Website: www.VCEplus.io

Twitter: https://twitter.com/VCE_Plus

Exam Code: NSE5_FMG-7.2

Exam Name: Fortinet NSE 5 - FortiManager 7.2

Exam A

QUESTION 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-WAN template settings

D. Remove all the interface references such as routes or policies that will be a part of SD-WAN member interfaces

Correct Answer: B, D
Section:

QUESTION 2
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.

Correct Answer: B, C
Section:

QUESTION 3
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-level database

Correct Answer: A, C
Section:
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
Topic 2, Main Questions Pool B

QUESTION 4
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 fdsl.fortinet.com
D. From public FDNI server with highest index number only

Correct Answer: A
Section:

QUESTION 5
View the following exhibit.

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

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

Correct Answer: B
Section:

QUESTION 6
View the following exhibit.

Import Device - Local-FortiGate [root]

Create a new policy package for import.

Policy Package Name   Local-FortiGate

Folder   root

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 the FortiManager database

Correct Answer: C
Section:

QUESTION 7
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.

Correct Answer: A
Section:
Explanation:
FortiManager_6.4_Study_Guide-Online -- page 331 & 332

QUESTION 8
Refer to the exhibit.

Create New CLI Script

Script Name	Routing	[View Sample Script]
Comments	Write a comment	0/255
Type	CLI Script	
Run script on	Device Database	

Script details
```
config router prefix-list
edit public
config rule
edit 1
set prefix 0.0.0.0/0
set action permit
next
edit 2
set prefix 8.8.8.8/32
set action deny
end
```

Advanced Device Filters >

OK   Cancel

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

Correct Answer: A, D
Section:

QUESTION 9
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.

Correct Answer: A, C
Section:

QUESTION 10
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 Fabric integration

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

Correct Answer: C, D
Section:

QUESTION 11
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

Correct Answer: B
Section:

QUESTION 12
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.

Correct Answer: A
Section:

QUESTION 13
View the following exhibit.
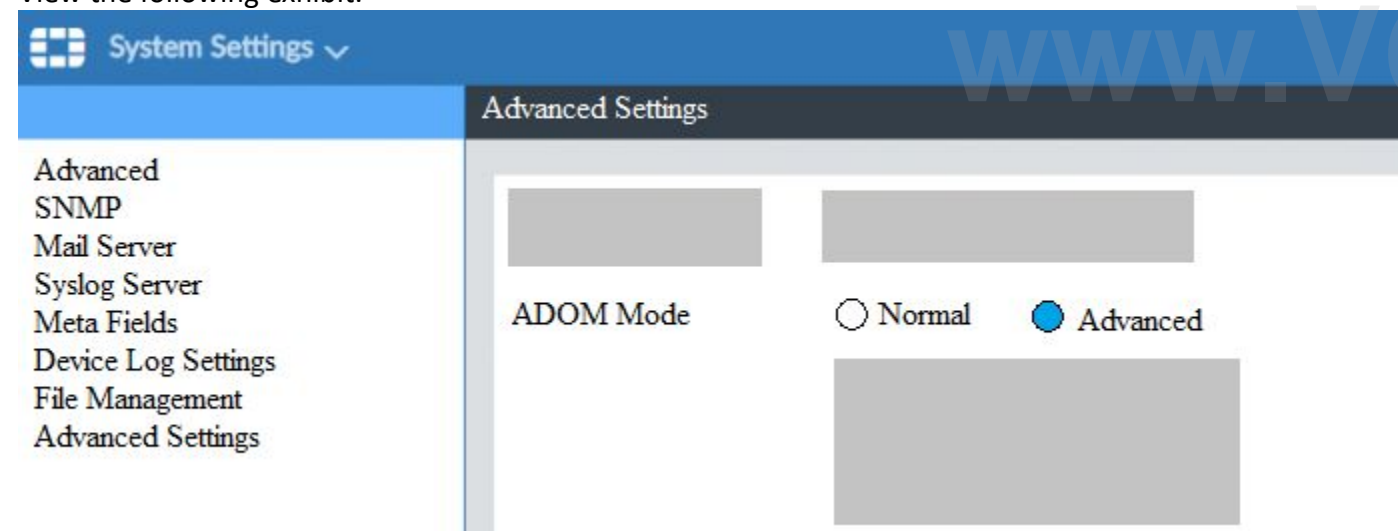
What is the purpose of setting ADOM Mode to Advanced?

