Fortinet.NSE6_FMG_AD-7.6.v2026-08-30.q25

Exam Code:	NSE6_FMG_AD-7.6
Exam Name:	Fortinet NSE 6 - FortiManager 7.6 Administrator
Certification Provider:	Fortinet
Free Question Number:	25
Version:	v2026-08-30
# of views:	124
# of Questions views:	250
https://www.freeqas.com/qa/Fortinet/NSE6_FMG_AD-7.6/Fortinet.NSE6_FMG_AD-7.6.v2026-08-30.q25.html	

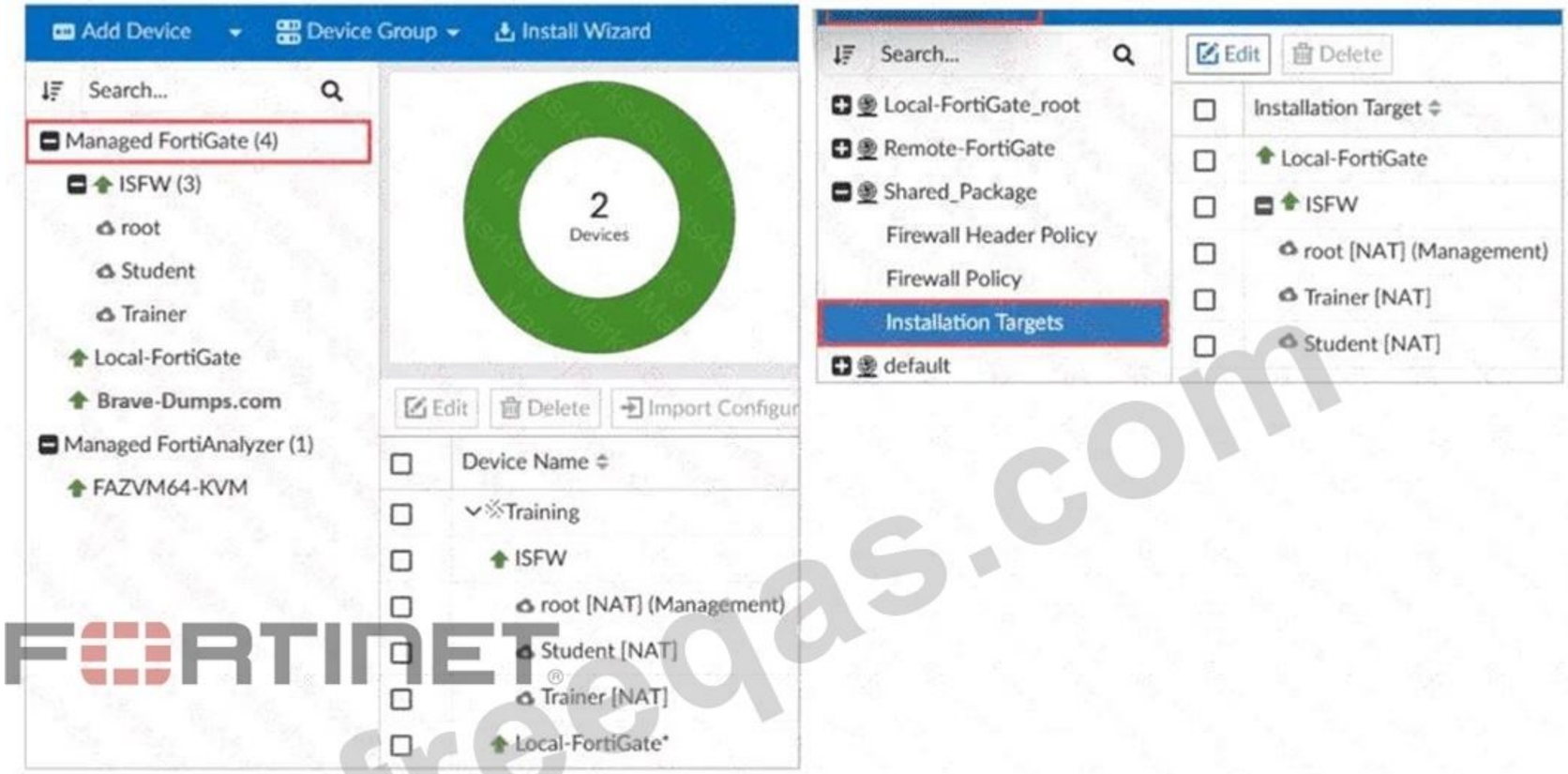
NEW QUESTION: 1
Refer to the exhibit.

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

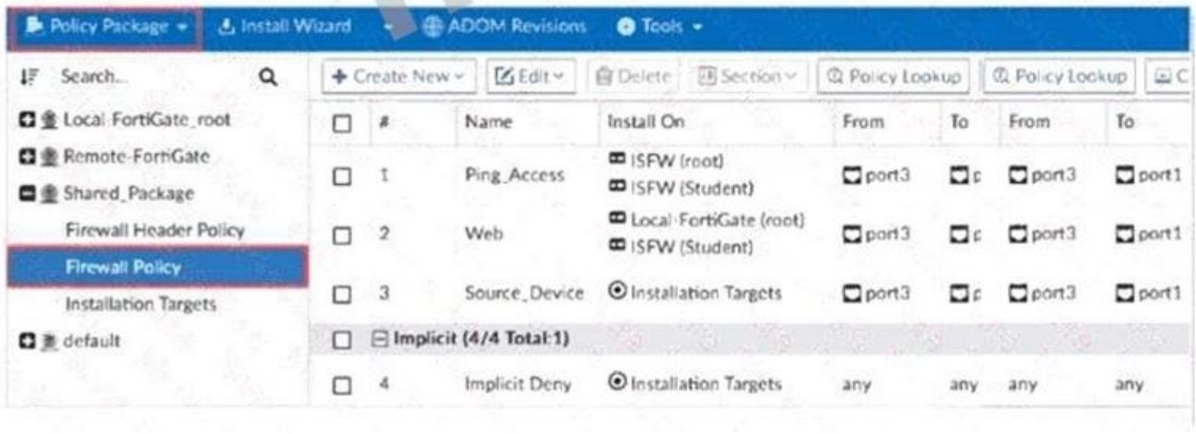

What are two results from the configuration shown in the exhibit? (Choose two.)
A. Ungraceful closed sessions will keep the ADOM in a locked state until the administrator session times out.
B. The administrator can lock policy blocks and FortiManager global ADOM.
C. The same administrator can lock more than one ADOM at the same time.
D. The administrator must have access to the ADOM to approve changes.
Answer: (SHOW ANSWER)
The command set workspace-mode normal enables Workspace (ALL ADOMs). The study guide states that in this mode "All ADOMs can be locked" and workspace mode lets administrators lock ADOMs, devices, policy packages, and objects. The lab guide then gives the exact behavior for ungraceful session closure: "If a session is not closed gracefully ... FortiManager does not close the administrator session until it times out or the session is deleted. Until this time, the ADOM remains in a locked state." That directly proves A.
C is also verified by the lab guide statement: "If an administrator locked one or more ADOMs, and then logs out of FortiManager, all of those ADOMs are unlocked." The phrase "one or more ADOMs" confirms the same administrator can lock multiple ADOMs at once.
D is a workflow mode approval concept, not workspace normal.

