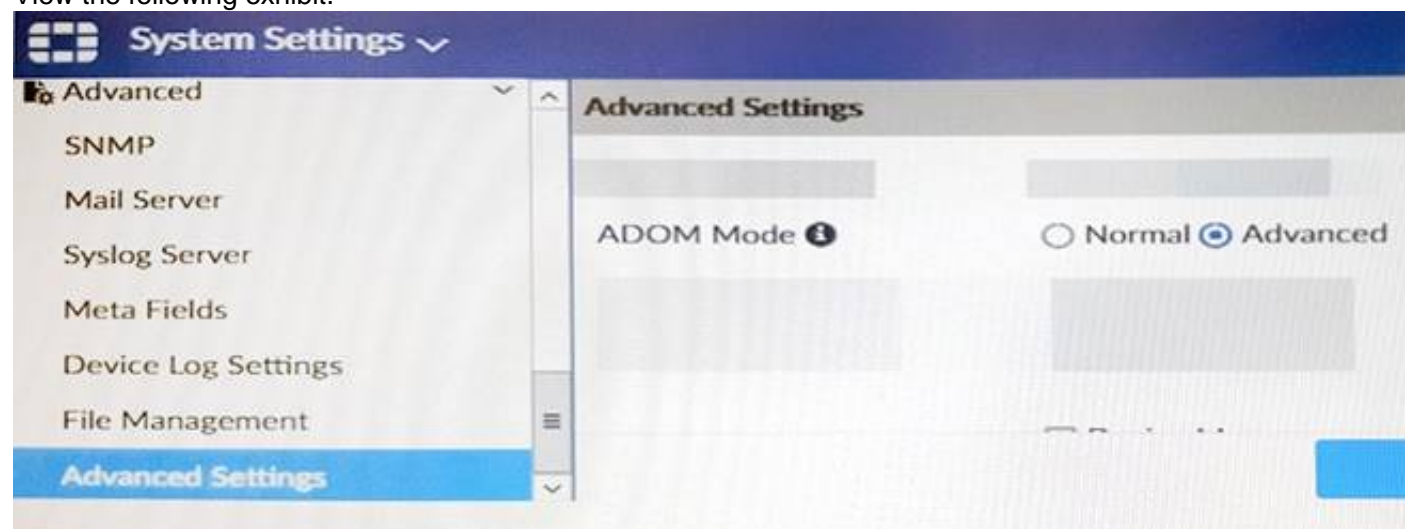
Which of the following statements are true based on this configuration setting? (Choose two.)

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 48
- (Topic 3)
In the event that one of the secondary FortiManager devices fails, which action must be performed to return the FortiManager HA manual mode to a working state?

A. The FortiManaqer HA state transition is transparent to administrators and does notrequire any reconfiguration.
B. Manually promote one of the working secondary devices to the primary role, and reboot the old primary device to remove the peer IP of the failed device.
C. Reconfigure the primary device to remove the peer IP of the failed device.
D. Reboot the failed device to remove its IP from the primary device.

Answer: C

NEW QUESTION 50
- (Topic 3)
What is the advantage of using FortiManager to manage PortiAnalyzer?

A. It allows FortiManager to manage all FortiGate devices
B. It allows FortiManager to fun reports based on FortiAnalyzer
C. It allows FortiManager to store all managed FortiGate device logs
D. It allows FortiManager to act as a collector and FortiAnalyzer device

Answer: D

NEW QUESTION 55
- (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 59
- (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 61
- (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 63
- (Topic 3)
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)"

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: D

NEW QUESTION 65
- (Topic 3)
What does thediagnose dvm check-integritycommand do? (Choose two.)

A. Internally upgrades existing ADOMs to the same ADON version in order to clean up and correct the ADOMsyntax
B. Verifies and corrects unregistered, registered, and deleted device states
C. Verifies and corrects database schemas in all object tables
D. Verifies and corrects duplicate VDOM entries

Answer: BD

Explanation:
* 6.2 Study Guide page 305verify and correct parts of the device manager databases, including:– inconsistent device-to-group and group-to-ADOM memberships– unregistered, registered, and deleted device states– device lock statuses– duplicate VDOM entries

NEW QUESTION 67
- (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 71
- (Topic 3)
Refer to the exhibit.

```
FortiManager # diagnose fmupdate view-serverlist fds
Fortiguard Server Comm : Enabled
Server Override Mode    : Strict
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
 ...
 9      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 or public FDN servers
B. From the default server fds1.fortinet.com
C. From the configured override server IP address 10.0.1.50 only
D. From public FDNI server IP address with the fourth highest octet only

Answer: A

NEW QUESTION 72
......

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

NSE5_FMG-7.2 Practice Exam Features:

* NSE5_FMG-7.2 Questions and Answers Updated Frequently

* NSE5_FMG-7.2 Practice Questions Verified by Expert Senior Certified Staff

* NSE5_FMG-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE5_FMG-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE5_FMG-7.2 Practice Test Here](https://www.surepassexam.com/NSE5_FMG-7.2-exam-dumps.html)