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

Correct Answer: C
Section:

QUESTION 14
An administrator, Trainer, who is assigned the Super_User profile, 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 has Super_User rights over the device from approving a workflow session?

Session List

View Diff

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

+ Add Comment

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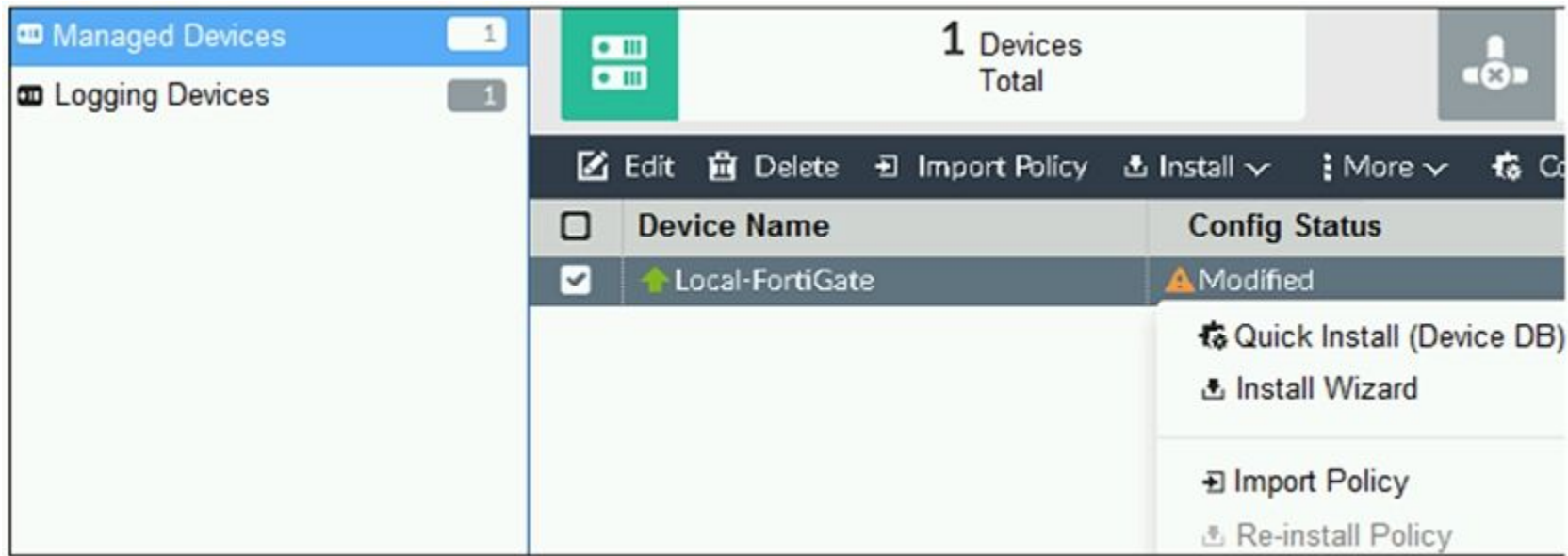13:31:35
firewall policies
[Student] - 2017-06-01
16:29:27

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

Correct Answer: A
Section:

QUESTION 15
Refer to the exhibit.

| Managed Devices | 1 |
| Logging Devices | 1 |

1 Devices
Total

☑ Edit 🗑 Delete ➦ Import Policy ⬇ Install ∨ ⋮ More ∨ 🔧 C

☐	Device Name	Config Status
☑	⬆ Local-FortiGate	⚠ Modified

🔧 Quick Install (Device DB)
⬇ Install Wizard

➦ Import Policy
⬇ Re-install Policy

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

A. It will not create a new revision in the revision history

B. It installs device-level changes to FortiGate without launching the Install Wizard

C. It cannot be canceled once initiated and changes will be installed on the managed device

D. It provides the option to preview configuration changes prior to installing them

Correct Answer: B, C
Section:
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.

QUESTION 16
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 panes do not appear? (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 the Super_User profile.
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.

Correct Answer: B, D
Section:

QUESTION 17
Which two items are included in the FortiManager backup? (Choose two.)

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

Correct Answer: B, D
Section:

QUESTION 18
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.

Correct Answer: D
Section:

QUESTION 19
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.

Correct Answer: B, C
Section:

QUESTION 20
Refer to the exhibit.

Create New ADOM

Name	Training
Type	FortiGate ▾ 6.2 6.0 5.6 5.4
Comments	

Devices

+ Select Device

▲ Name	IP Address	Platform
Click to select devices for this ADOM.		

