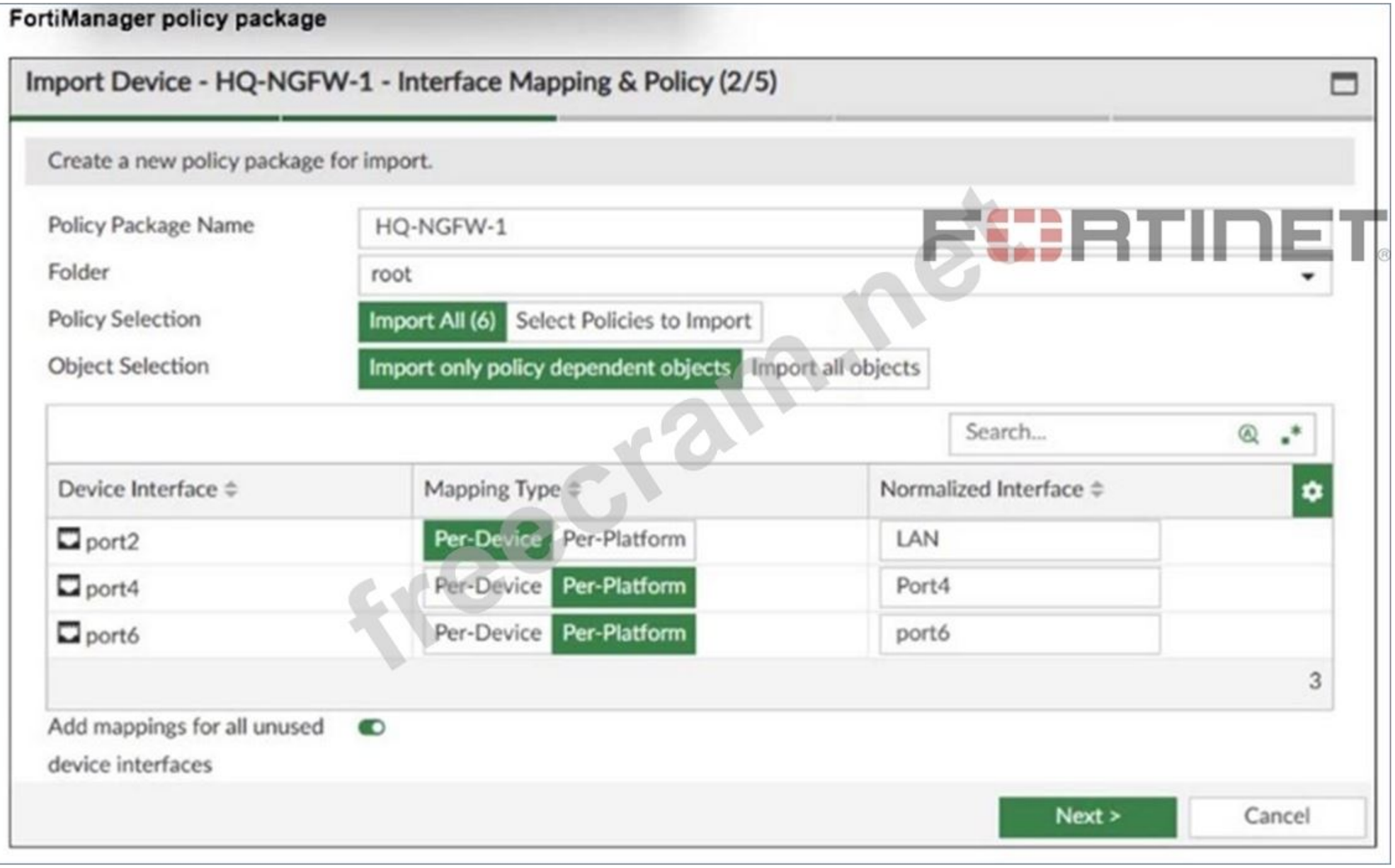
Fortinet.FCP_FMG_AD-7.6.v2026-07-10.q29

Exam Code:	FCP_FMG_AD-7.6
Exam Name:	FCP - FortiManager 7.6 Administrator
Certification Provider:	Fortinet
Free Question Number:	29
Version:	v2026-07-10
# of views:	105
# of Questions views:	317
https://www.freecram.net/torrent/Fortinet.FCP_FMG_AD-7.6.v2026-07-10.q29.html	

NEW QUESTION: 1
Refer to the exhibit.

