NSE5_FMG-7.0 (70 Questions)

Number: 000-000
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

Vendor: Fortinet

Exam Code: NSE5_FMG-7.0

Exam Name: Fortinet NSE 5 - FortiManager 7.0

Innovior ITTech

Q&A

Fortinet NSE 5 - FortiManager 7.0
NSE5_FMG-7.0

(70 Questions)

http://www.facebook.com/ InnoviorITTech

We Offer Free Update Service
For One Year.

QUESTION 1
Which two statements about Security Fabric integration with FortiManager are true? (Choose two.)

A. The Fabric View module enables you to view the Security Fabric ratings for Security Fabric devices.
B. The Security Fabric license, group name, and password are required for the FortiManager Security Fabric integration.
C. The Security Fabric settings are part of the device-level settings.
D. The Fabric View module enables you to generate the Security Fabric ratings for Security Fabric devices.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Refer to the exhibit.

An administrator would like to create a policy on the Staging ADOM in backup mode, and install it on the FortiGate device in the same ADOM.
How can the administrator perform this task?

A. The administrator must change the ADOM mode to Advanced to bring the FortiManager online.
B. The administrator must disable the FortiManager offline mode first.
C. The administrator must use the Policy & Objects section to create a policy first.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
What is the purpose of the Policy Check feature on FortiManager?

A. It provides recommendations for optimizing policies in a policy package.
B. It provides recommendations to combine similar policy packages within an ADOM into one single policy package.

C. It compares the policy packages with the revision history, and updates policy packages in the ADOM database.
D. It merges and creates dynamic mappings for duplicate objects used in a policy package.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

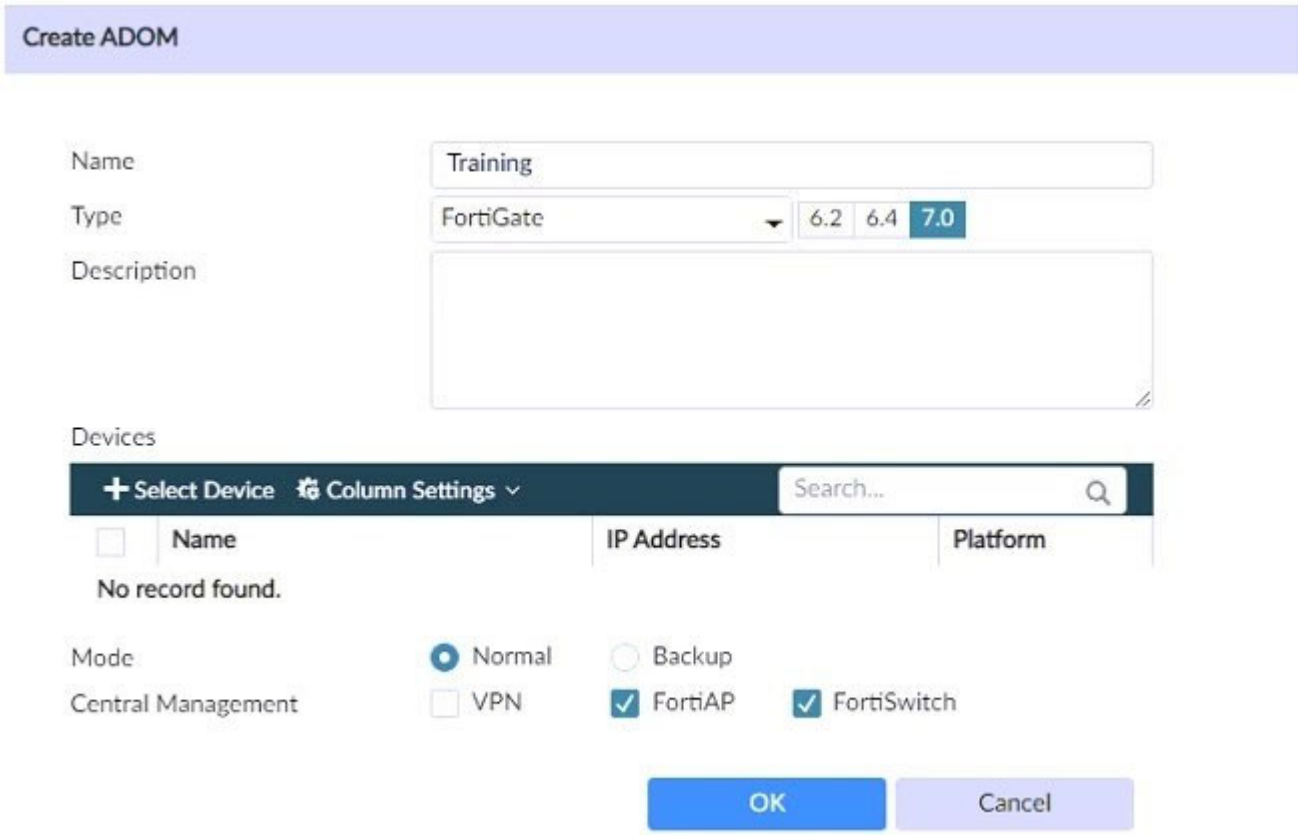
QUESTION 4
An administrator's PC crashes before the administrator can submit a workflow session for approval. After the PC is restarted, the administrator notices that the ADOM was locked from the session before the crash.
How can the administrator unlock the ADOM?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Refer to the exhibit.