NEW QUESTION: 2
Refer to the exhibits.

Managed FortiGate devices



FortiManager policy package



What can you conclude, based on the configuration shown in the exhibit? Choose one answer

A. The administrator needs to retrieve the Local-FortiGate configuration to sync with the Security Fabric group, Training.

B. Policy sequence #1 will be installed on the internal segmentation firewall ISFW device root NAT and Trainer NAT VDOMs.

C. Policy sequence #3 must have devices or VDOMs listed in the Install On column; otherwise, it will cause errors.

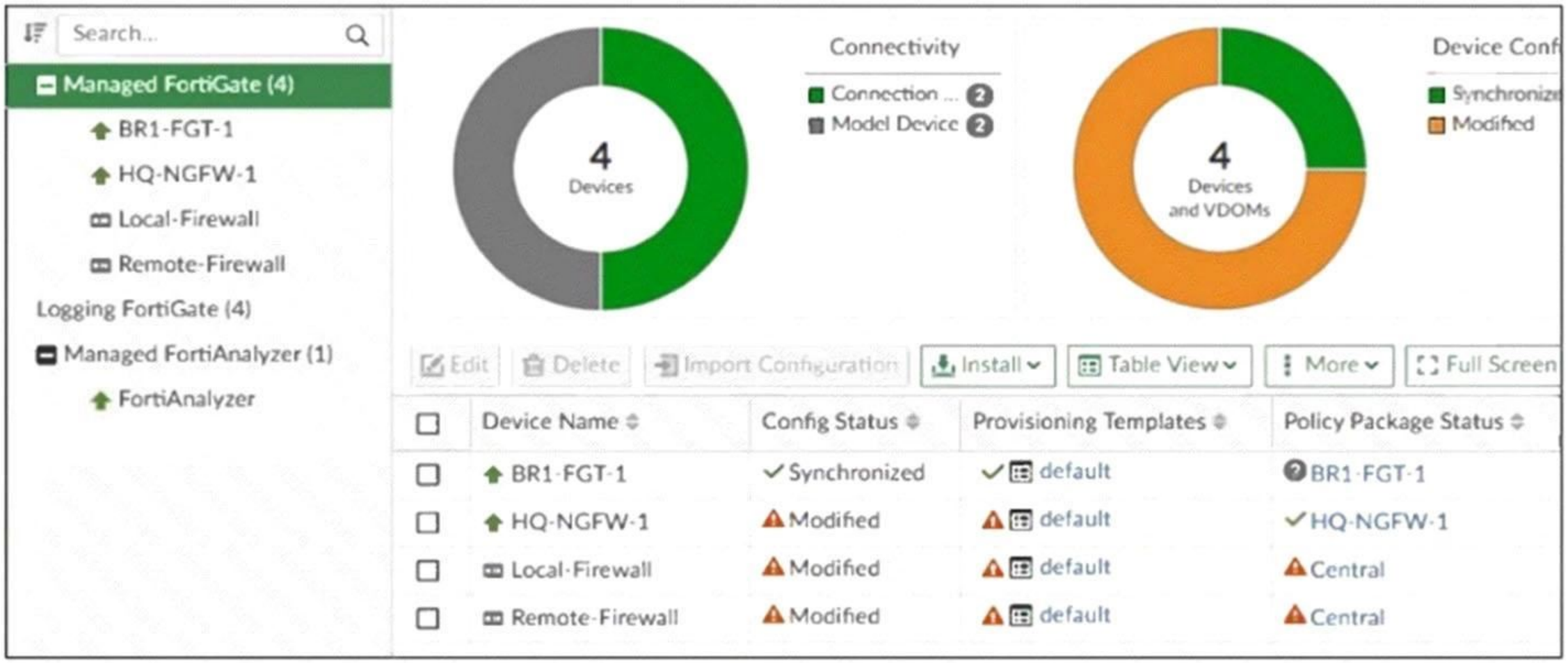
D. The global policy package will be added to the top of the ISFW policy package.
Answer: A (LEAVE A REPLY)
The best conclusion is A. From the exhibit, B is clearly incorrect because policy sequence #1 Ping_Access is targeted to ISFW root and ISFW Student, not to root NAT and Trainer NAT. Also, C is incorrect because FortiManager allows a rule to inherit Installation Targets. The study guide explains that a policy package can target one or more devices or VDOMs, and the Install On column is used only for per-rule exceptions in a shared policy package. A rule does not need explicit devices listed if it is meant to apply to the package's installation targets.
D is also incorrect because global header policies are created in the Global Database ADOM and placed at the top only when a global package is assigned. The exhibit shows a shared policy package, not a global ADOM header-policy assignment.
=========

NEW QUESTION: 3
An administrator must create a policy and install it on a FortiGate device within an ADOM in backup mode.
How can the administrator perform this task?
A. Use the Install Wizard located on the device manager.
B. Enable workflow mode to allow policy creation and approval.
C. Make sure the ADOM and FortiGate firmware versions match and use the ADOM policy package.
D. Use a FortiManager script to apply the configuration changes.
Answer: D (LEAVE A REPLY)
In backup mode, FortiManager does not directly manage policy installation via the usual ADOM policy packages; instead, administrators use FortiManager scripts to push configuration changes, including policies, to FortiGate devices.

NEW QUESTION: 4
A FortiManager administrator has moved a FortiGate device to a new ADOM, but they cannot see the policy or object configurations for that FortiGate.
What should the administrator do to see the policy or object configurations?
A. Use ADOM sync to restore the missing configurations.
B. Reset the device and add it to the new ADOM again.
C. Use ADOM shared objects to restore all missing data.
D. Import the policy package manually using the Import Configuration wizard.
Answer: (SHOW ANSWER)

NEW QUESTION: 5
Refer to the exhibits.

