

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 review, approve, or reject all the firewall policy changes made by the junior administrators.

How should the Workspace mode be configured on FortiManager?

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

Answer: A

Explanation:

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

NEW QUESTION 3

- (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 4

- (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 5

- (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 6

- (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 runningconfiguration 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 7

- (Topic 1)

Refer to the exhibits. Exhibit one.

Exhibit two.

```

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

```

An administrator created a new system template 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 8

- (Topic 1)

Which two settings must be configured for SD-WAN Central Management? (Choose two.)

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

Answer: AC

NEW QUESTION 9

- (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 10

- (Topic 1)

What is the purpose of thePolicy Checkfeature on FortiManager?

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

Answer: C

Explanation:

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

NEW QUESTION 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 serverfdsl.fortinet.com
- D. From public FDN 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 15

- (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 18

- (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 23

- (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 28

- (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)"
```

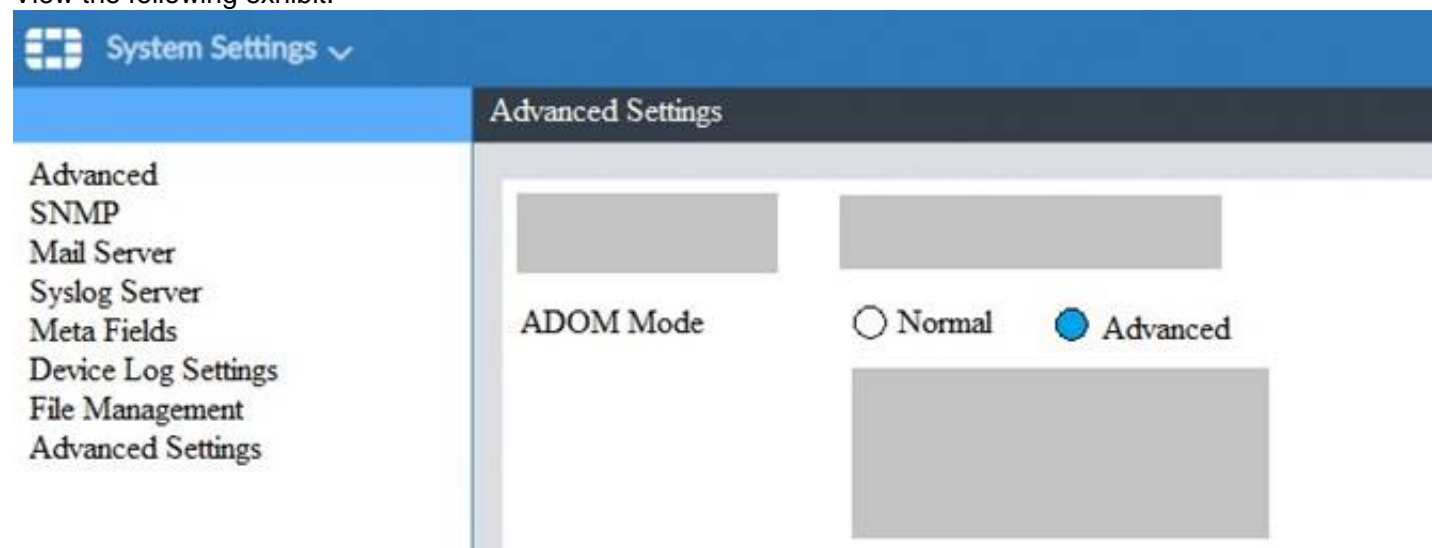
Which statement about the object named ALL is true?

- 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 33

- (Topic 1)
 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

Answer: C

Explanation:

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

NEW QUESTION 38

- (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 the none address object in the referenced firewall policy