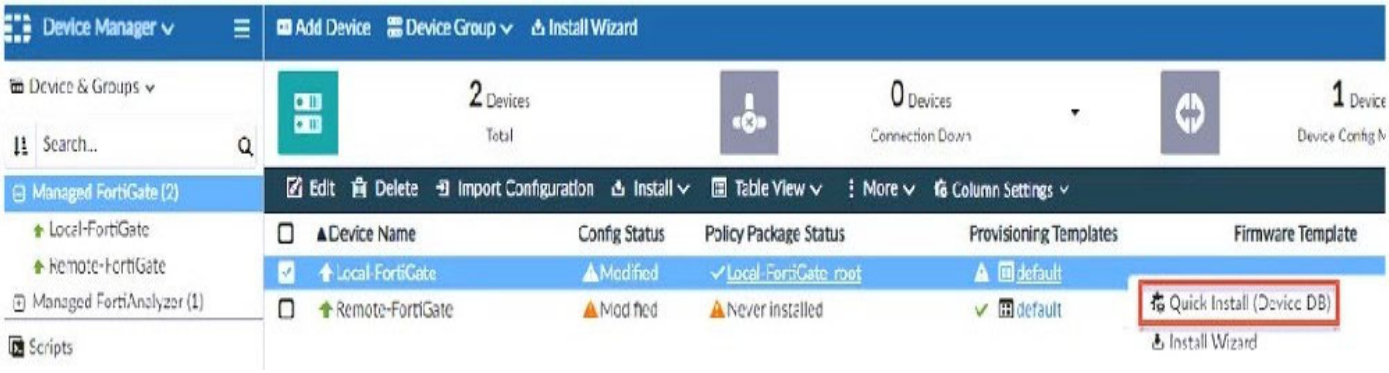
Which two statements about an ADOM set in Normal mode on Fortitvlanager are true? (Choose two.)

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
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 all the changes in the device database first and the administrator must reinstall the changes on the FortiGate device.
B. It provides the option to preview only the policy package changes before installing them.
C. It installs provisioning templates changes on the FortiGate device.
D. It installs device-level changes on the FortiGate device without launching the Install Wizard.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Refer to the exhibit.

```
FortiManager # config system dm
(dm)# set rollback-allow-reboot enable
(dm)# end
FortiManager #
```

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8

An administrator would like to review, approve, or reject all the firewall policy changes made by the junior administrators.
How should the workspace mode settings be configured on FortiManager?

A. Set to read/write and using the policy locking feature
B. Set to normal and using the approval group feature
C. Set to workflow and using the ADOM locking feature
D. Set to workspace and using the policy locking feature

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
What is the purpose of ADOM revisions?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

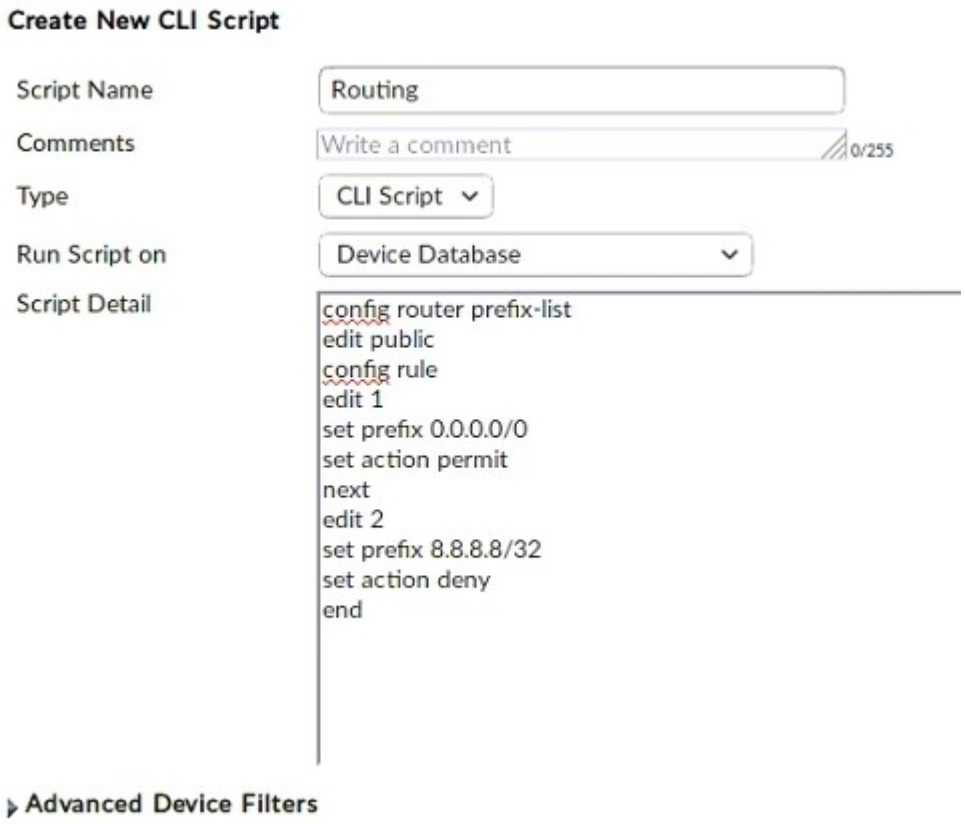
QUESTION 10
An administrator configures a new OSPF route on FortiManager and has not yet pushed the changes to the managed FortiGate device.
In which database will the configuration be saved?

A. ADOM-level database
B. Configuration-level database
C. Revision history database
D. Device-level database

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Refer to the exhibit.



What will happen 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: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Refer to the exhibit.