FortiManager device database



An administrator has been asked to install the same policies from a central policy package onto the BR1-FGT-1 firewall.
The administrator added BR1-FGT-1 as a target in the central policy package installation.
What should the administrator do when reinstalling the central policy package on the BR1-FGT-1 firewall?
A. Assign only one policy package to the firewall because FortiManager does not allow more than one policy package assigned per device at the same time.
B. Import the policy package to change the unknown status and synchronize the policy package.
C. Use the install wizard to install the central policy package on the BR1-FGT-1 firewall.
D. First resolve the modified status in the configuration and provisioning templates to allow a smooth installation.
Answer: (SHOW ANSWER)
Using the Install Wizard is the recommended method to reinstall the central policy package on the BR1-FGT-1 firewall, ensuring all settings, installation targets, and dependencies are correctly processed during installation.

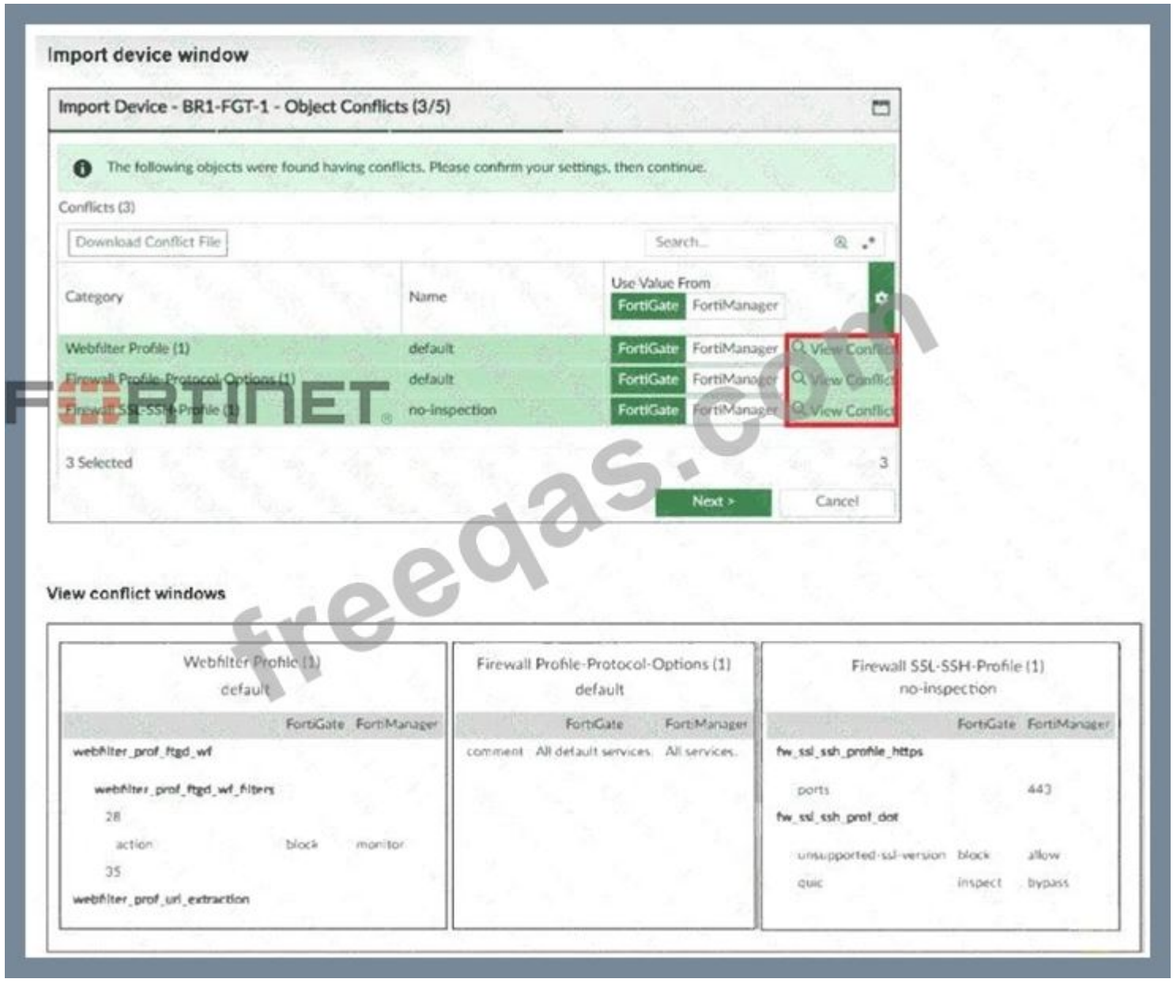
NEW QUESTION: 6
What is the purpose of ADOM revisions?
A. ADOM revisions find unused, duplicate, and unnecessary firewall policies and objects.
B. ADOM revisions show specific changes in a policy package when it is installed.
C. ADOM revisions compare previous snapshots of the Policy Package and ADOM-level objects with the device-level database.
D. ADOM revisions save the current state of all policy packages and objects for an ADOM.
Answer: D (LEAVE A REPLY)
ADOM revisions save the current state of all policy packages and objects within an ADOM, allowing administrators to track changes over time and revert to previous configurations if needed.

NEW QUESTION: 7
Refer to the exhibit.

An administrator created two new meta fields in FortiManager.
Which operation can you perform with these parameters?
A. You can add them to objects as custom attributes.
B. You can export them to be used in other ADOMs.
C. You can use them as variables in scripts.
D. You can invoke them using the $ character.
Answer: A (LEAVE A REPLY)
Meta fields in FortiManager can be added to objects as custom attributes, allowing administrators to categorize and add additional information to firewall objects for easier management and identification.

NEW QUESTION: 8
What is the best explanation of how FortiManager helps with mass provisioning?
A. It upgrades the OS of each FortiGate device.
B. It provides local FortiGuard Distribution Server (FDS) services to the network.
C. It uses templates to configure the same settings on many devices simultaneously.
D. It sends email alerts when new devices connect.
Answer: C (LEAVE A REPLY)
FortiManager helps with mass provisioning by using templates that allow administrators to configure the same settings on multiple FortiGate devices simultaneously, streamlining deployment and management.

NEW QUESTION: 9
Refer to the exhibits.



An administrator added BR1-FGT-1 to FortiManager and started importing the policy package. During the process, they saw that they need to choose values from FortiGate or FortiManager.
Which conclusion is most clearly supported by the exhibits?

A. BR1-FGT-1 does not support the SSL/SSH profile with HTTPS on port 443.

B. The administrator must match the FortiOS firmware version with the FortiManager ADOM firmware version to resolve the conflict status.

C. The default Firewall Profile-Protocol-Options object is the only profile that does not significantly affect any configuration changes on either FortiManager or FortiGate.