FortiManager policy package



An administrator added a FortiGate device to FortiManager with the default object settings at the ADOM layer.
What can you conclude from the import policy package process of the HQ-NGFW- 1 device?

A. The administrator must select Per Platform for all interfaces to correctly detect all interfaces from HQ- NGFW-1.
B. The administrator must manually create the port4 interface on the ADOM layer to avoid import policy errors.
C. FortiManager will create LAN, port4, and port6 as normalized interfaces at the ADOM layer.
D. FortiGate may not work as expected when the administrator does not import all objects.

Answer: (SHOW ANSWER)

The import process shows that FortiManager will create normalized interfaces named LAN, port4, and port6 at the ADOM layer, mapping them to the corresponding device interfaces based on the import settings.

NEW QUESTION: 2

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: (SHOW ANSWER)
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: 3
Which FortiGate configuration settings is part of an ADOM-level database on FortiManager?
A. NSX-T service template
B. Security template
C. Routing
D. SNMP
Answer: B (LEAVE A REPLY)
The best verified answer is B . The FortiManager 7.6 Administrator Study Guide shows that the ADOM Layer contains Policy and Objects , and specifically states: "Policy & Objects: Centralize the management of firewall policies, objects, and security profiles, among others." Because security-related policy settings belong to the Policy and Objects layer, they are part of the ADOM-level database .
By contrast, Routing and SNMP are treated as device-level settings . The lab guide shows Routing under the device/network configuration view, and SNMP as a setting in the system template that "pushes configuration changes to the device level." Also, provisioning templates such as NSX-T service are listed as having precedence over device-layer configurations , which further indicates they are not the Policy and Objects ADOM database answer here.
=========

NEW QUESTION: 4
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: 5

FortiGate is integrated with FortiAnalyzer and FortiManager.
When creating a firewall policy, which attribute must an administrator include to enhance functionality and enable log recording on FortiAnalyzer and FortiManager?
A. Policy ID
B. Log ID
C. Universally Unique Identifier
D. Sequence ID
Answer: (SHOW ANSWER)
The correct answer is C . The uploaded FortiManager 7.6 Administrator Lab Guide gives the exact extract:
"FortiManager will update the universally unique identifiers (UUID) without deleting other configurations" and "UUIDs on both FortiGate and FortiManager are critical for ensuring the unique identification, consistency, and correct management of firewall policies across multiple devices and configurations. They provide a reliable and immutable reference for policies."
The same source also shows administrators enabling UUIDs in Traffic Log on FortiGate log settings, which supports the logging and policy-correlation use case with FortiAnalyzer/FortiManager.
So the attribute that improves policy identification and logging correlation is the Universally Unique Identifier , not Policy ID, Log ID, or Sequence ID.
=========

NEW QUESTION: 6
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: (SHOW ANSWER)
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: 7
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: 8
Which FortiGate configuration settings is part of an ADOM-level database on FortiManager?
A. Routing
B. NSX-T service template
C. SNMP
D. Security template
Answer: (SHOW ANSWER)