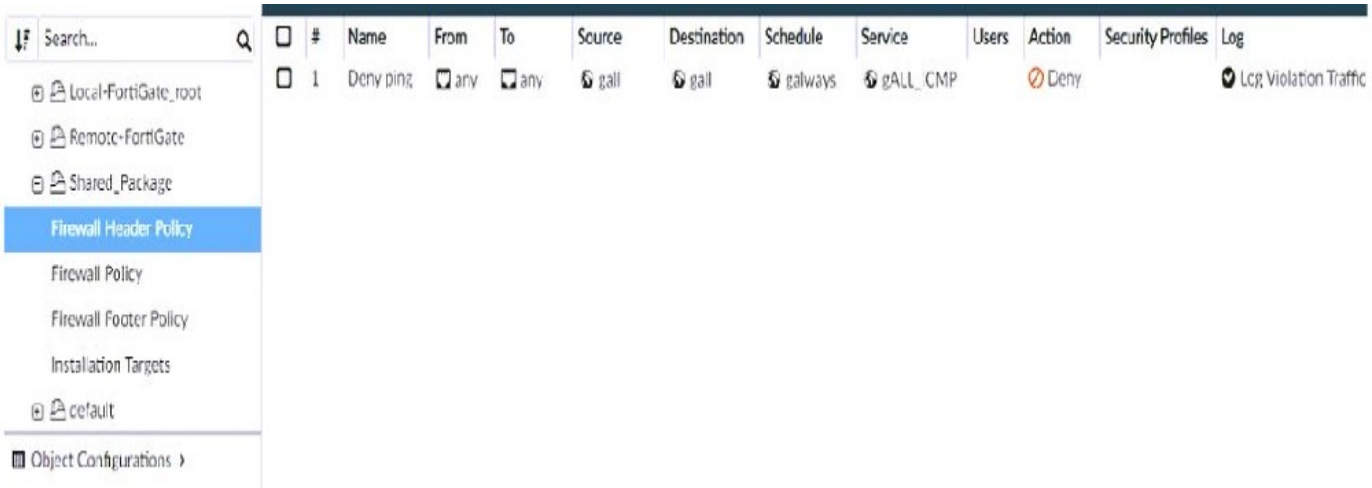
An administrator logs in to the FortiManager GUI and sees the panes shown in the exhibit. Which two reasons can explain why the FortiAnalyzer feature panes do not appear? (Choose two.)

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Refer to the exhibit.



A service provider administrator has assigned a global policy package to a managed customer ADOM named

My_ADOM, which has four policy packages. The customer administrator has access only to My_ADOM.
How can customer or service provider administrators remove both global header and footer policies from the policy package named Shared_Package?

A. The service provider administrator can unassign both global policies from My_ADOM.
B. The service provider administrator can unassign both policies from the global ADOM.
C. The customer administrator can unassign both global polices from My_ADOM.
D. The customer administrator can unassign both polices by locking My_ADOM.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Refer to the exhibit.

```
FortiManager # diagnose dvm device list
--- There are currently 1 devices/vdoms managed ---
--- There are currently 1 devices/vdoms count for license ---

TYPE            OID    SN              HA      IP           NAME            ADOM       IPS                FIRMWARE

fmgfaz-managed  161    FGVM010000064692 -      10.200.1.1   Local-FortiGate  My_ADOM    18.00171 (extended) 7.0 MR0 (157)
                |- 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 not match the device-level database.
B. Configuration changes have been installed on FortiGate, which means the FortiGate configuration has been changed.
C. Configuration changes directly made on FortiGate have been automatically updated to the device-level database.
D. The latest revision history for the managed FortiGate does match the FortiGate running configuration.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
What will be the result of reverting to a previous revision version in the revision history?

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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
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?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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: BD
Section: (none)
Explanation

Explanation/Reference:
Reference:

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

QUESTION 18
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: BC
Section: (none)
Explanation

Explanation/Reference:
Reference:

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

QUESTION 19
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: (none)
Explanation

Explanation/Reference:

QUESTION 20
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
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

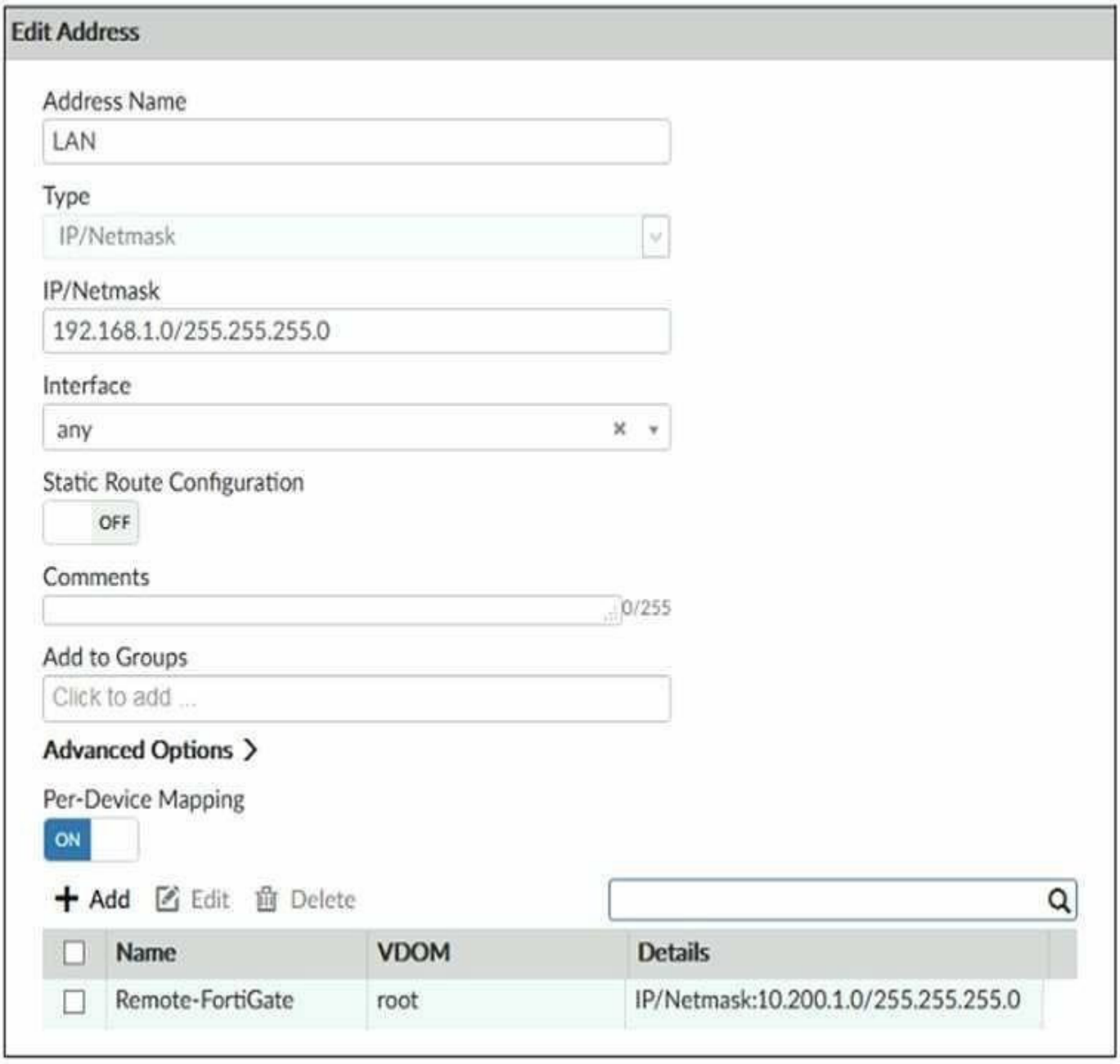
Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 22
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In the example, the dynamic address object LocalLan refers to the internal network address of the managed firewalls. The object has a default value of 192.168.1.0/24. The mapping rules are defined per device. For Remote-FortiGate, the address object LocalLan referes to 10.10.11.0/24. The devices in the ADOM that do not have dynamic mapping for LocalLan have a default value of 192.168.1.0/2.

QUESTION 23