D. FortiManager has a different FortiGuard database compared to FortiGate BR1-FGT-1 for the QUIC protocol.

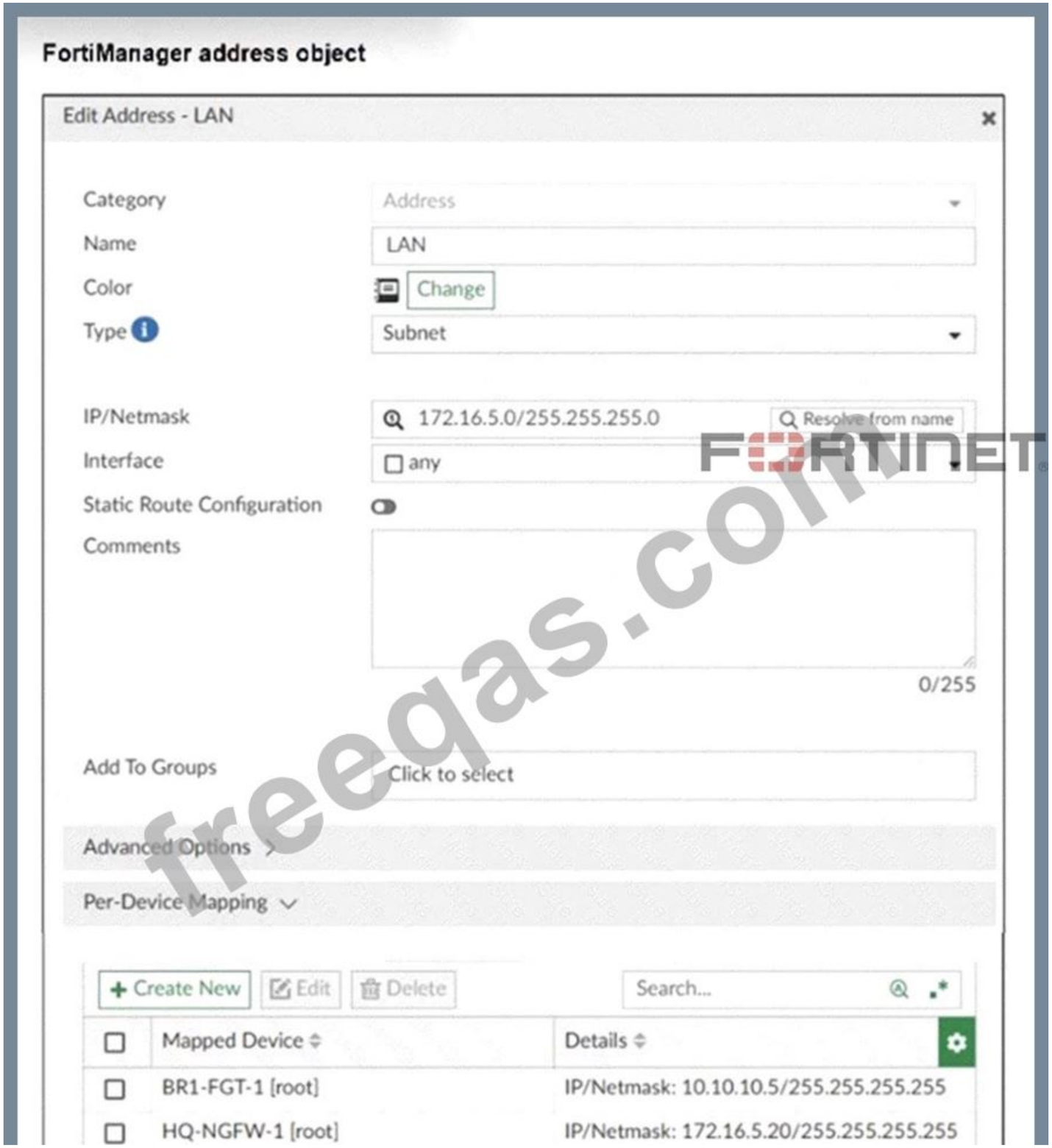
Answer: C (LEAVE A REPLY)

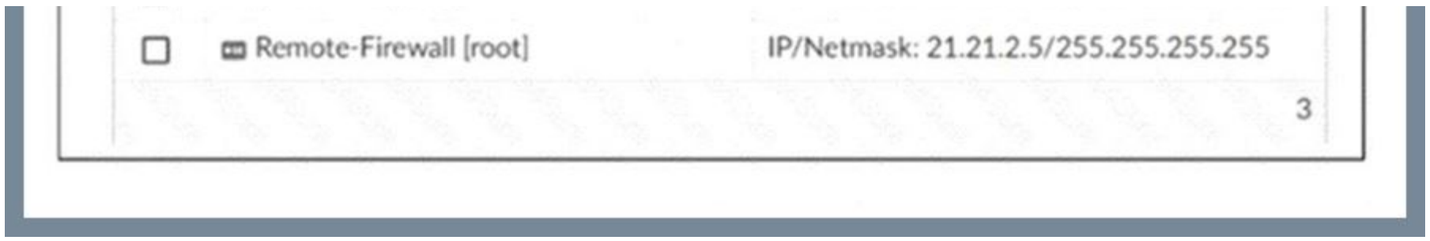
The exhibits are directly supported by the lab guide's troubleshooting section. It states: "The only profile that can be replaced is the Firewall Profile-Protocol-Options profile, because the only difference is a change in the comment field." It then explains that for the other two profiles, "Whether you accept the value from BR1- FGT-1 or FortiManager, it will cause changes on different devices." That exactly matches C. The conflict window is not primarily showing a firmware mismatch, and the guide does not say BR1-FGT-1 lacks HTTPS 443 support. It also does not describe this as a FortiGuard database mismatch for QUIC. Instead, the key point is that only the default Firewall Profile-Protocol-Options conflict is minor enough to safely take from FortiManager because the difference is only in the comment field. The web filter and SSL/SSH profiles would cause real configuration differences if replaced.

NEW QUESTION: 10

Refer to the exhibit.