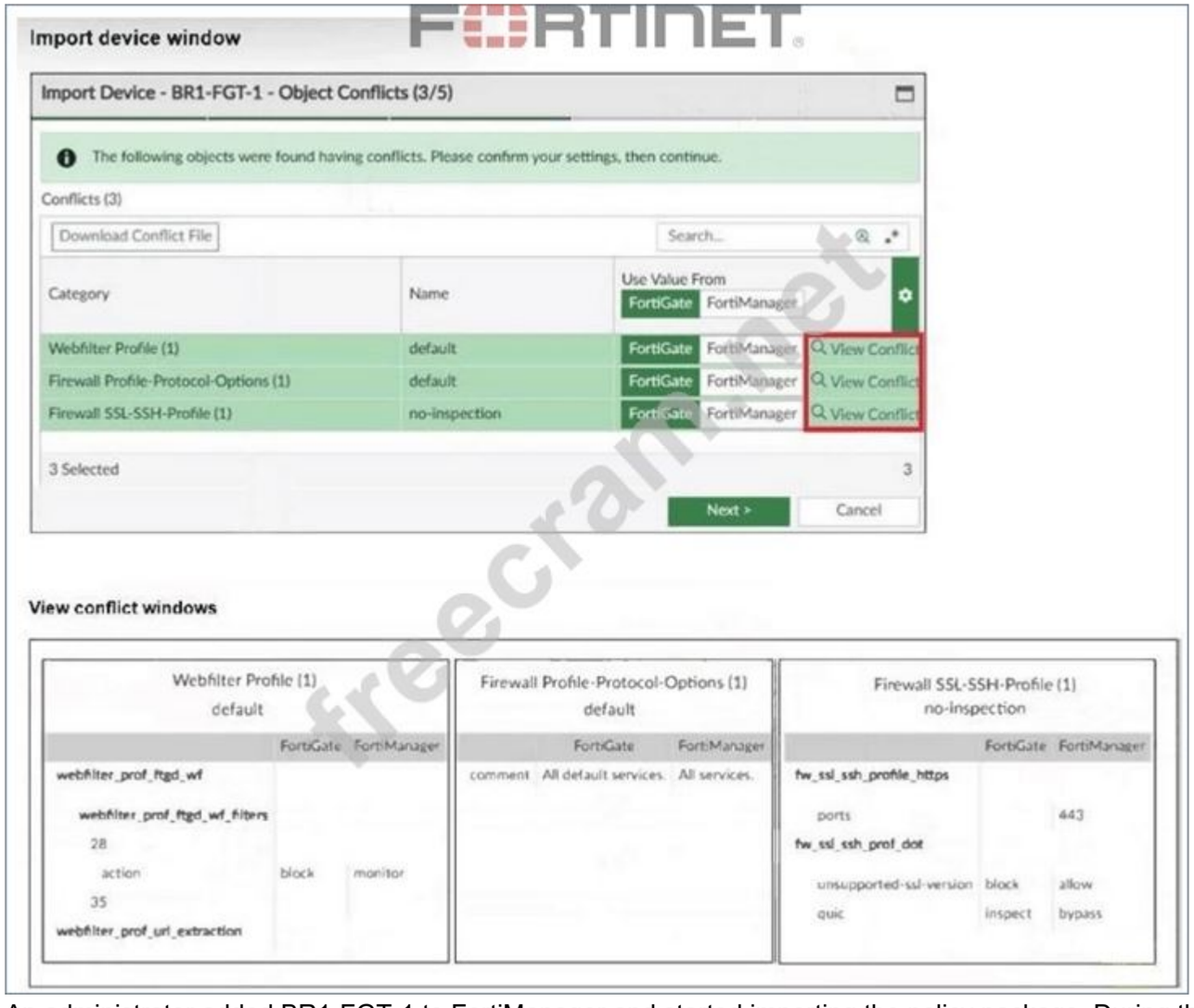
NEW QUESTION: 9
An administrator must create a policy and install it on a FortiGate device within an ADOM in backup mode.
How can the administrator perform this task?
A. Use the Install Wizard located on the device manager.
B. Enable workflow mode to allow policy creation and approval.
C. Make sure the ADOM and FortiGate firmware versions match and use the ADOM policy package.
D. Use a FortiManager script to apply the configuration changes.
Answer: (SHOW ANSWER)
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: 10
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: 11
Which two conditions trigger FortiManager to create a new revision history? (Choose two.)
A. When FortiManager installs device-level changes on a managed device

B. When changes to the device-level database are made on FortiManager
C. When FortiManager is auto-updated with configuration changes made directly on a managed device
D. When a provisioning template is assigned to a managed device on the device-level database
Answer: (SHOW ANSWER)
The correct answers are A and C . The FortiManager 7.6 Administrator Study Guide gives the exact extract:
"FortiManager creates a configuration revision when: FortiGate is added to FortiManager, Device changes are installed from FortiManager, FortiGate configuration is retrieved from FortiManager, A local change on FortiGate causes an automatic update" .
This exactly proves A , because device changes are installed from FortiManager , and C , because a local change on FortiGate causes an automatic update . The guide also states: "By default, all changes made on a managed FortiGate device are automatically updated on FortiManager and reflected in revision history" .
B and D only modify the FortiManager device-level database status to Modified . They do not, by themselves, create a new revision history until an install, retrieve, or auto-update occurs.

