Fortinet NSE 5 - FortiManager 7.2

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

A. The shared 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.

Answer(s): C

---

2. An administrator enabled workspace mode and now wants to delete an address object that is currently referenced in a firewall policy.
Which two results can the administrator expect to happen? (Choose two.)

- [ ] A. FortiManager will temporarily change the status of the referenced firewall policy.
- [ ] B. FortiManager will disable the status of the address object.
- [ ] C. FortiManager will replace the deleted address object with the none address object in the referenced firewall policy.
- [ ] D. FortiManager will not allow the administrator to delete a referenced address object until the ADOM is locked.

Answer(s): C D

---

3. An administrator runs the Policy Check feature on FortiManager ADOM.
What will be the result?

A. It will find and provide recommendations to combine multiple separate policy packages into one common policy package.

B. It will find and merge duplicate policies in the policy package.

C. It will find and provide recommendations for optimizing policies in a policy package.

D. It will find and delete disabled firewall policies in the policy package.

Answer(s): C

---

4. 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, FortiManager removes previously assigned policies.
- [ ] D. You can edit or delete all the global objects in the global ADOM.

Answer(s): C D

---

5. An administrator is replacing a failed device on FortiManager by running the following command: execute device replace sn .
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

Answer(s): C

---

6. Refer to the exhibit.

```
FortiManager # diagnose fmupdate view-serverlist fds
Fortiguard Server Comm : Enabled
Server Override Mode   : Strict
FDS server list        :
Index   Address                    Port  TimeZone  Distance Source
-------------------------------------------------------------------
*0      10.0.1.50                  8890  -5        0        CLI
 1      96.45.33.89                443   -5        0        FDNI
 2      96.45.32.81                443   -5        0        FDNI
 ...
 9      fds1.fortinet.com          443   -5        0        DEFAULT
```

How will FortiManager try to get updates for antivirus and IPS?

A. From the list of configured override servers or public FDN servers

B. From the default server fds1.fortinet.com

C. From the configured override server IP address 10.0.1.50 only

D. From public FDNI server IP address with the fourth highest octet only

Answer(s): C

---

7. Refer to the exhibit.

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

TYPE             OID    SN               HA      IP          NAME
fmgfaz-managed   161    FGVM010000064692 -      10.200.1.1  Local-FortiGate   M
                 |- STATUS: dev-db: modified; conf: in sync cond: pending; dm:r
                 |- vdom:[3]root flags:0 adom:My_ADOM pkg: [imported]Local-Fort
```

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

- ☐ A. Configuration changes have been installed on FortiGate, which means the FortiGate configuration has been changed.
- ☐ B. The latest revision history for the managed FortiGate does match the FortiGate running configuration.
- ☐ 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 not match the device-level database.

Answer(s): B D

---

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

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

Answer(s): B D

---

9. Refer to the exhibit.