FortiManager address object

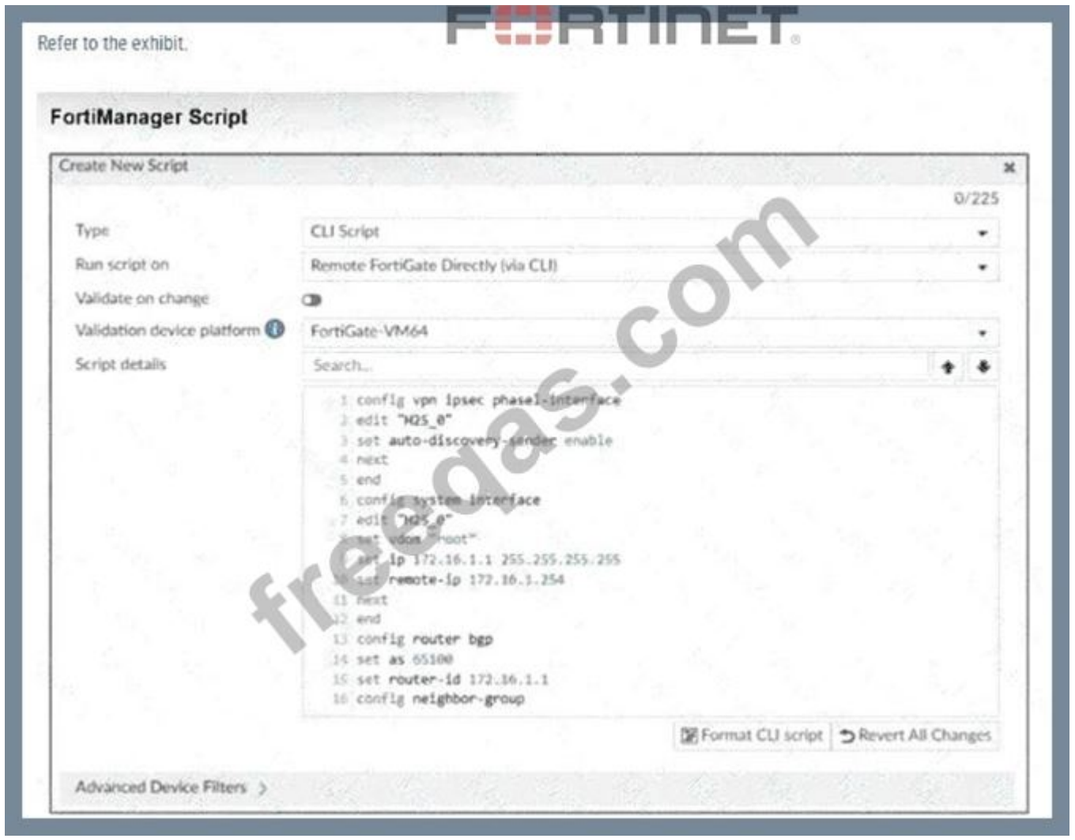




An administrator has created a firewall address object that is used in multiple policy packages for multiple FortiGate devices in an ADOM.
After the installation operation is performed, which IP/netmask will be installed on Remote-Firewall
[VDOM1] for the LAN firewall address object?
A. 21.21.2.5/255.255.255.255
B. 172.16.5.20/255.255.255.255
C. 172.16.5.0/255.255.255.0
D. 10.10.10.5/255.255.255.255
Answer: (SHOW ANSWER)
The exhibit shows the default value of the LAN address object as 172.16.5.0/255.255.255.0. It also shows Per- Device Mapping entries only for BR1-FGT-1 [root], HQ-NGFW-1 [root] , and Remote-Firewall [root]. There is no mapping shown for Remote-Firewall [VDOM1] .
The FortiManager 7.6 Administrator Study Guide gives the exact rule: "The devices in the ADOM that do not have a dynamic mapping for LAN have a default value." It also states that dynamic mappings are configured per device in the Per-Device Mapping section.
Since Remote-Firewall [VDOM1] does not have its own mapping entry, it will use the object's default value, which is 172.16.5.0/255.255.255.0.

NEW QUESTION: 11
A FortiManager administrator opens the revision history and choose to revert to a previous version.
What will this action do to the current device configuration?
A. It will trigger an unknown device-level database status, and the administrator will have to import a policy package to sync.
B. It will trigger a conflict status if it is using any provisioning template, and the administrator will have to install changes.
C. It will revert both configurations: device-level database and policy layer database.
D. It will modify the device-level database.
Answer: D (LEAVE A REPLY)
The correct answer is D. The FortiManager 7.6 Administrator Study Guide states: "You can revert to a previous configuration revision" and "Reverts only the device database to the previous revision". It also states
"Does not revert policies and objects-you must import them" and "You must install reverted changes on FortiGate." This exactly means a revert operation changes the device-level database on FortiManager, not the policy layer database. The guide further clarifies: "Performing a revert operation followed by an installation only reverts device-level changes and does not revert policy packages." So C is incorrect because both layers are not reverted together. A and B are also incorrect because the documented and verified effect is specifically a modification of the device database, followed by install and, if needed, policy re-import for synchronization.
=========

NEW QUESTION: 12
Refer to Exhibit:



Which two actions will occur if you run the script using the Remote FortiGate Directly via CLI option?
Choose two answers
A. FortiManager will provide 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-updated the FortiManager device-level database.
D. You will have to install these changes using the Install Wizard.
Answer: B,C (LEAVE A REPLY)
The correct answers are B and C. The FortiManager 7.6 Administrator Study Guide explicitly states: "Scripts that you run directly on remote devices also cause automatic updates and create a revision history." This exact extract proves both results: FortiManager creates a new revision history and the device status becomes Auto- Updated, meaning the FortiGate change is automatically reflected in the FortiManager device-level database.
The lab guide also distinguishes this from database-targeted scripts by stating: "You must perform an installation if you run a script on a device database, policy package, or ADOM database." That wording excludes Remote FortiGate Directly via CLI, so D is incorrect.
A is also incorrect because direct remote execution does not use the install preview workflow; preview and validation are tied to Install Wizard operations, not direct CLI execution.
=========

NEW QUESTION: 13
Refer to the exhibit.

FortiManager script

Which two results occur if you run the script using the Device Database option? (Choose two.)

A. The device Config Status is tagged as Modified.

B. The script history shows the successful installation of the script on the remote FortiGate.

C. The successful execution of a script on the Device Database creates a new revision history.

D. The administrator must install these changes on a managed device using the Install Wizard.

Answer: A,D (LEAVE A REPLY)

Running a script on the Device Database marks the configuration as modified but does not immediately apply changes to the device.

The administrator must use the Install Wizard to push and install these changes from the Device Database onto the managed device.

NEW QUESTION: 14

Refer to the exhibit.