Mode   ⦿ Normal   ◯ Backup

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

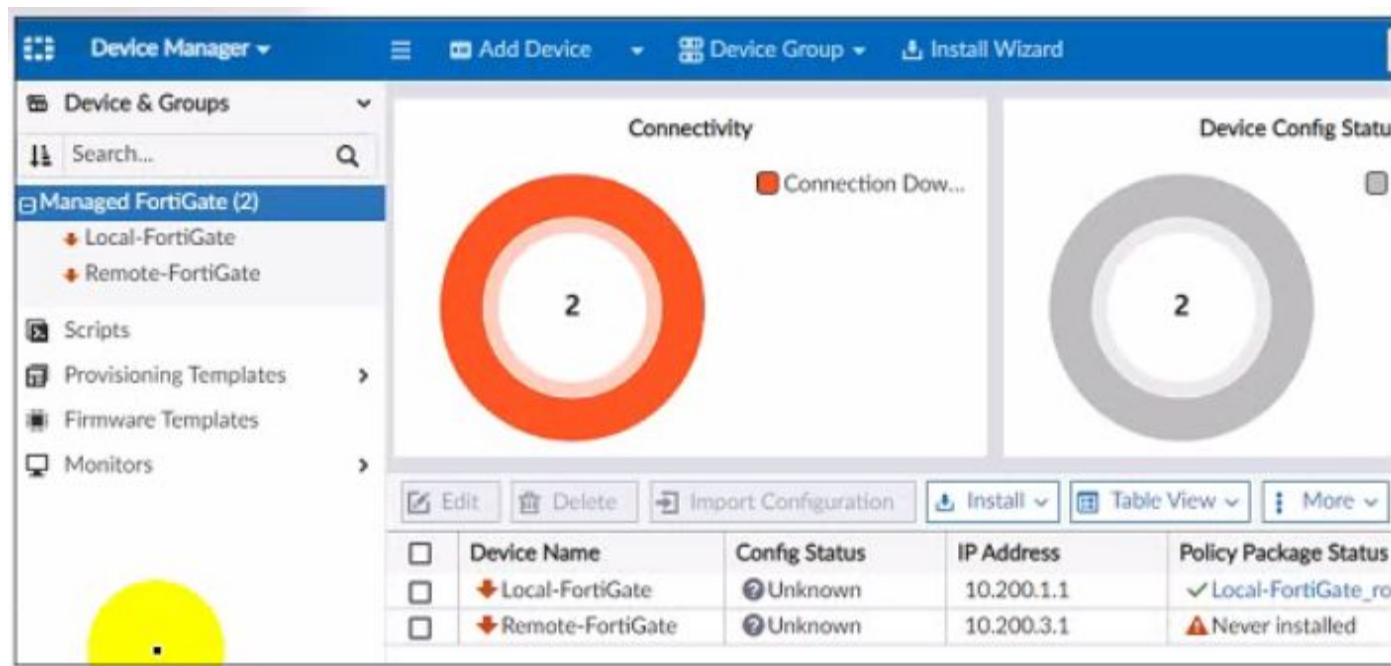**Correct Answer: A, B**
Section:
Explanation:
'FortiGate units in the ADOM will query their own configuration every 5 seconds. If there has been a configuration change, the FortiGate unit will send a diff revision on the change to the FortiManager using the FGFM protocol.'

QUESTION 21
Refer to the exhibit.

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

Correct Answer: C
Section:

QUESTION 22
View the following 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 one of the following statements is true regarding the object named ALL?

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

Correct Answer: A
Section:

QUESTION 23
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

Correct Answer: D
Section:

QUESTION 24
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

Correct Answer: C
Section:
Explanation:
Fortimanager 6.4 Study guide page 198

QUESTION 25
An administrator has assigned a global policy package to custom ADOM1. Then the administrator creates a new policy package, Fortinet, in the custom ADOM1.
Which statement about the global policy package assignment to the newly-created policy package Fortinet is true?

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

Correct Answer: A
Section:
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).

QUESTION 26
What will be the result of reverting to a previous revision version in the revision history?

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

Correct Answer: D

Section:

QUESTION 27
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

Correct Answer: C
Section:

QUESTION 28
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 hidden from 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.

Correct Answer: A, D
Section:

QUESTION 29
An administrator is replacing a failed device on FortiManager by running the following command:
execute device replace sn <devname> <serialnum>.
Which device name and serial number must the administrator use?