```
FortiManager # config system global
(global)# set workspace-mode normal
(global)# end
FortiManager #
```

Given the configuration shown in the exhibit, what are two results from this configuration? (Choose two.)

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

Answer(s): B C

---

10. 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 a new policy package is created, the administrator must import the global policy package to ADOM1.

B. When the new policy package is created, FortiManager automatically assigns the global policy package to the new policy package.

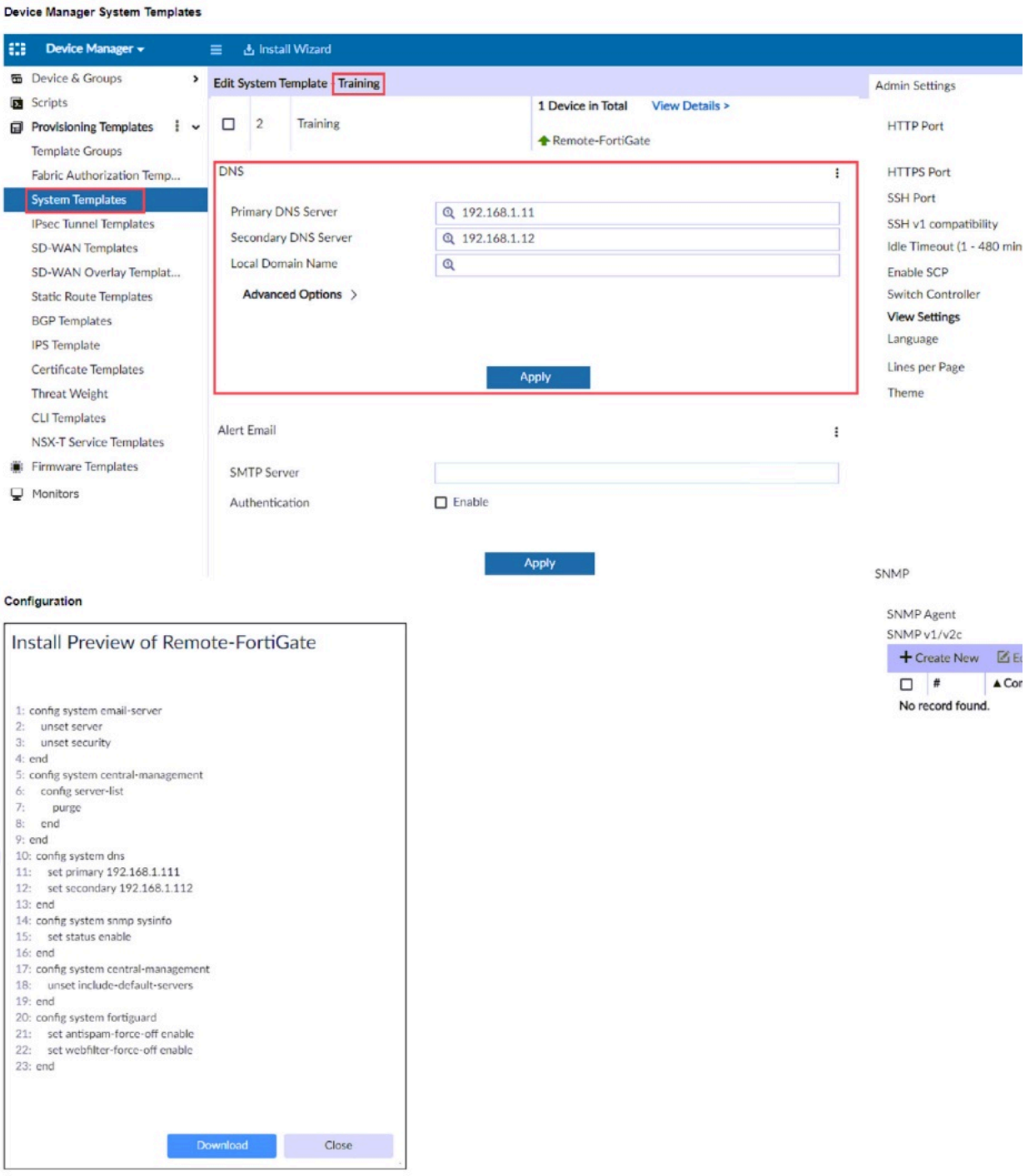
C. When a new policy package is created, the administrator must assign the global policy package from the global ADOM.

D. When creating a new policy package, the administrator can select the option to assign the global policy package to the new policy package.

Answer(s): B

---

11. Refer to the exhibit.



On FortiManager, an administrator created a new system template named Training with two new DNS

addresses. During the installation preview stage, the administrator notices that central-management settings need to be purged.
What can be the main reason for the central-management purge command?

A. The Remote-FortiGate device does not have any DNS server-list configured in the central-management settings.

B. The DNS addresses in the default system settings are the same as the Training system template.

C. The ADOM is locked by another administrator.

D. The Training system template has a default FortiGuard widget.

Answer(s): D

---

12. 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(s): A

---

13. 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 install the logging configuration to the managed devices.

C. FortiManager can be used only as a logging device.