FortiManager CLI output

```
FortiManager # execute top
top - 13:08:23 up 1 day,  1:01,  0 users,  load average: 2.40, 3.19, 3.34

Tasks: 188 total,   2 running, 186 sleeping,   0 stopped,   0 zombie

%Cpu(s): 15.4 us,  7.7 sy,  0.0 ni, 76.9 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st

MiB Mem : 7955.5 total,   2235.6 free,  2895.6 used,  2824.1 buff/cache

MiB Swap: 2048.0 total,   2048.0 free,     0.0 used.  4011.0 avail Mem

  PID USER      PR  NI    VIRT    RES  %CPU  %MEM     TIME+ S COMMAND
 1163 root      20   0   17.6m   2.1m   7.1   0.1   0:00.05 R top
    1 root      20   0  602.2m  14.9m   0.0   0.7   0:11.67 S /bin/initXXXXXXXXXX
    2 root      20   0    0.0m   0.0m   0.0   0.0   0:00.00 S [kthreadd]
 1462 root      20   0  303.2m 248.0m   0.0   3.1   0:14.72 S fwmsvrd
 1463 root      20   0  288.2m 232.3m   0.0   2.9   0:16.47 S fgdlinkd
 1465 root      20   0  383.7m 328.0m   0.0   4.1   0:15.26 S fgdsvr
 1467 root      20   0   84.0m  23.6m   0.0   0.3   0:00.06 S /bin/fgdhttpd
 1468 root      20   0   63.9m  13.1m   0.0   0.2   0:13.00 S fgdupd
 1469 root      20   0   63.5m  12.6m   0.0   0.2   0:00.07 S fmtr_svrd
 1470 root      20   0    6.3m   3.5m   0.0   0.0   0:00.09 S /bin/webconsoled
 1471 root      20   0  996.4m 850.6m   0.0  10.7   0:00.01 S srchd
 1475 root      20   0  996.4m 170.6m   0.0   1.9   0:00.00 S fclinkd
```

What percentage of the available RAM is being used by the process in charge of downloading the web and email filter databases from the public FortiGuard servers?

A. 1.5

B. 3.1

C. 4.1

D. 2.9

Answer: D (LEAVE A REPLY)

The correct answer is D. The FortiManager 7.6 Administrator Study Guide gives the exact extract under Web Filter and Email Filter: "fgdlinkd - Responsible for downloading web filter and email filter databases".

The same study guide section explains that the execute top command displays real-time CPU and RAM usage, and the %MEM column shows the memory percentage used by each process.

In the exhibit, the line for fgdlinkd shows %MEM 2.9. Therefore, the process responsible for downloading the web and email filter databases is using 2.9% of RAM. That matches option D exactly. The other values belong to different processes, such as fgdsvr and other FortiGuard-related daemons, but not the downloader process identified in the study guide.

=========

NEW QUESTION: 15

Push updates are failing on a FortiGate device located behind a network address translation (NAT) device?

Which two settings should the administrator check to correct this problem? (Choose two.)

A. Make sure the NAT device IP address and the correct ports are configured on FortiManager.

B. Make sure FortiGuard updates and web service are enabled on the FortiGuard service interface.

C. Make sure the virtual IP address and the correct ports are configured on the NAT device.

D. Make sure the Bind to IP address option on the FortiGuard service interface is set to the virtual IP address from the NAT device.

Answer: A,C (LEAVE A REPLY)

FortiManager must have the NAT device ' s IP address and correct ports configured to communicate properly with the FortiGate behind NAT.

The NAT device must have the correct virtual IP address and ports configured to allow push updates to reach the FortiGate device.

NEW QUESTION: 16

What allows FortiManager to run CLI scripts on FortiGate devices without prompting for SSH authentication each time?
A. FortiGate devices using the legacy login method.
B. The secure management tunnel between FortiManager and FortiGate devices.
C. The script using the Remote FortiGate Directly via CLI option.
D. The script on the FortiManager device database.
Answer: (SHOW ANSWER)
The correct answer is B. The FortiManager 7.6 Administrator Study Guide explicitly states: "CLI scripts use the FGFM tunnel and the FGFM tunnel is authenticated using the FortiManager and FortiGate serial numbers." It also states: "Tcl scripts do not run through the FGFM tunnel like CLI scripts do. Tcl scripts use SSH to tunnel through FGFM and they require SSH authentication to do so." This is the exact reason CLI scripts can run without prompting for SSH authentication every time: they use the existing secure FGFM management tunnel, not a separate interactive SSH login. The FGFM section of the study guide also confirms that this is a secure communication tunnel established between FortiManager and managed FortiGate devices.
So the enabler is not legacy login, script location, or the "Remote FortiGate Directly" option by itself. It is the FGFM secure management tunnel.

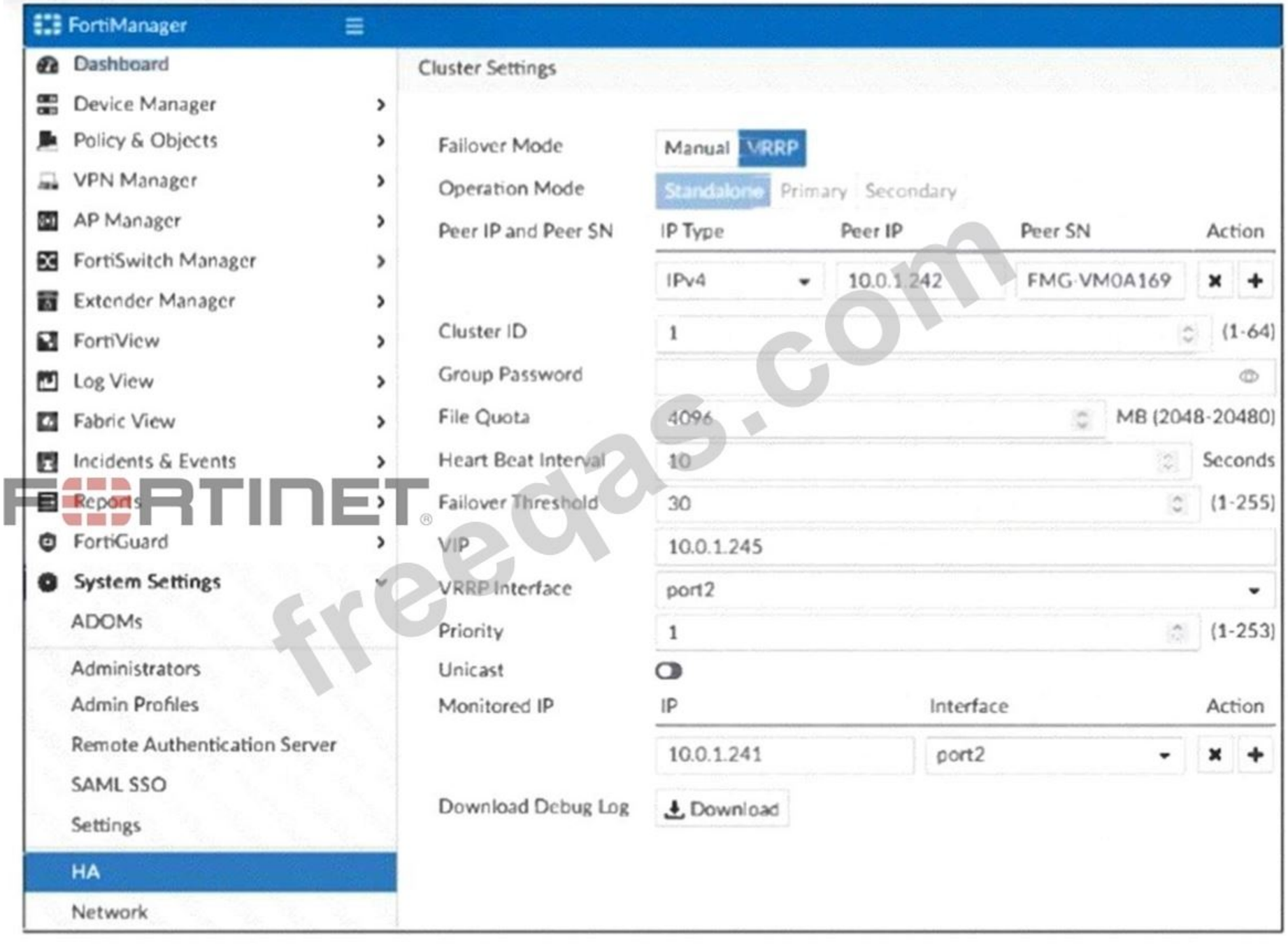
NEW QUESTION: 17
If one of the secondary FortiManager devices fails, which action must be performed to return the FortiManager HA manual mode to a working state?
A. The FortiManager high availability HA state transition is transparent to administrators and does not require any reconfiguration.
B. Run a sanity check on the failed device to make sure HA heartbeat packets are using TCP port 5199.
C. Manually promote one of the working secondary devices to the primary role.
D. Remove the peer IP of the failed device on the primary device.
Answer: (SHOW ANSWER)
The correct answer is D. In FortiManager HA manual mode, the study guide explains what happens when members change: if the primary fails, you must manually promote a secondary and repoint the others, but that is not this scenario. For a failed secondary, the relevant exact extract is: "if you remove a secondary member from the HA configuration, the primary FortiManager removes the secondary serial number from the central management configuration of FortiGate, and updates the managed FortiGate devices immediately." Operationally, in the HA configuration, removing that failed secondary means deleting its HA peer entry from the primary, which corresponds to removing the failed device's peer IP. A is false because manual HA is not transparent in this case. B is only a diagnostic detail. C applies when the primary fails, not a secondary.
=========