- D. FortiManager will replace the deleted address object with the all address 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%20objects/0800_Remove%20an%20object.htm

NEW QUESTION 40

- (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 45

- (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 46

- (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 49

- (Topic 2)

What is the purpose of ADOM revisions?

- A. To createSystem Checkpointsfor 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 54

- (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 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 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 56

- (Topic 2)

Which two statements about Security Fabric integration with FortiManager are true? (Choose two.)

- A. The Security Fabric license, group name and password are required for the FortiManager Security Fabric integration
- B. TheFabric Viewmodule 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. TheFabric Viewmodule enables you to view the Security Fabric ratings for Security Fabric devices

Answer: CD

NEW QUESTION 59

- (Topic 2)

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

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

Answer: BD

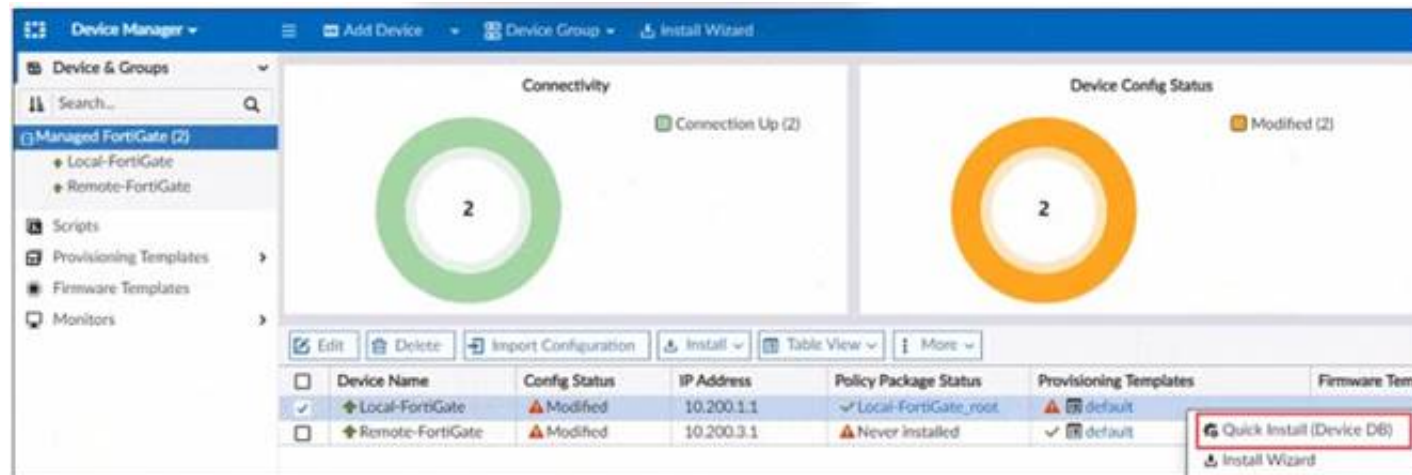
Explanation:

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

NEW QUESTION 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)

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: A

NEW QUESTION 65

- (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 the FortiManager NATed IP address on FortiGate
- B. During discovery FortiManager sets both the 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 70

- (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?

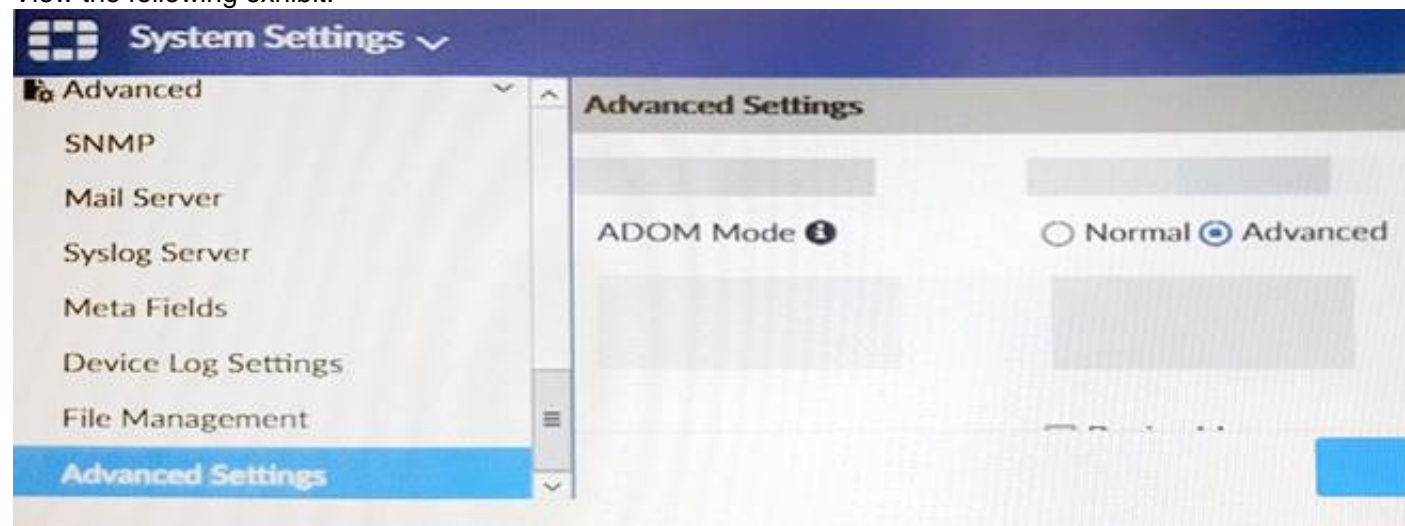
- A. First create an SD-WAN firewall policy, add member interfaces to the SD-WAN template and create a static route
- B. You must specify a gateway address when you create a default static route
- C. Remove all the interface references such as routes or policies
- D. Enable SD-WAN central management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

Answer: D

NEW QUESTION 73

- (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 74