NEW QUESTION: 12
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: (SHOW ANSWER)

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: 13

Refer to the following configuration. 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 answers

A. The same administrator can lock more than one ADOM at the same time.

B. Multiple administrators can lock and work on separate ADOMs at the same time.

C. All changes must be approved before they can be installed on a device.

D. Concurrent read-write access to an ADOM is disabled.

Answer: (SHOW ANSWER)

The command set workspace-mode normal enables Workspace (ALL ADOMs) . In this mode, FortiManager uses ADOM locking to prevent configuration conflicts. The study guide explains that workspace mode is used to prevent concurrent ADOM access , and once an ADOM is locked, only the administrator who locked it has read-write access while all others have read-only access. That makes D correct.

B is also correct because locking is applied per ADOM, so different administrators can work at the same time on different ADOMs without conflicting with each other. This is consistent with the design goal of workspace mode and ADOM locking.

C describes workflow mode , not workspace normal. Approval before installation is required only with set workspace-mode workflow.

=========

NEW QUESTION: 14

Refer to Exhibits:

HA configuration

```
HQ-NGFW-1 # config system ha

HQ-NGFW-1 (ha) # show
config system ha
    set group-id 5
    set group-name "Training"
    set mode a-p
    set password ENC a4fbyqY4iPexFmAnZgzDY
    set hbdev "port7" 0
    set session-pickup enable
    set override disable
    set priority 200
    set monitor "port1"
    set memory-based-failover enable
    set memory-failover-threshold 70
    set memory-failover-monitor-period 50
    set memory-failover-sample-rate 10
    set memory-failover-flip-timeout 60
end
```

HQ-NGFW-1 System Performance output

```
HQ-NGFW-1 # get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 1837868k used (90%), 104146k free (5.1%), 100062k freeable (4.9%)
Average network usage: 19/2 kbps in 1 minute, 19/4 kbps in 10 minutes, 19/3 kbps in 30 minutes
Maximal network usage: 36/16 kbps in 1 minute, 58/86 kbps in 10 minutes, 58/87 kbps in 30 minutes
Average sessions: 21 sessions in 1 minute, 22 sessions in 10 minutes, 21 sessions in 30 minutes
Maximal sessions: 22 sessions in 1 minute, 28 sessions in 10 minutes, 28 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 22 hours, 50 minutes
```

HQ-NGFW-2 System Performance output

```
HQ-NGFW-2 # get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 993836k used (48.7%), 690352k free (33.8%), 357888k freeable (17.5%)
Average network usage: 26/18 kbps in 1 minute, 25/18 kbps in 10 minutes, 24/18 kbps in 30 minutes
Maximal network usage: 91/27 kbps in 1 minute, 92/27 kbps in 10 minutes, 92/32 kbps in 30 minutes
Average sessions: 9 sessions in 1 minute, 9 sessions in 10 minutes, 9 sessions in 30 minutes
Maximal sessions: 11 sessions in 1 minute, 11 sessions in 10 minutes, 13 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 10 hours, 50 minutes
```

An administrator has observed the performance status outputs on an HA cluster for 55 seconds.

Which FortiGate is the primary?

A. HQ-NGFW-2 with the parameter memory-failover-threshold setting

B. HQ-NGFW-2 with the parameter priority setting

C. HQ-NGFW-1 with the parameter memory-failover-flip-timeout setting

D. HQ-NGFW-1 with the parameter override setting

Answer: (SHOW ANSWER)