NEW QUESTION: 18
Company policy dictates that any time a change is made to a policy package on FortiManager an ADOM revision is created before the change installed, and that revision is held for a minimum of 90 days.
Over the past three months, each installed change has resulted in several unused policies and duplicate objects.
The FortiManager administrator plans to upgrade the FortiGate devices and then upgrade the FortiManager ADOM from version 7.4 to 7.6.
Which action can the administrator take to avoid slow ADOM upgrades?
A. Check and repair the global configuration database before upgrading.
B. Export firewall policies to Excel, delete them on the ADOM. then reimport them after upgrading the ADOM.
C. Find unused firmware templates, then delete them before upgrading.
D. Limit ADOM revisions before upgrading.

Answer: D (LEAVE A REPLY)
Limiting ADOM revisions reduces the number of stored historical configurations, which helps avoid performance degradation and slow ADOM upgrades caused by a large volume of revisions.

NEW QUESTION: 19
Refer to the exhibit.

FortiManager cluster settings



If the monitored interface for the primary FortiManager device fails, what must you do to maintain high availability (HA)?

A. The FortiManager HA failover is transparent to administrators and does not require any additional action.

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

C. Reconfigure the primary device to remove the peer IP address of the failed device from its configuration.
D. Check the integrity database of the primary device to force a secondary device to become the new primary with all active interfaces.
Answer: A (LEAVE A REPLY)
In a FortiManager HA cluster configured with VRRP failover, the failover process is automatic and transparent to administrators. If the monitored interface on the primary device fails, the secondary device takes over without requiring manual intervention to maintain HA.

NEW QUESTION: 20
A FortiManager administrator has moved a FortiGate device to a new ADOM, but they cannot see the policy or object configurations for that FortiGate.
What should the administrator do to see the policy or object configurations?
A. Use ADOM shared objects to restore all missing data.
B. Reset the device and add it to the new ADOM again.
C. Import the policy package manually using the Import Configuration wizard.
D. Use ADOM sync to restore the missing configurations.
Answer: (SHOW ANSWER)
The correct answer is C. The FortiManager 7.6 Administrator Study Guide gives the exact extract: "If you need to move a device from one ADOM to another, run the Import Configuration wizard to import the policy package into the new ADOM." It also states: "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." That is exactly why the administrator cannot see the policy and object configuration after the move: the device itself moved, but its shared policy package and objects did not automatically move with it. The required corrective action is to manually import the policy package into the new ADOM using Import Configuration. Options A, B, and D are not the documented remedy in the uploaded FortiManager sources.
=========

NEW QUESTION: 21
An administrator suspects that the Collector Agent is not forwarding login events to FortiGate.
What is the most effective troubleshooting step?
A. Verify if DC agent is enabled on the FortiGate.
B. Restart the domain controller to refresh authentication services.
C. Verify if FortiGate is set to use LDAP authentication instead of FSSO.
D. Check if TCP port 8000 is open between the collector agent and FortiGate.
Answer: (SHOW ANSWER)
This point is not covered in the uploaded FortiManager 7.6 study guide, so the answer is based on Fortinet's official FSSO documentation. Fortinet documents that in FSSO Collector Agent deployments, the FortiGate connects to the Collector Agent on TCP port 8000 by default, and if a different port is not configured, that is the port that must be reachable. Fortinet also explains that the DC agents monitor user logon events and pass the information to the Collector Agent, which stores the information and sends it to the FortiGate.
So, when login events are not reaching FortiGate, the most effective first troubleshooting step is to verify connectivity on TCP 8000 between the Collector Agent and FortiGate. Options A, B, and C are less direct and do not test the actual transport path used by the Collector Agent to send FSSO information to FortiGate.

NEW QUESTION: 22
An administrator configures a new BGP peer in the FortiManager device-level database of FortiGate. They reinstall the policy package to the managed FortiGate device without any errors. However, when the administrator logs in to FortiGate, they do not see the BGP configuration changes.
What is the most likely reason why FortiManager did not push the BGP peer changes to FortiGate?
A. The administrator must run a sanity check on FortiManager to make sure the database is not corrupted.
B. Fortigate has a BGP template assigned on the FortiManager database.

C. The administrator must use the Install Wizard and select Install device settings only to push BGP settings
D. The FortiGate firmware version is different from the FortiManager ADOM version.
Answer: B (LEAVE A REPLY)
If a BGP template is assigned to the FortiGate device on FortiManager, device-level BGP configurations made directly in the device-level database are overridden by the template settings, so the changes do not get pushed to the device.