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 25

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: (none)
Explanation

Explanation/Reference:

QUESTION 26
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Which of the following statements are true regarding schedule backup of FortiManager? (Choose two.)

A. Backs up all devices and the FortiGuard database.
B. Does not back up firmware images saved on FortiManager
C. Supports FTP, SCP, and SFTP
D. Can be configured from the CLI and GUI

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
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 mark(?) at the end of the device name
D. By an Asterisk (*) at the end of the device name

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 31
What does a policy package status of Modified indicate?

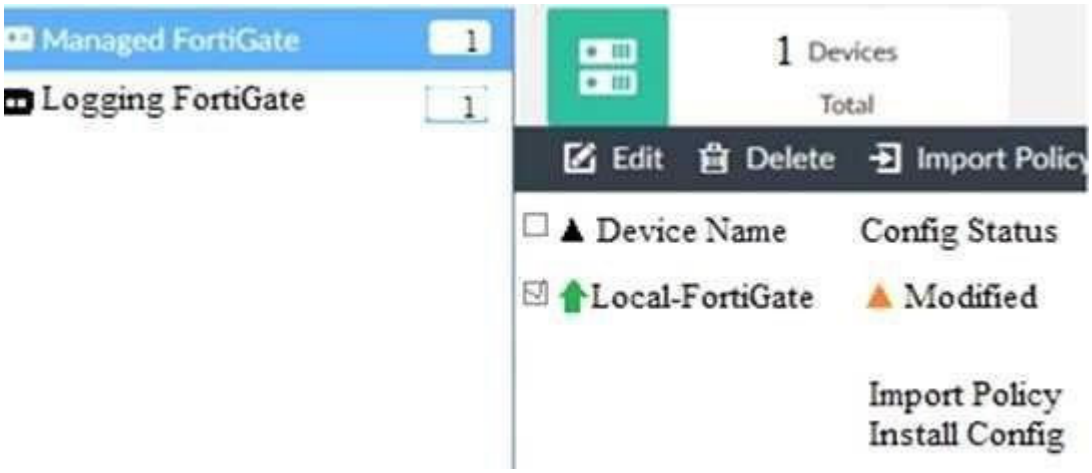
A. FortiManager is unable to determine the policy package status
B. The policy package was never imported after a device was registered on FortiManager
C. The Policy configuration has been changed on a managed device and changes have not yet been imported into FortiManager
D. The Policy package configuration has been changed on FortiManager and changes have not yet been installed on the managed device.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference:

http://help.fortinet.com/fmgr/50hlp/56/5-6-1/FortiManager_Admin_Guide/1200_Policy%20and%20Objects/0800_Managing%20policy%20packages /2200_Policy%20Package%20Installation%20targets.htm

QUESTION 32
View the following exhibit.



When using Install Config option to install configuration changes to managed FortiGate, which of the following statements are true? (Choose two.)

A. Once initiated, the install process cannot be canceled and changes will be installed on the managed device
B. Will not create new revision in the revision history
C. Installs device-level changes to FortiGate without launching the Install Wizard
D. Provides the option to preview configuration changes prior to installing them

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Which of the following statements are true regarding VPN Manager? (Choose three.)

A. VPN Manager must be enabled on a per ADOM basis.
B. VPN Manager automatically adds newly-registered devices to a VPN community.
C. VPN Manager can install common IPsec VPN settings on multiple FortiGate devices at the same time.
D. Common IPsec settings need to be configured only once in a VPN Community for all managed gateways.
E. VPN Manager automatically creates all the necessary firewall policies for traffic to be tunneled by IPsec.

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

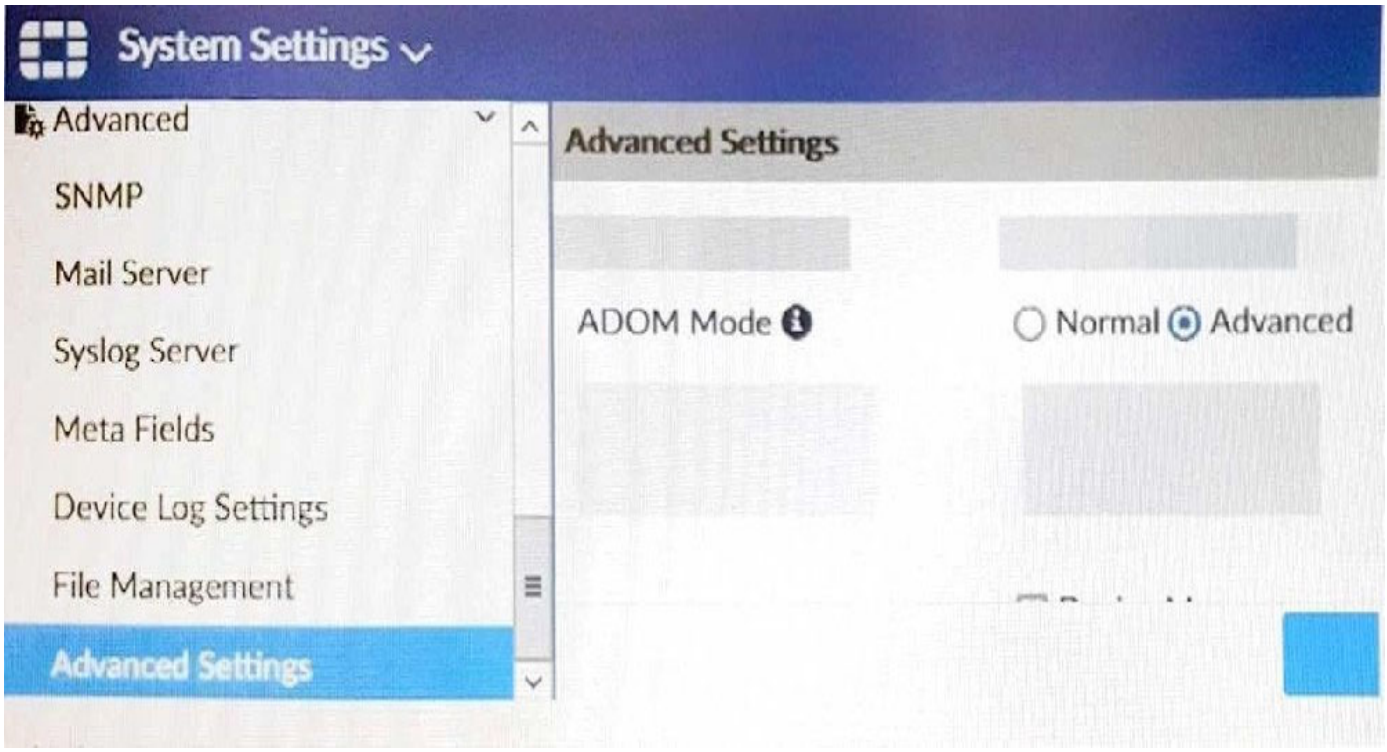
QUESTION 34