- (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?

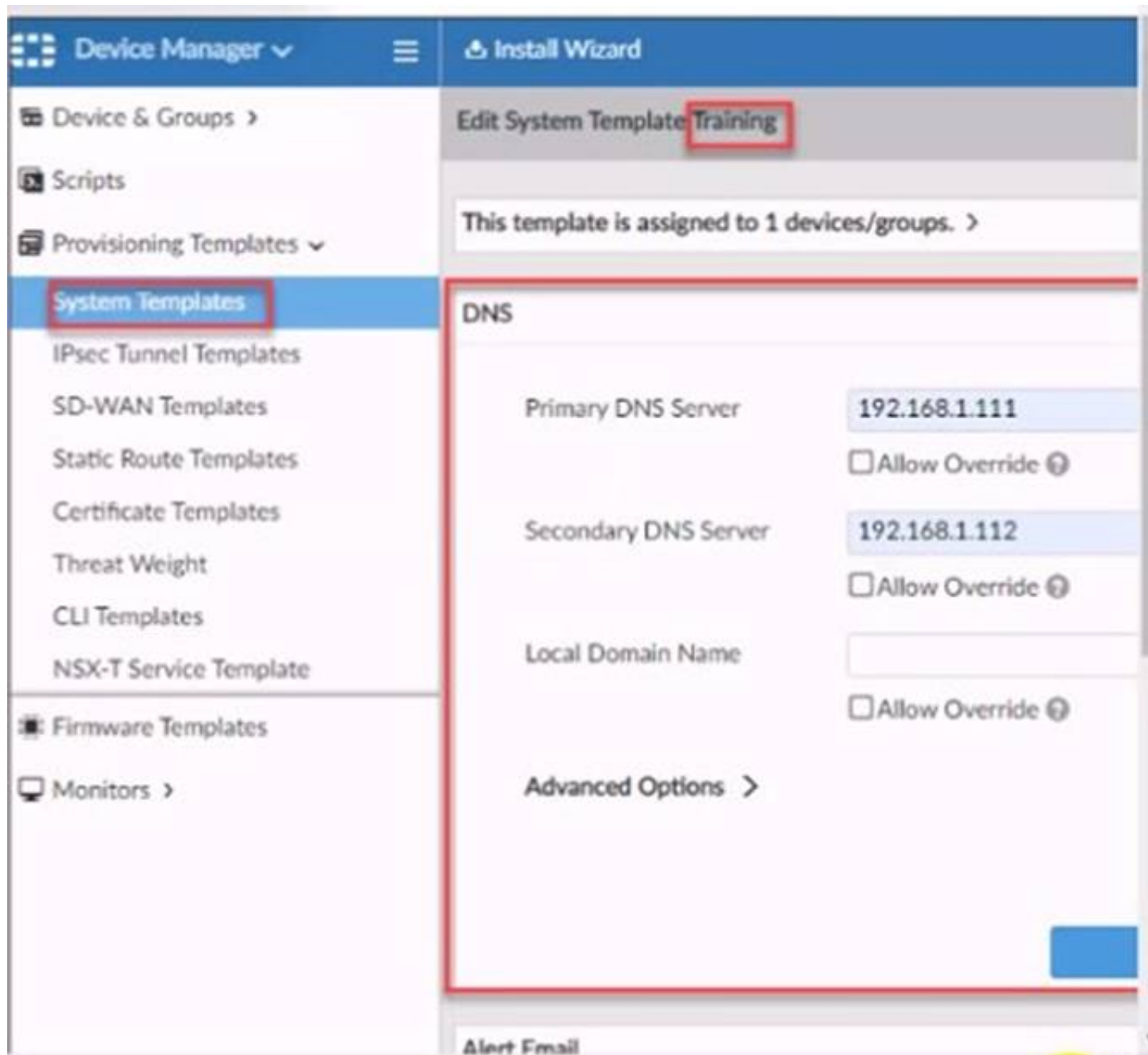
- A. You need to assign the global policy package from the global ADOM
- B. You need to reapply the global policy package to the ADOM
- C. it automatically assigns the global policies
- D. You can select the option to assign the global policies

Answer: C

NEW QUESTION 75

- (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 77

- (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. FortiAnalyzer features are disabled.

Answer: ABE

NEW QUESTION 81

- (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 versionID and remove all other history versions.
- 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 83

- (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 84

- (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 87

- (Topic 3)

What does the diagnose dvm check-integrity command do? (Choose two.)

- A. Internally upgrades existing ADOMs to the same ADON version in order to clean up and correct the ADOM syntax
- 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 305 verify 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 90

- (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 94

- (Topic 3)

Which of the following statements are true regarding VPN Gateway configuration in VPN Manager? (Choose two.)

- A. Managed gateways are devices managed by FortiManager in the same ADOM
- B. External gateways are third-party VPN gateway devices only
- C. Protected subnets are the subnets behind the device that you don't want to allow access to over the 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 96

- (Topic 3)

An administrator would like to create an SD-WAN default static route for a newly created SD-WAN using the FortiManager GUI. Both port1 and port2 are part of the SD-WAN member interfaces.

Which interface must the administrator select in the static route device drop-down list?

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

Answer: B

NEW QUESTION 99

.....

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-7.2 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 First Try
- * NSE5_FMG-7.2 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE5_FMG-7.2 Practice Test Here](#)