A. The device name of the new device and serial number of the failed device

B. The device name and serial number of the failed device

C. The device name of the failed device and serial number of the new device

D. The device name and serial number of the new device

Correct Answer: C
Section:

QUESTION 30
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

Correct Answer: A
Section:

QUESTION 31
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
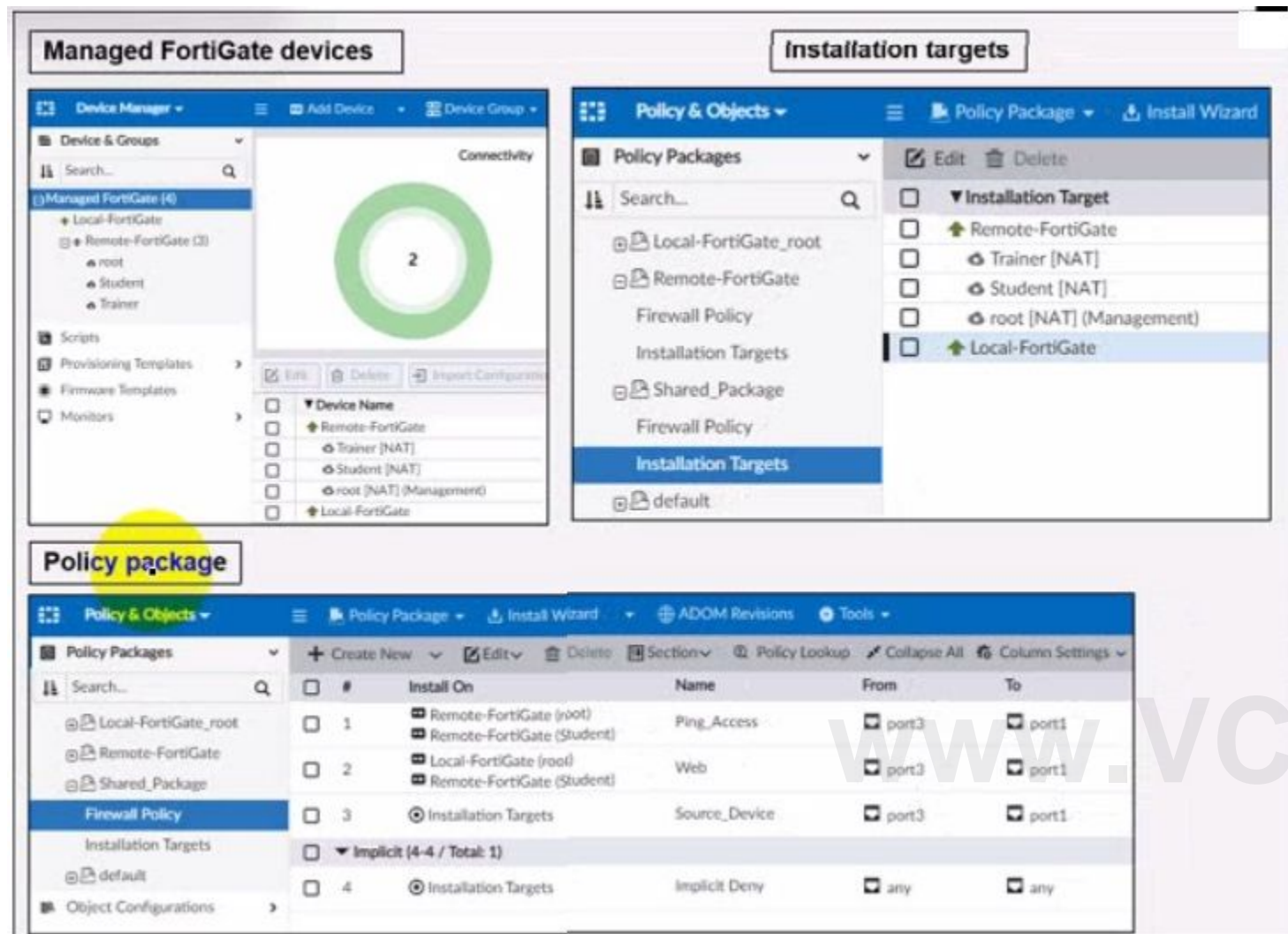What is the expected result?

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

Correct Answer: C

QUESTION 32
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

Correct Answer: B, C
Section:

QUESTION 33
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.

Correct Answer: D
Section:

QUESTION 34
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.

Correct Answer: B
Section: