**Vendor:** Fortinet

**Exam Code:** NSE5_FMG-7.2

**Exam Name:** Fortinet NSE 5 - FortiManager 7.2

**Version:** 24.021

**QUESTION 1**
Refer to the exhibit. Given the configuration shown in the exhibit, what are two results from this configuration? (Choose two.)

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

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:** BC
**Explanation:**
The policy lock is automatically released at administrator timeout, or if the administrator closes a session gracefully without unlocking the policy package or policy.

**QUESTION 2**
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:** B
**Explanation:**
When a device is authorized and ADOMs are enabled, the device appears in the root ADOM.

**QUESTION 3**
In the event that one of the secondary FortiManager devices fails, which action must be performed to return the FortiManager HA manual mode to a working state?

A. The 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:** C

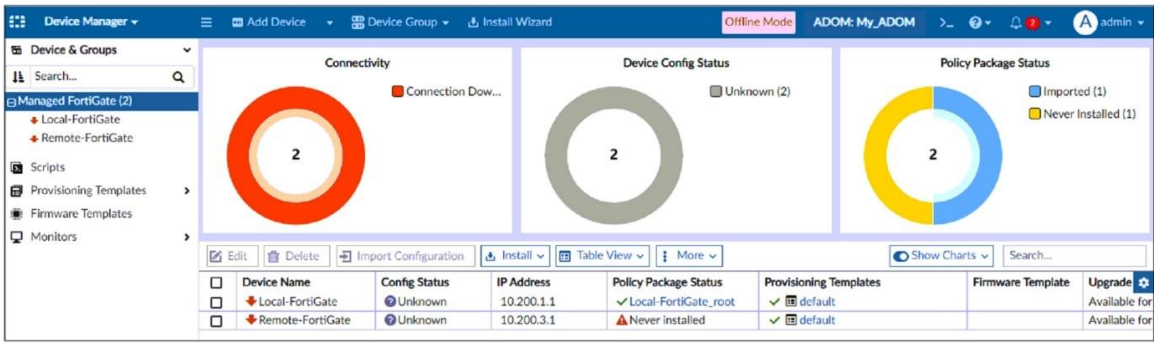
**Explanation:**
If the secondary FortiManager fails, the administrator can reconfigure the primary device to remove the secondary configuration.

**QUESTION 4**
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
**Explanation:**
Management Extension apps are disabled in the FortiManager default configuration and when you log in to FortiManager for the first time the setup wizard displays.

**QUESTION 5**
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:** C
**Explanation:**
By default, offline mode is enabled when a Fortimanager backup is restored.

**QUESTION 6**
Refer to the exhibit. Given the configuration shown in the exhibit, how did FortiManager handle the service category named General?

```
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)"
```

A. FortiManager ignored the firewall service category General and updated the FortiGate duplicate value in the FortiGate database.
B. FortiManager ignored the firewall service category General and did not update its database with the value.
C. FortiManager ignored the firewall service category General but created a new service category in its database.
D. FortiManager ignored the firewall service category General and deleted the duplicate value in its database.

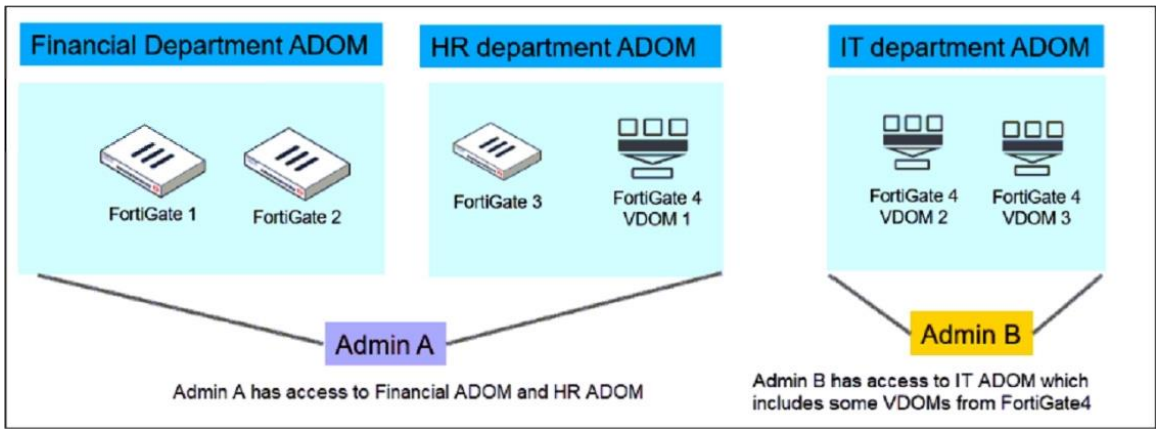
**Answer:** B
**Explanation:**
FortiManager does not import already existing, or duplicate, entries into the ADOM database.

**QUESTION 7**
An administrator is in the process of moving the system template profile between ADOMs by running the following command: execute fmprofile 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
**Explanation:**
The command in question is execute fmprofile import-profile ADOM2 3547 /tmp/myfile. If the administrator is importing the system template profile into ADOM2, and considering each ADOM has a unique object database, the file is likely being imported from the FortiManager file system.

**QUESTION 8**
Refer to the exhibit. An administrator would like to create three ADOMs on FortiManager with different access levels based on departments.
What two conclusions can you draw from the design shown in the exhibit? (Choose two.)




A. Admin A can access VDOM2 and VDOM3 with the super user profile.
B. The FortiManager policies and objects database can be shared between the Financial and HR ADOMs.
C. The administrator must set the FortiManager ADOM mode to Advanced.
D. The administrator must configure FortiManager in workspace mode.

**Answer:** AC
**Explanation:**
Administrators who have the Super_User profile have full access to all ADOMs, whereas administrators with any other profile have access only to those ADOMs to which they are assigned—this can be one or more.
In Advanced mode, you can assign different VDOMs from the same FortiGate device to different ADOMs.

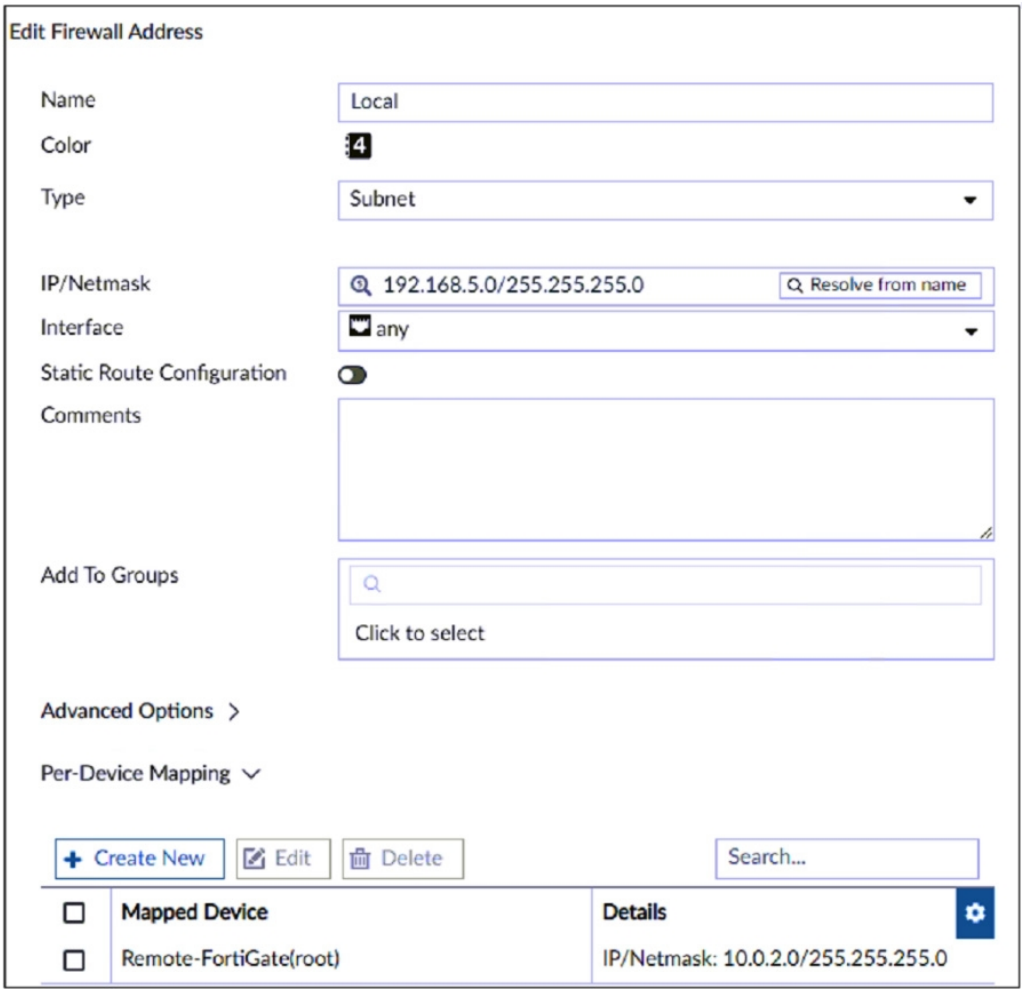
**QUESTION 9**
An administrator runs the reload failure command diagnose test deploymanager reloadconf <deviceid> on FortiManager.
What does this command do?

A. It reloads the policy package from the FortiManager to FortiGate.
B. It installs the latest configuration on the specified FortiGate and updates the revision history database.
C. It downloads the latest configuration from the specified FortiGate and performs a reload operation on the device database.
D. It compares and provides differences in configuration on FortiManager with the current running configuration of the specified FortiGate.

**Answer:** C
**Explanation:**
The command #diagnose test deploymanager reloadconf <deviceid/OID> is used to update the device-level database in case of a failure. It works by having FortiManager download and reload the FortiGate's configuration file. If the FortiGate configuration is error-free, the update succeeds. Otherwise, the command output shows where the update failed.

**QUESTION 10**
Refer to the exhibit. An administrator has created a firewall address object, Local, which is used in the Remote-FortiGate policy package.
When the installation operation is performed, which IP/Netmask will be installed on Remote-

FortiGate, for the Local firewall address object?




A. 192.168.5.0/24
B. Remote-FortiGate will automatically choose an IP/netmask based on its network interface settings.
C. 10.0.2.0/24
D. It will create the Local and Remote-Local firewall address objects on Remote-FortiGate with 192.168.5.0/24 and 10.0.2.0/24 values.

**Answer:** C
**Explanation:**
Per-Device Mapping (or dynamic objects) maps a single logical object to a unique definition/value per device.
In the exhibit, the object called Local has a default value of 192.168.5.0/24. For Remote-FortiGate device, the address object Local will refers to 10.0.2.0/24.
The devices in the ADOM that do not have dynamic mapping for Internal have a default value of 192.168.5.0/24.

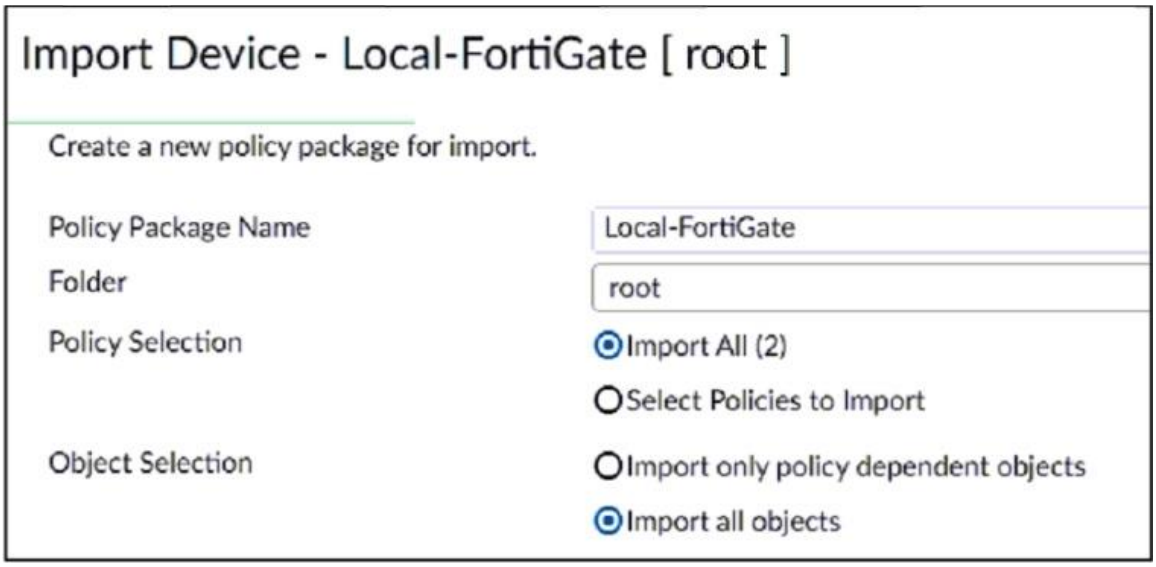
**QUESTION 11**
What are two outcomes of ADOM revisions? (Choose two.)

A. ADOM revisions can save the current state of the whole ADOM.

B. ADOM revisions can save the current state of all policy packages and objects for an ADOM.
C. ADOM revisions can significantly increase the size of the configuration backups.
D. ADOM revisions can create System Checkpoints for the FortiManager configuration.

**Answer:** BC
**Explanation:**
ADOM revisions are different from Configuration revisions.
Configuration revision is the complete configuration of the managed device, including device-level, policy, and object configuration.
ADOM revision is policy packages, objects, and VPN console settings in an ADOM.

**QUESTION 12**
Refer to the exhibit. An administrator is importing a new device to FortiManager and has selected the options shown in the exhibit.
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 locally on FortiGate will be deleted.
B. The unused objects that are not tied to the firewall policies in the policy package will be deleted from the FortiManager database.
C. The unused objects that are not tied to the firewall policies will remain as read-only locally on FortiGate.
D. The unused objects that are not tied to the firewall policies will be installed on FortiGate.

**Answer:** A
**Explanation:**
FortiManager does not need to keep unused objects during the Import configuration operation. So, the first Policy package installation after the import will not include the unused objects, therefore the unused objects will be deleted on FortiGate after the Policy package installation.

**QUESTION 13**
Which configuration setting for FortiGate is part of an ADOM-level database on FortiManager?

A. Routing
B. NSX-T Service Template
C. SNMP
D. Security profiles

**Answer:** D
**Explanation:**
Device Database: all configuration that can be seen under 'Device Manager'.
ADOM Database: all configuration that can be seen under 'Policy & Objects'

**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?

A. Trainer must first create their own workflow session to approve student session.
B. Trainer is not a part of workflow approval group.
C. Trainer must close Student's workflow session before approving the request.
D. Trainer does not have full rights over this ADOM.

**Answer:** B
**Explanation:**
An administrator must be part of an approval group. Being part of the Super_Admin profile is not enough to approve a session.

**QUESTION 15**
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:** C
**Explanation:**
When you move devices from one ADOM to another ADOM, shared policy packages, and objects do not move to the new ADOM. You will need to import policy packages from managed devices.

**QUESTION 16**
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:** CD
**Explanation:**
If you delete a used object, FortiManager will replace it with a none object. The none object is equal to null, which means any traffic that meets that firewall policy will be blocked.
When workspace is enabled, the ADOM is initially read-only. To enable read/write permission, and make changes to the ADOM, you must lock the ADOM, device, or policy package.

**QUESTION 17**
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:** C
**Explanation:**
Policy Check provides recommendations only on what improvements can be made - it does not perform any changes. It uses an algorithm to evaluate policy objects based on:
- Source and destination interface policy objects
- Source and destination address policy objects
- Service and schedule policy objects

Policy Check checks for:
- Duplication, where two objects have identical definitions
- Shadowing, where one object completely shadows another object of the same type
- Overlap, where one object partially overlaps another object of the same type
- Orphaning, where an object has been defined but has not been used anywhere

**QUESTION 18**
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:** CD
**Explanation:**
- All global objects start with "g" and are edited or deleted in the global ADOM only.
- Assigning an additional global policy package to the same individual ADOM policy package removes previously assigned policies.

**QUESTION 19**
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

**Answer:** C
**Explanation:**
To replace the faulty device with the new device, take the following steps:
1. Note the device name of the original FortiGate.
If the replacement device is already listed as unregistered, then you will need to delete it from the unregistered device list in the root ADOM.
2. Add the serial number of the replacement FortiGate.
After the replace command is executed, FortiManager updates the serial number in its database.
3. Verify that the new device serial number is associated with the faulty device in FortiManager.
You can do this using the CLI or the System Information widget of FortiGate.
4. Send a request from the replacement device to register it with FortiManager

**QUESTION 20**
Refer to the exhibit. How will FortiManager try to get updates for antivirus and IPS?

```
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
```

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:** C
**Explanation:**
When Server Override Mode is set to Strict, FortiManager gets updates only from override server address (source type CLI).
When source type is CLI means manual override configured, when is FDNI means public FDS.

**QUESTION 21**
Refer to the exhibit. Which two statements about the output are true? (Choose two.)

```
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             ADOM         IPS        FIRMWARE

fmgfaz-managed   161    FGVM010000064692 -       10.200.1.1  Local-FortiGate  My_ADOM      6.00741    7.0 MR2 (1254)
                 |- 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
```

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:** BD
**Explanation:**
The example on this slide shows that the FortiGate configuration is in sync with the latest running revision history. However, changes have been made to the device-level settings. That is why the CLI output is showing db:modified and the cond is showing as pending. After you install the changes on FortiGate, it will show db: not modified and cond:OK.
db:modified = Config changes made on FMG
cond:in sync = Latest revision history in sync with FGT running-config
cond:pending = Config changes needed to be installed

**QUESTION 22**
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:** BD
**Explanation:**
B: FortiManager uses port TCP port 443 or TCP port 4443 to connect to the Fortinet registry and download MEAs. Make sure that the port is also open on any upstream FortiGate devices.
D: FMG administrator with super user profile can enable MEAs.

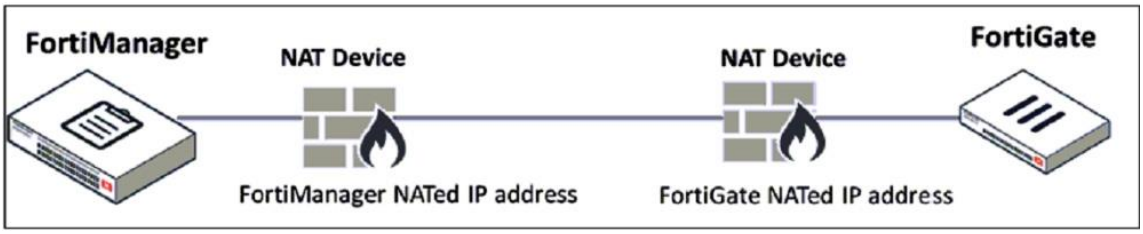
**QUESTION 23**
What does a policy package status of Never Installed indicate?

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

**Answer:** D
**Explanation:**

https://community.fortinet.com/t5/FortiManager/Technical-Tip-FortiManager-policy-package-installation-and/ta-p/195923

**QUESTION 24**
Refer to the exhibit. If both FortiManager and FortiGate are behind the NAT devices, what are the two expected results? (Choose two.)




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

**Answer:** AC

**QUESTION 25**
When an installation is performed from FortiManager, what is the recovery logic used between FortiManager and FortiGate for an FGFM tunnel?

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

**Answer:** D
**Explanation:**
If the connection fails to reestablish, FortiGate applies the unset command after 15 minutes (not configurable and not based on sock timeout values). If the connection remains down, and rollback-allow-reboot is enabled on FortiManager, FortiGate reboots to recover the previous configuration from its configuration file.

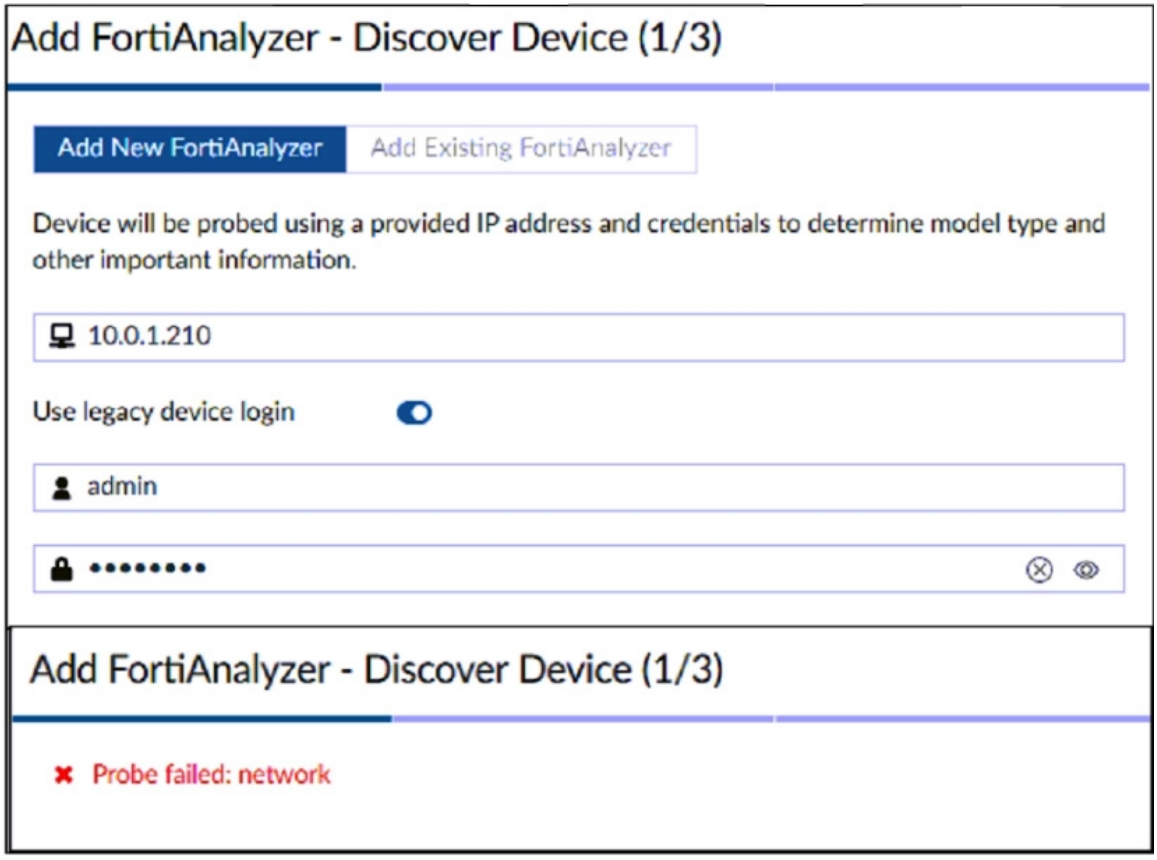
**QUESTION 26**
Which two statements about the scheduled backup of FortiManager are true? (Choose two.)

A. It can be configured using the CLI and GUI.
B. It does not back up firmware images saved on FortiManager.
C. It backs up all devices and the FortiGuard database.
D. It supports FTP, SCP, and SFTP.

**Answer:** BD

**Explanation:**
The backup contains everything except the logs, FortiGuard cache, and firmware images saved on FortiManager.
It supports FTP, SCP, and SFTP.

**QUESTION 27**
Refer to the exhibit. According to the error message, why is FortiManager failing to add the FortiAnalyzer device?




A. The administrator must use the correct user name and password of the FortiAnalyzer device.
B. The administrator must turn off the Use Legacy Device login and add the FortiAnalyzer device to the same network as FortiManager.
C. The administrator must use the Add Model Device section and discover the FortiAnalyzer device.
D. The administrator must select the FortiManager administrative access checkbox on the FortiAnalyzer management interface.

**Answer:** D
**Explanation:**
Before you add FortiAnalyzer to FortiManager, you must enable the FortiManager Administrative Access checkbox on the FortiAnalyzer management interface.
https://docs.fortinet.com/document/fortianalyzer/7.2.0/administration-guide/578841/configuring-network-interfaces

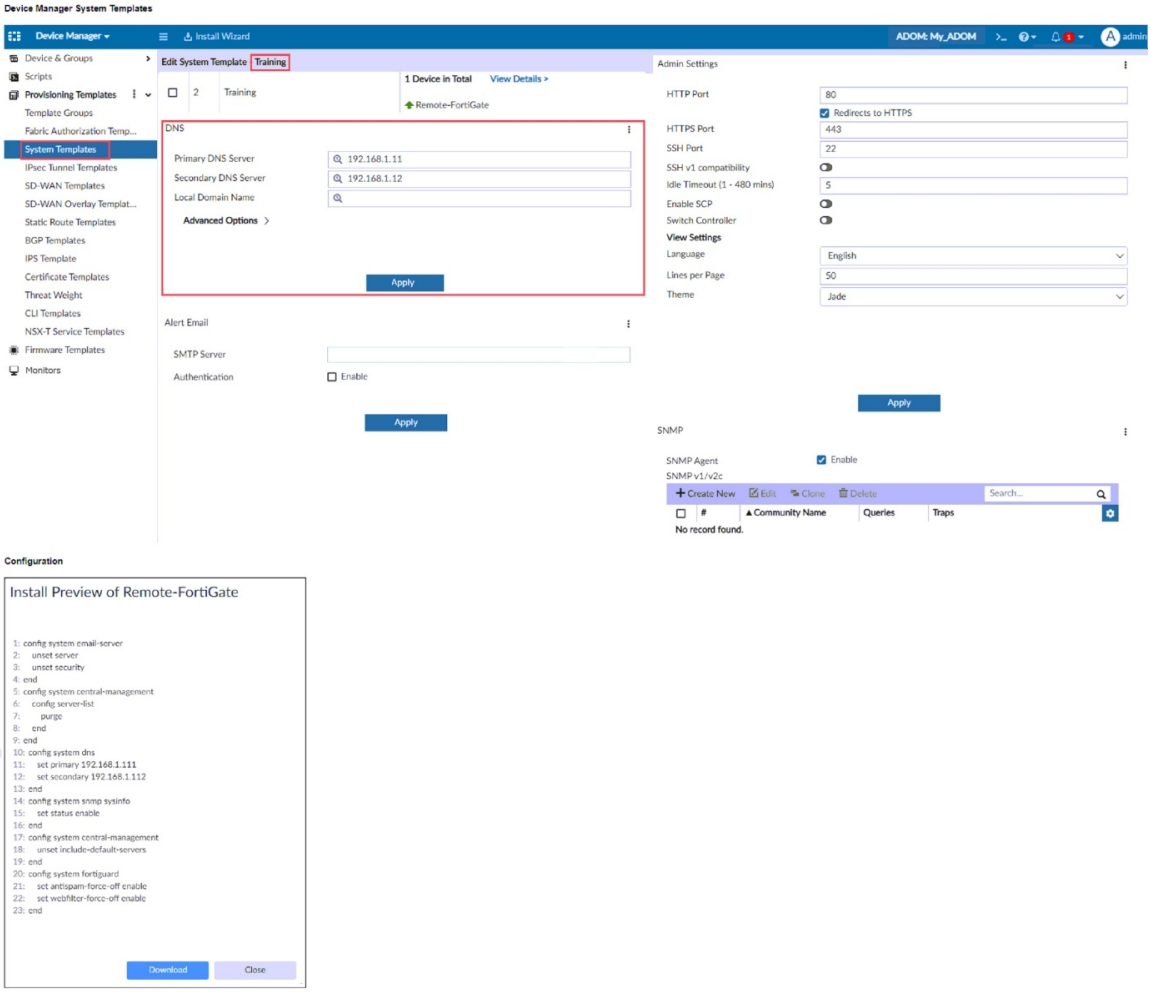
**QUESTION 28**

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

A. When FortiManager is auto-updated with configuration changes made directly on a managed device
B. When changes to the device-level database are made on FortiManager
C. When FortiManager installs device-level changes on a managed device
D. When a configuration revision is reverted to a previous revision in the revision history

**Answer:** AC
**Explanation:**
After every auto-update operation FortiManager stores the FortiGate configuration in the revision history.
Reverted changes must be installed, which creates a new revision entry.

**QUESTION 29**
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:** D
**Explanation:**
For the Install Preview, the config system central-management -> config server-list is being purged (clear all table values).
According to the FortiOS documentation, the config system central-management -> config server-list is for configuring "Additional severs that the FortiGate can use for updates (for AV, IPS, updates) and ratings (for web filter and antispam ratings) servers."
In the System Templates, those additional servers are configured on the FortiGuard Widget which doesn't appear on the screenshot provided.
If the config system central-management -> config server-list is being purged, that means the Training system template has a default FortiGuard widget settings.

**QUESTION 30**
Refer to the exhibit. Which statement is true about the FortiManager ADOM policy tab based on the API request?

```
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
```

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.

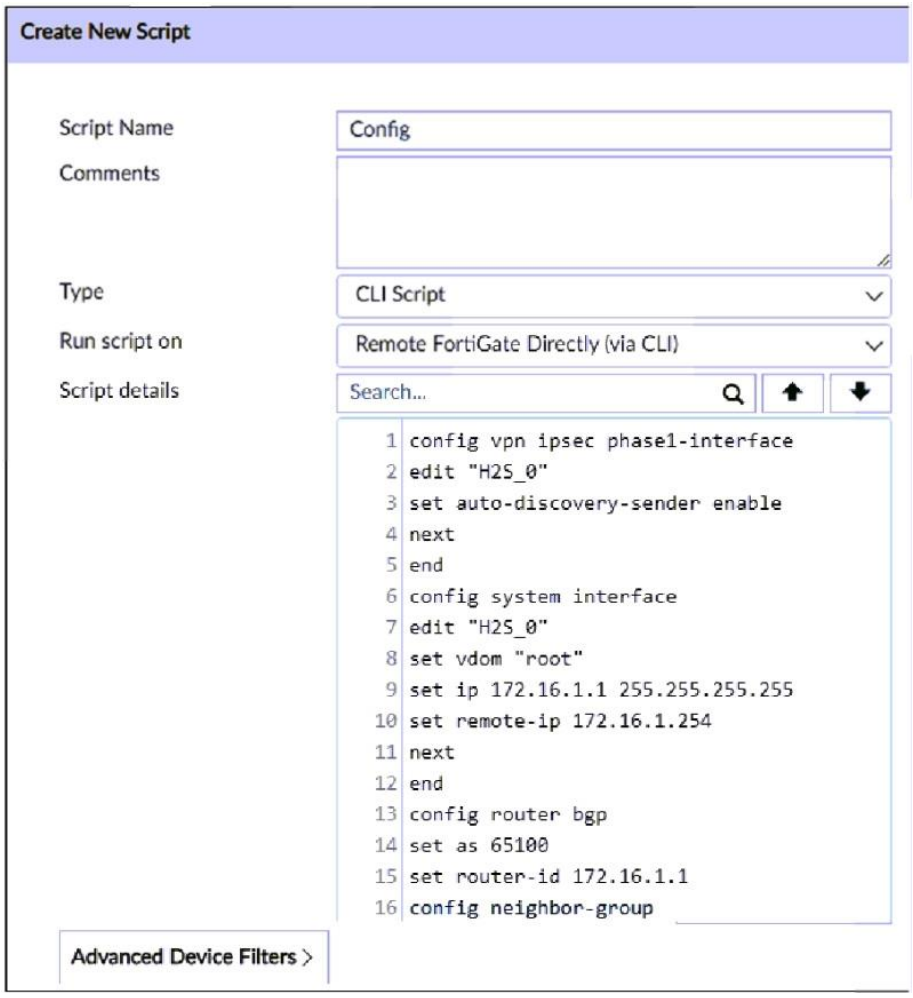
**Answer:** A

**QUESTION 31**
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:** C

**QUESTION 32**
Refer to the exhibit. What will happen if the script is run using the Remote FortiGate Directly (via CLI) option? (Choose two.)

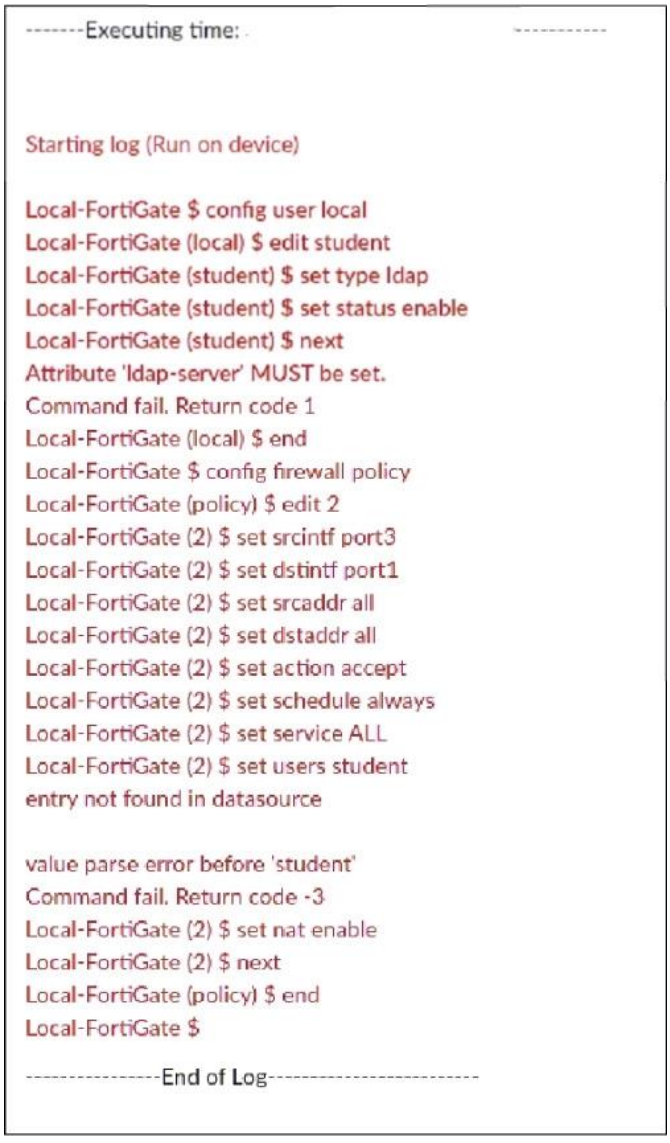



A. FortiManager provides a preview of CLI commands before executing this script on a managed FortiGate.

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:** BC
**Explanation:**
Remote FortiGate Directly (through the CLI): A script can be executed directly on the device and you don't need to install the changes using the installation wizard. As the changes are directly installed on the managed device, no option is provided to verify and check the configuration changes through FortiManager prior to executing it.

**QUESTION 33**
Refer to the exhibit. 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:** D
**Explanation:**
Since "users" is not mandatory, and all the other elements are set, the policy will be created.
Tested in lab:
Local-FG # config firewall policy
Local-FG (policy) # edit 2
new entry '2' added
Local-FG (2) # set srcintf a
Local-FG (2) # set dstintf b
Local-FG (2) # set srcaddr all
Local-FG (2) # set dstaddr all
Local-FG (2) # set action accept
Local-FG (2) # set schedule always
Local-FG (2) # set service ALL
Local-FG (2) # set users student
entry not found in datasource
value parse error before 'student'
Command fail. Return code -3
Local-FG (2) # set nat enable
Local-FG (2) # next
Local-FG (policy) # end
Local-FG # show firewall policy
config firewall policy
edit 2
set uuid 00879f84-bf81-51ee-3191-7623414c44a4
set srcintf "a"
set dstintf "b"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
set nat enable

**QUESTION 34**
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:** B
**Explanation:**
When assigning Global Policy packages to ADOMs you must chose:
- All Policy Packages: Assigns the global policy package to all policy packages.

- Specify Policy Packages to Exclude: Assigns the global policy package to all except the specified policy packages.
- Specify Policy Packages to Include: Assigns the global policy package to only the specified policy packages.

**QUESTION 35**
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:** A
**Explanation:**
When the features are enabled manually by using the System Settings module, logs are stored and FortiAnalyzer features are configured on the FortiManager.
https://docs.fortinet.com/document/fortimanager/7.2.4/administration-guide/253964/fortianalyzer-features