An administrator would like to authorize a newly-installed AP using AP Manager. What steps does the administrator need to perform to authorize an AP?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
View the following exhibit.



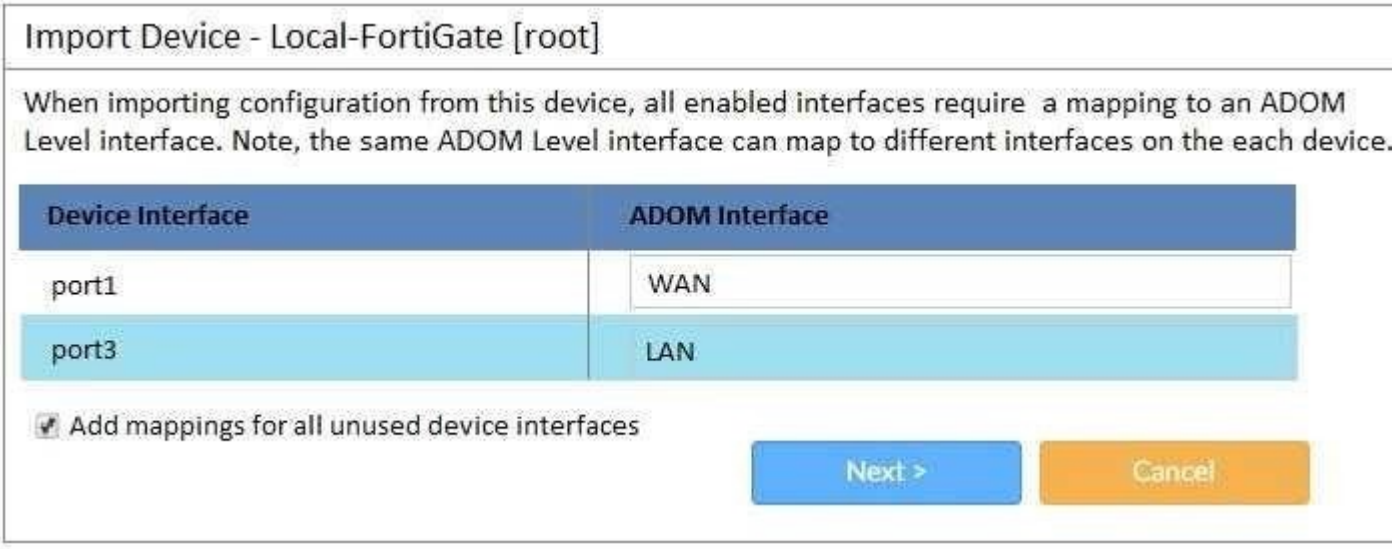
Which of the following statements are true based on this configuration setting? (Choose two.)

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.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
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: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
Refer to the exhibit.

Which two statements about the output are true? (Choose two.)

A. The latest revision history for the managed FortiGate does match with the FortiGate running configuration
B. Configuration changes have been installed to FortiGate and represents FortiGate configuration has been changed
C. The latest history for the managed FortiGate does not match with the device-level database
D. Configuration changes directly made on the FortiGate have been automatically updated to device- level database

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 39
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: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
In addition to the default ADOMs, an administrator has created a new ADOM named Training for 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 device manually to the Training ADOM using the Add Device wizard

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference:

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

QUESTION 41
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 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.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
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: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/676493/removing-existing- configuration-references-to-interfaces

QUESTION 43
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 all address object in the referenced firewall policy.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

https://help.fortinet.com/fmgr/50hlp/56/5-6-

2/FortiManager_Admin_Guide/1200_Policy%20and%20Objects/1200_Managing%20objects/0800_Rem ove%20an%20object.htm

QUESTION 44
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.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
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.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 46
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 47
You are moving managed FortiGate devices from one ADOM to a new ADOM. Which statement correctly describes the expected result?

A. Any pending device settings will be installed automatically