D. FortiManager will enable ADOMs to collect logs automatically from non-FortiGate devices.

Answer(s): A

---

14. 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 normal and using the approval group feature

B. Set to read/write and using the policy locking feature

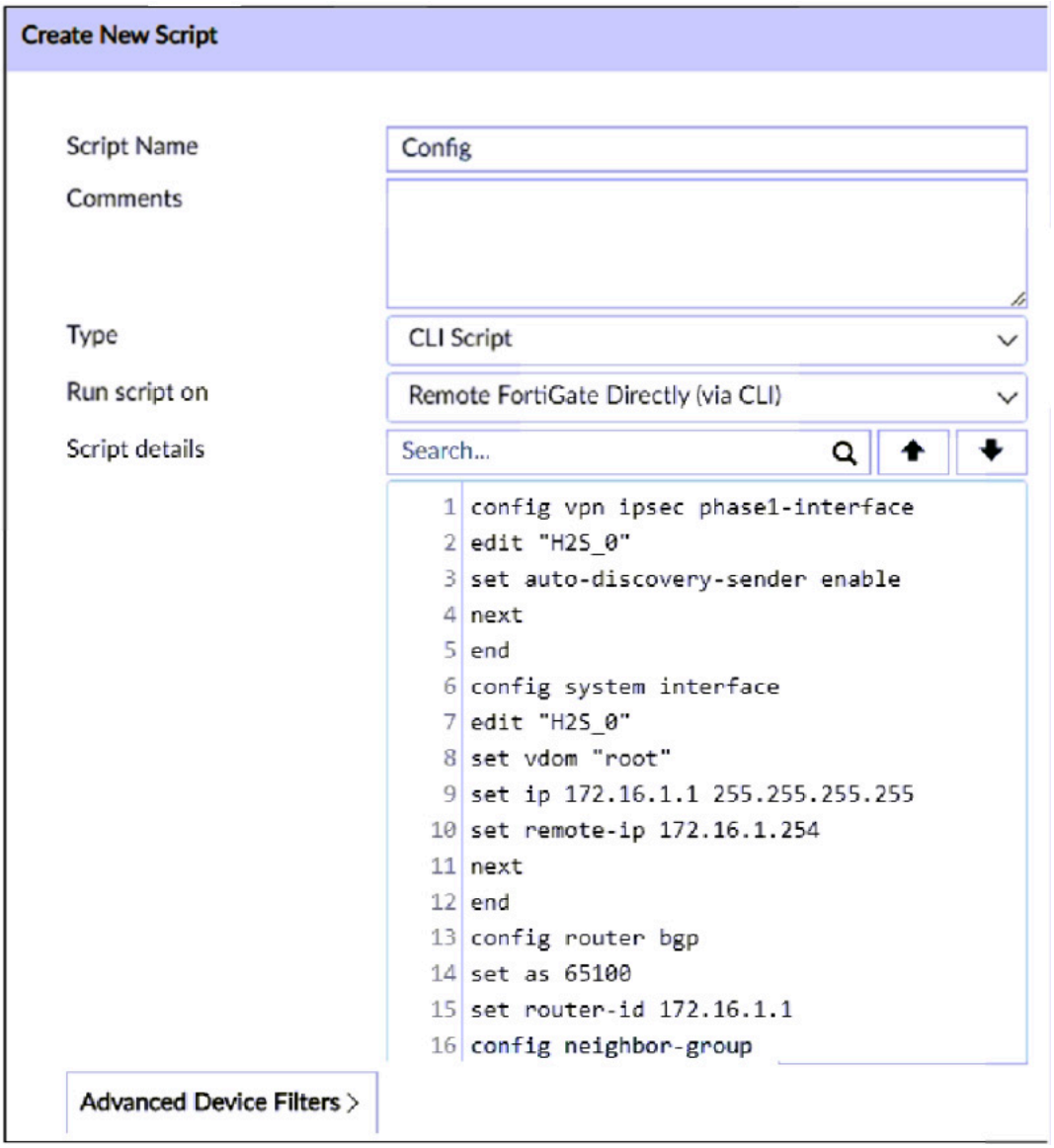
C. Set to workflow and using the ADOM locking feature

D. Set to workspace and using the policy locking feature

Answer(s): C

---

15. Refer to the exhibit.



What will happen if the script is run using the Remote FortiGate Directly (via CLI) option? (Choose two.)

- [ ] A. FortiManager provides a preview of CLI commands before executing this script on a managed FortiGate.
- [ ] B. FortiManager will create a new revision history.
- [ ] C. FortiGate will auto-update the FortiManager device-level database.
- [ ] D. You must install these changes using the Install Wizard.

Answer(s): B C

---

16. In addition to the default ADOMs, an administrator has created a new ADOM named Training for FortiGate devices only. 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 appear in the root ADOM.

C. The authorized FortiGate can be added to the Training ADOM using FortiGate Fabric Connectors.

D. The authorized FortiGate will be automatically added to the Training ADOM.

Answer(s): B

---

17. In the event that one of the secondary FortiManager devices fails, which action must be performed to return the FortiManager HA manual mode to a working state?

A. The FortiManager HA state transition is transparent to administrators and does not require any reconfiguration.

B. Manually promote one of the working secondary devices to the primary role, and reboot the old primary device to remove the peer IP of the failed device.

C. Reconfigure the primary device to remove the peer IP of the failed device.

D. Reboot the failed device to remove its IP from the primary device.

Answer(s): C

---

18. 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(s): A B E

---

19. Refer to the exhibit.

A junior administrator is troubleshooting a FortiManager connectivity issue that is occurring with managed FortiGate devices.

Given the FortiManager device manager settings shown in the exhibit, what can you conclude from the exhibit?

A. FortiManager lost internet connectivity, therefore, both devices appear to be down.

B. The administrator must refresh both devices to restore connectivity.

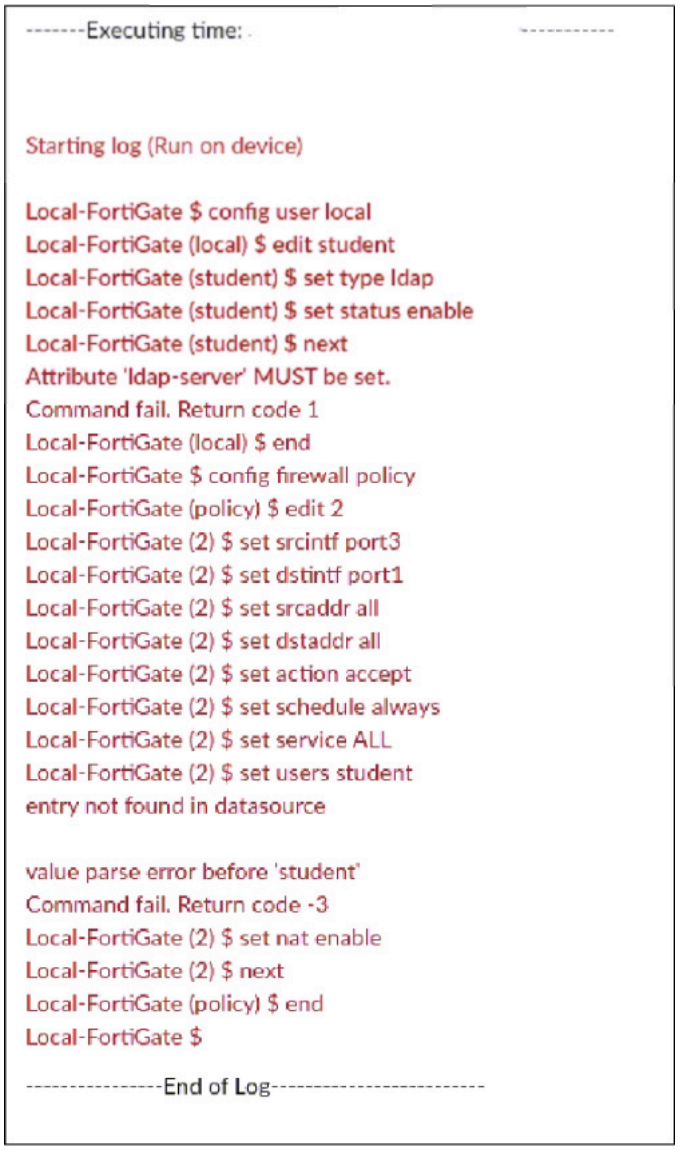
C. The administrator had restored the FortiManager configuration file.

D. The administrator can reclaim the FGFM tunnel to get both devices online.

Answer(s): C

---

20. Refer to the exhibit.



```
-------Executing time: .                                  ----------


Starting log (Run on device)

Local-FortiGate $ config user local
Local-FortiGate (local) $ edit student
Local-FortiGate (student) $ set type ldap
Local-FortiGate (student) $ set status enable
Local-FortiGate (student) $ next
Attribute 'ldap-server' MUST be set.
Command fail. Return code 1
Local-FortiGate (local) $ end
Local-FortiGate $ config firewall policy
Local-FortiGate (policy) $ edit 2
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 users student
entry not found in datasource

value parse error before 'student'
Command fail. Return code -3
Local-FortiGate (2) $ set nat enable
Local-FortiGate (2) $ next
Local-FortiGate (policy) $ end
Local-FortiGate $

----------End of Log-------------------------
```

What can you conclude from the failed installation log shown in the exhibit?

A. Policy ID 2 will not be installed.

B. Policy ID 2 is installed in the disabled state.

C. Policy ID 2 is installed without a source address.

D. Policy ID 2 is installed without the remote user student.

Answer(s): D