NEW QUESTION: 23
What are two outcomes of ADOM revisions? Choose two answers.
A. ADOM revisions can save the current state of the entire ADOM.
B. ADOM revisions do not increase the size of configuration backups.
C. ADOM revisions can save the current state of all policy packages and objects for an ADOM.
D. ADOM revisions appear in the Install Policy and Package Settings section of the install wizard.
Answer: (SHOW ANSWER)
The correct answers are A and C. The FortiManager 7.6 Administrator Study Guide states: "An ADOM revision creates a snapshot of all policy and object configurations for the ADOM". The lab guide says the same thing in practical terms: "An ADOM revision creates a snapshot of the policy and object configuration for the ADOM" and that these revisions are useful for comparing differences and reverting to a previous revision.
Because the revision is a snapshot of the ADOM's policy-and-object state, it saves the current ADOM policy
/object state, which supports A and directly proves C. B is false because the study guide warns: "ADOM revisions can significantly increase the size of the configuration backup files." D is not supported by the uploaded sources.
=========

NEW QUESTION: 24
The administrator uses FortiManager to push a CLI script using the Remote FortiGate Directly (via CLI) option to configure an IPsec VPN. However, when running the script, the administrator receives the following error:
config vpn ipsec phase2-interface [parameter(s) invalid. detail: object mismatch] What must the administrator do to resolve the script error and successfully apply the IPsec configuration?
A. Add the end command after finishing the IPsec phase 1-interface configuration block.
B. Use IPsec templates to deploy provisioning templates.
C. Add a second config vpn ipsec phase2-interface block without linking it to phase1.
D. Run the script using the policy package or ADOM database method.
Answer: D (LEAVE A REPLY)
Running the script through the policy package or ADOM database method allows FortiManager to properly interpret object relationships and dependencies in the IPsec configuration, preventing object mismatch errors when pushing complex VPN settings directly via CLI.
When a script is run using Remote FortiGate Directly via CLI, FortiManager sends the commands straight to the FortiGate and does not preview or validate dependent objects first. The study guide also explains that scripts containing ADOM-level objects or dynamic mappings must be executed on the Policy Package or ADOM Database, then installed through the installation workflow. That matches this IPsec error scenario, where phase2-interface is referencing an object relationship that FortiManager cannot properly validate in direct CLI mode. Therefore, the administrator should run the script on the policy package or ADOM database method, then install it.
Option A addresses only one possible syntax issue. B is a valid deployment approach in general, but it is not what the question asks as the direct fix for this script execution error. C is incorrect and would not resolve the object dependency mismatch.

NEW QUESTION: 25
Refer to the exhibit.

FortiManager—HQ-NGFW-1 install preview

Install Preview of HQ-NGFW-1

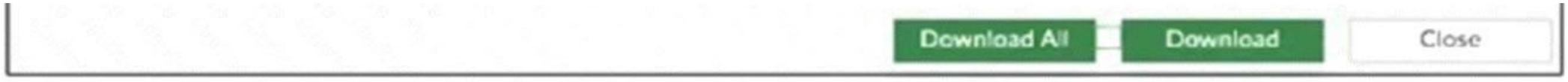
Assigned Devices: HQ-NGFW-1

HQ-NGFW-1

Search...

```
--- Preview result ---
config system central-management
    config server-list
        edit 1
            set server-type update rating
        next
    end
end
config vpn certificate ca
    edit "root_CA3"
        set ca "-----BEGIN CERTIFICATE-----
```


MIIDUzCCAjugAwIBAgIgQTlFOTUwQzBGNTIxNjlGNkUwRDcwN0JGNjY2NzI0Qzkw
DQYJKoZIhvcNAQEFBQAwKzEhMBQGA1UEChMNRm9ydGluZXQgTHRkLjERMA8GA1UE
AxMIRm9ydGluZXQwHhcNMjQxMDA0MTgwNDQ1WhcNMzQxMDA5MTgwNDQ1WjArMRYw
FAYDVQQKEw1Gb3J0aW5ldCBMdGQuMREwDwYDVQQDEwhGb3J0aW5ldDCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ/MKHOHuDNwd2yJTQpdm6uubolWTUlh
rHKolBxcuDajYEJiW8Ab5IIipE/noqR7X+xo0BJZLxuuyC9dmSgQKZSFAXUXaNkS
BVMjlzeMgwcAr5CtEQ/aFg/ZhU/ZRvjb0mpAs2dOzy1u/cCenq9B7wwNfTCfJ3Fj
zbifh33nRr+zg/Sr/wzynicqIada7TS9F+/V4z44ZD8HHD3mBztiUU3OIiqK+HJo
unNWYSdka8lIMW+J39ZXS2Swp9NyrmqcA3nzGb/DfO9eUdLlrvmAh3xpzuDcD4Od
e3Ff8P82cgS36NJ3SK/GSfEml/wMOPS/vPuc6elI6gVmv+d8HB40TA0CAwEAAaNj
MGEwHQYDVR0OBBYEFAoH8wIfafmV8ABgObY9VhxETjTsMB8GA1UdIwQYMBaAFAoH
8wIfafmV8ABgObY9VhxETjTsMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQD
AgGGMA0GCSqGSIb3DQEBBQUAA4IBAQA8AjIaQJCpbXxqzi/jG7JjqIVcu28qt4Zx
PrBeUwZJwSwRuiCVGMFsN6agU0QwUle5Gn508vEiQNeyIrWVLb4+f4qeg0Iq6PmD



An administrator assigned a new policy package to FortiGate HQ-NGFW-1. In the installation preview, they noticed some settings they did not modify and are unsure about the changes.
Based on the exhibit, which two things will happen if they continue with the installation? (Choose two.)
A. FortiGate HQ-NGFW-1 can use FortiManager firmware templates to upgrade firmware and ratings.
B. FortiGate HQ-NGFW-1 can contact the FortiManager acting as FortiGuard Distribution Server (FDS) to download FortiGuard updates.
C. FortiGate HQ-NGFW-1 will use the root_CA3 certificate in firewall address objects or policies.
D. FortiManager will install the CA certificate named root_CA3 to authenticate FortiGate-to-FortiManager communication protocol (FGFM) tunnel connections with FortiGate HQ- NGFW-1.
Answer: (SHOW ANSWER)
The configuration includes a server-list with server-type set to " update rating, " which enables FortiGate HQ- NGFW-1 to contact FortiManager as a FortiGuard Distribution Server (FDS) for FortiGuard updates.
The installation includes a root_CA3 certificate, which FortiManager will install on FortiGate HQ-NGFW-1 to authenticate FGFM tunnel connections between the devices.