B. Any unused objects from a previous ADOM are moved to the new ADOM automatically
C. The shared policy package will not be moved to the new ADOM
D. Policy packages will be imported into the new ADOM automatically

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://community.fortinet.com/t5/FortiManager/Technical-Note-How-to-move-objects-to- new-ADOM-on-FortiManager/ta-p/198342

QUESTION 48
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Which two items does an FGFM keepalive message include? (Choose two.)

A. FortiGate uptime
B. FortiGate license information
C. FortiGate IPS version
D. FortiGate configuration checksum

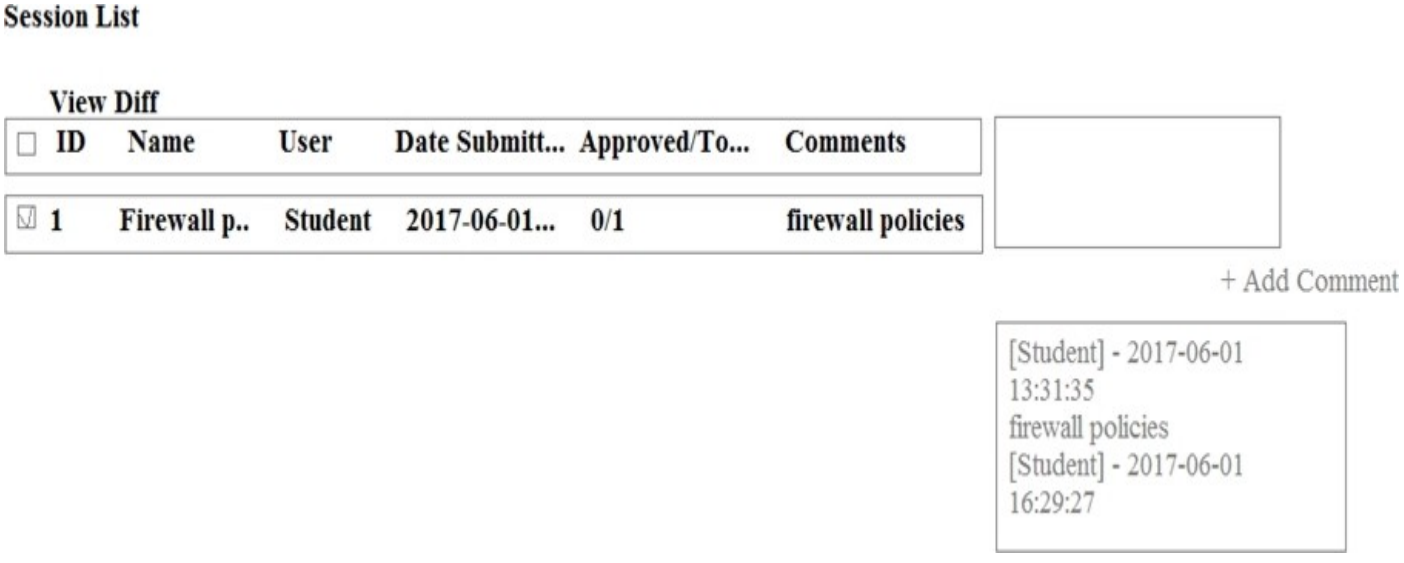
Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Reference: https://docs.fortinet.com/document/fortimanager/6.2.0/fortigate- fortimanagercommunications-protocol-guide/579138/keep-alive-messages

QUESTION 51
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?



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

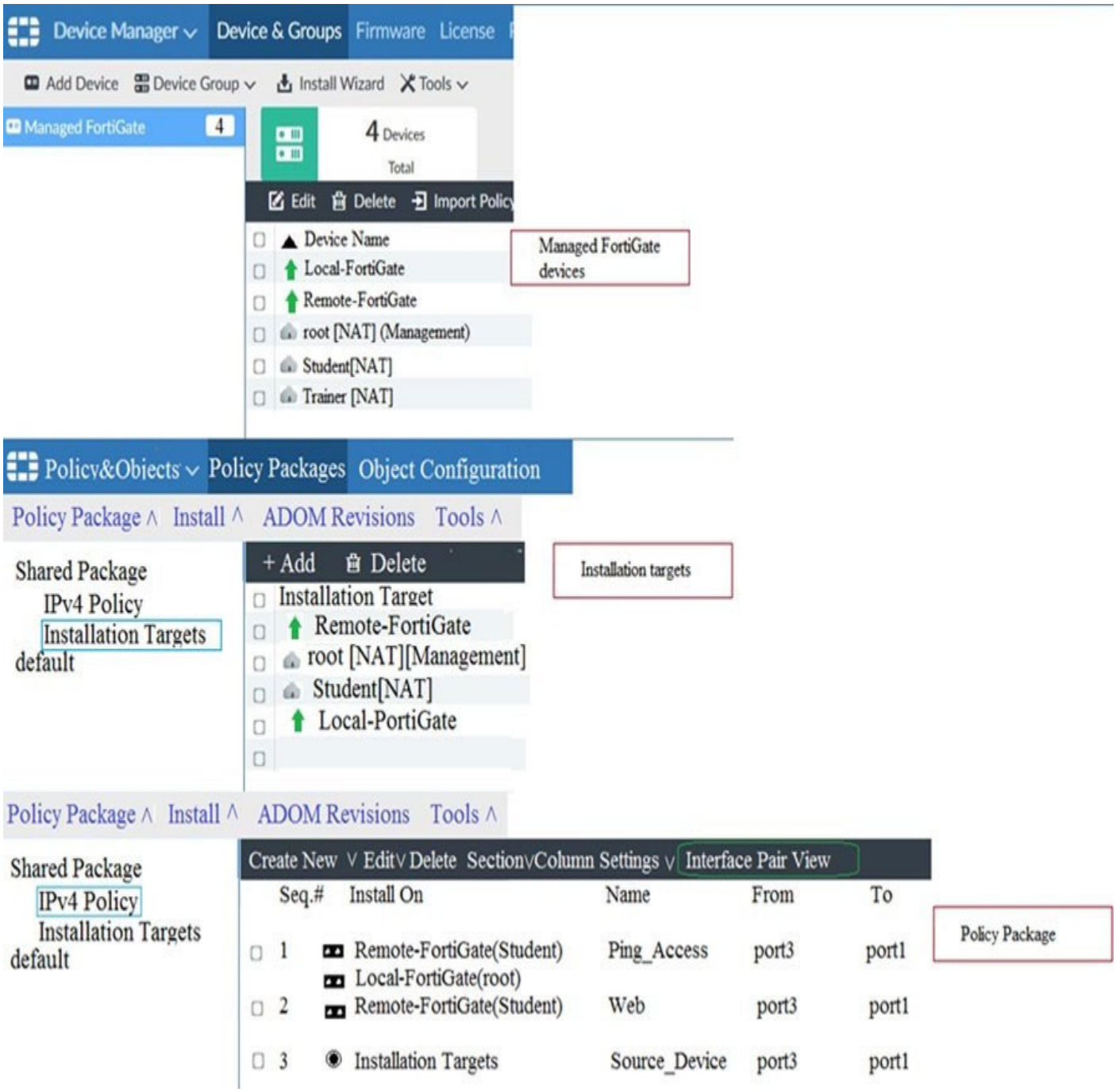
D. Student, who submitted the workflow session, must first self-approve the request

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 52
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: (none)
Explanation

Explanation/Reference:

QUESTION 53
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.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
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

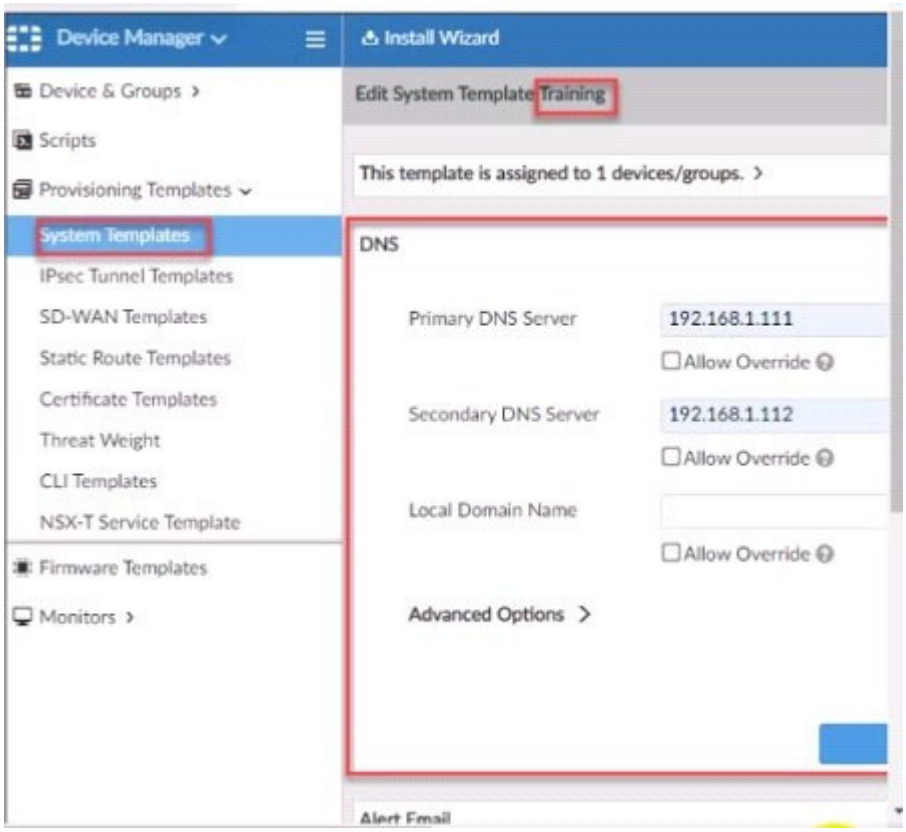
Where does the administrator import the file from?

A. File system
B. ADOM1
C. ADOM2 object database
D. ADOM2

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Refer to the exhibit.



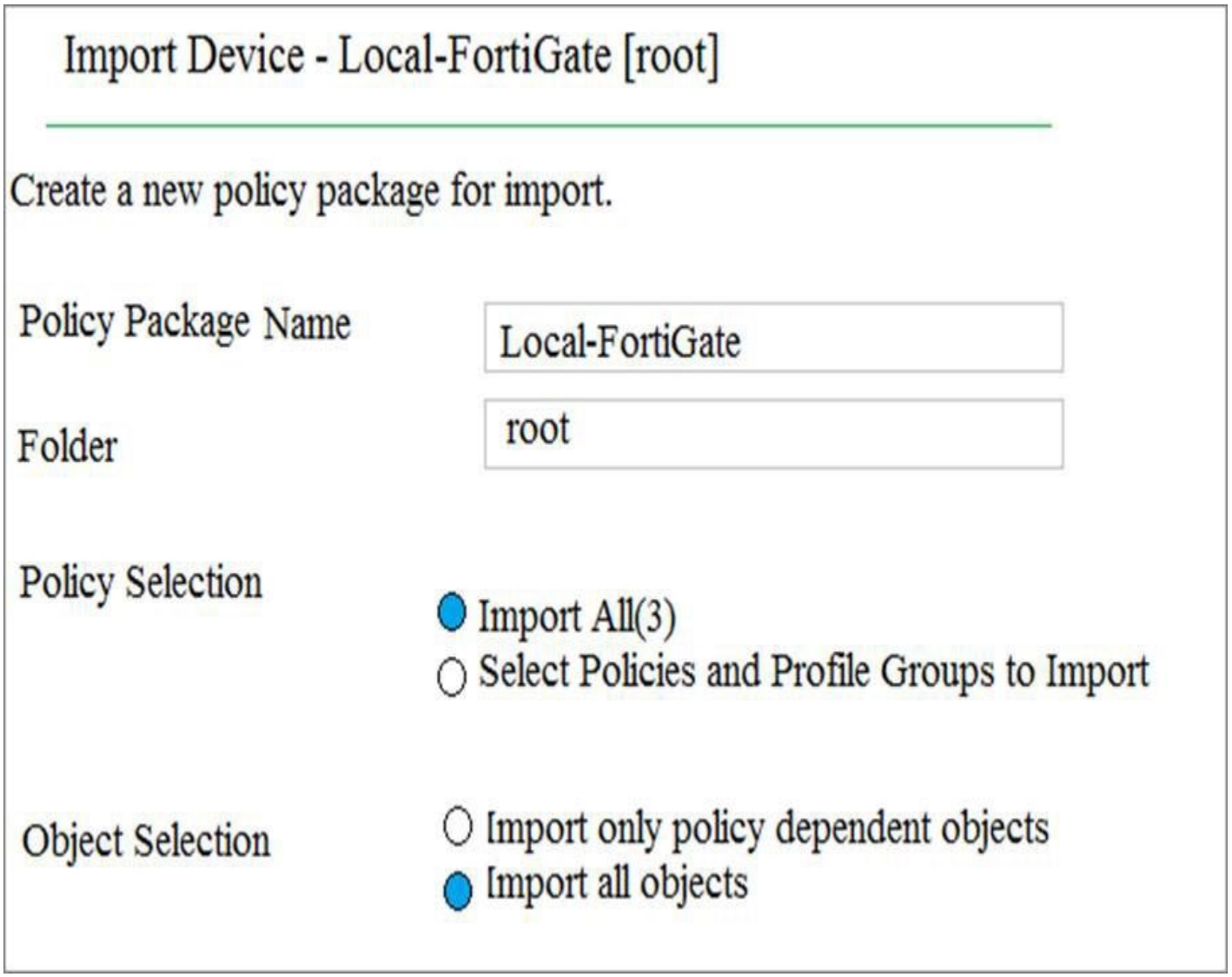
According to the error message why is FortiManager failing to add the FortiAnalyzer device?

A. The administrator must turn off the Use Legacy Device login and add the FortiAnaJyzer 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 FortiAnaJyzer device
D. The administrator must use the correct user name and password of the FortiAnalyzer device

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
View the following exhibit.



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: (none)
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 57
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 58
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: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
In the event that the primary FortiManager fails, which of the following actions must be performed to return the FortiManager HA to a working state?

A. Secondary device with highest priority will automatically be promoted to the primary role, and manually reconfigure all other secondary devices to point to the new primary device
B. Reboot one of the secondary devices to promote it automatically to the primary role, and reconfigure all other secondary devices to point to the new primary device.
C. Manually promote one of the secondary devices to the primary role, and reconfigure all other secondary devices to point to the new primary device.
D. FortiManager HA state transition is transparent to administrators and does not require any reconfiguration.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
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: (none)
Explanation

Explanation/Reference:

QUESTION 61
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 62
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: (none)
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 63
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
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

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 66
An administrator has assigned a global policy package to a new ADOM called ADOM1.

What will happen if the administrator tries to create a new policy package in ADOM1?

A. When creating a new policy package, the administrator can select the option to assign the global policy package to the new policy package
B. When a new policy package is created, the administrator needs to reapply the global policy package to ADOM1.
C. When a new policy package is created, the administrator must assign the global policy package from the global ADO
D. When the new policy package is created, FortiManager automatically assigns the global policy package to the new policy package.

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation:

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

QUESTION 67
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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

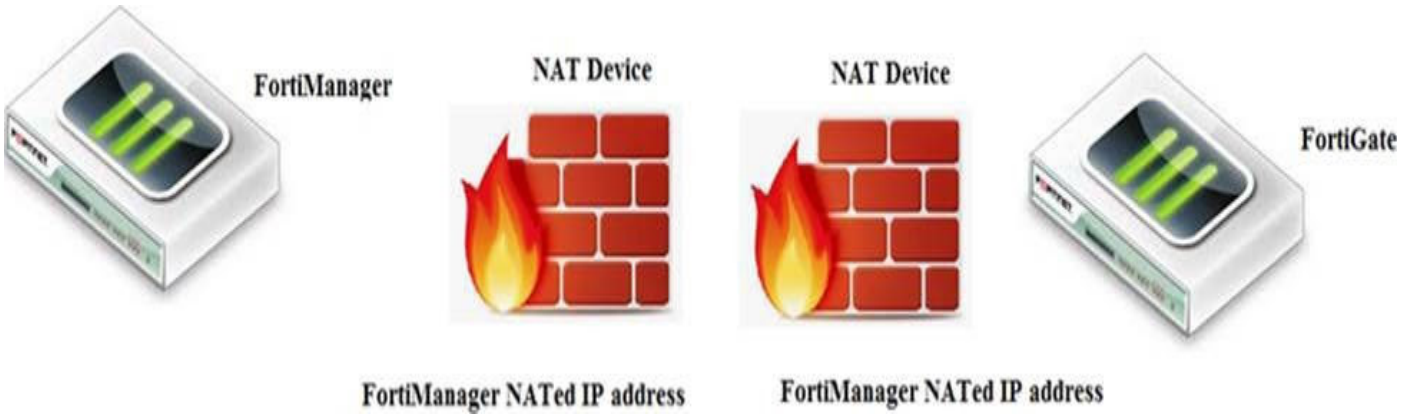
QUESTION 68
Which two conditions trigger FortiManager to create a new revision history? (Choose two.)

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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
View the following exhibit.



If both FortiManager and FortiGate are behind the NAT devices, what are the two expected results? (Choose two.)

A. FortiGate is discovered by FortiManager through the FortiGate NATed IP address.correct
B. FortiGate can announce itself to FortiManager only if the FortiManager IP address is configured on FortiGate under central management.
C. During discovery, the FortiManager NATed IP address is not set by default on FortiGate.
D. If the FCFM tunnel is torn down, FortiManager will try to re-establish the FGFM tunnel.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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