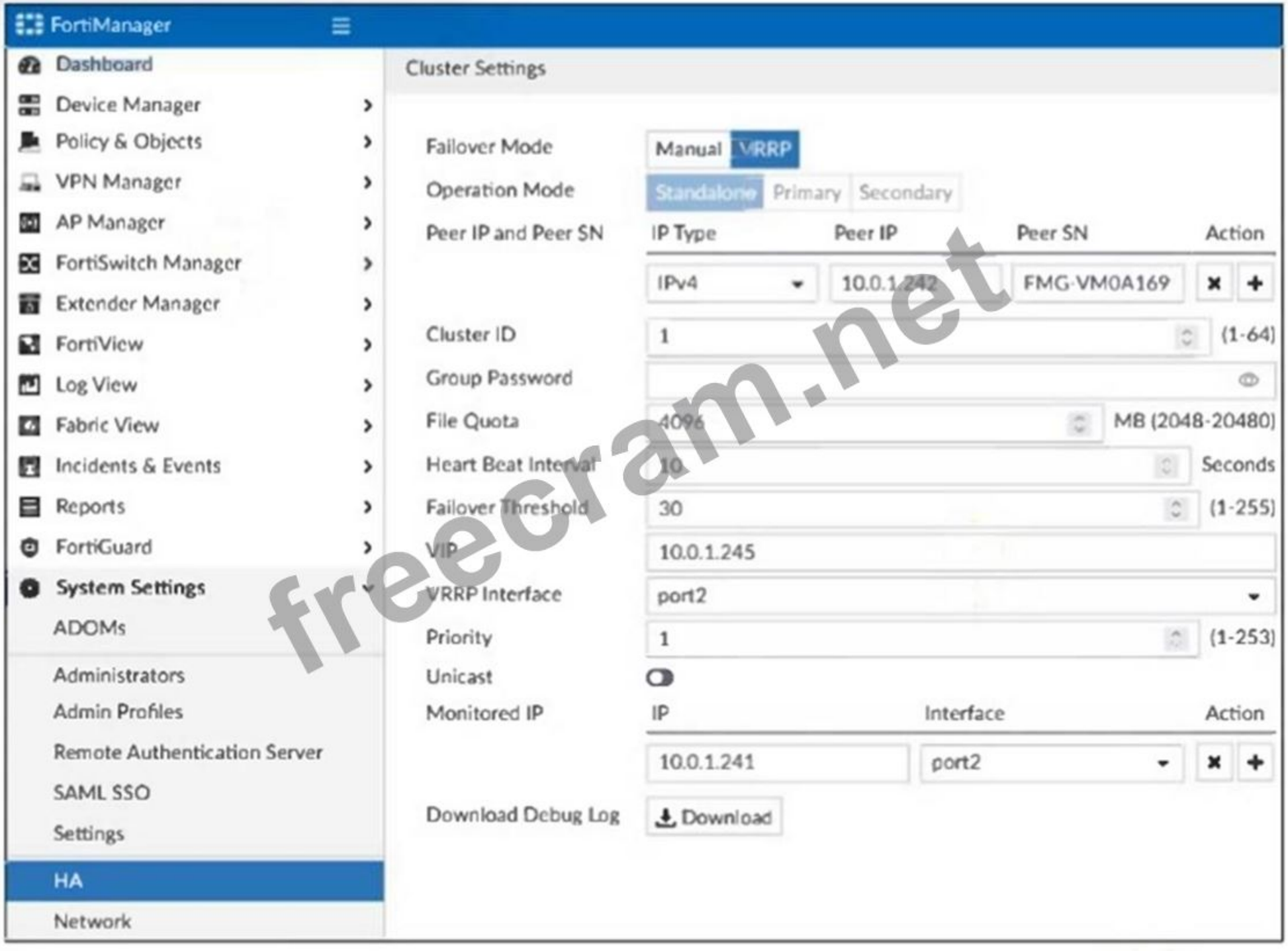
The correct answer is A . This conclusion comes from the HA settings shown in the exhibit plus Fortinet's HA behavior. In the exhibit, HQ-NGFW-1 has memory-based-failover enabled , memory-failover- threshold 70 , memory-failover-monitor-period 50 , and its memory usage is about 90% , while HQ- NGFW-2 is about 48.7% . Fortinet's official documentation states that memory-failover-threshold is the memory percentage that triggers failover, and memory-failover-monitor-period is the duration high memory must persist before failover occurs. It also states that if utilization stays above the threshold for the entire monitor period, a failover is triggered , and the peer becomes primary. (Fortinet Document Library) Because the condition was observed for 55 seconds , which is longer than the configured 50-second monitor period , the cluster would fail over from HQ-NGFW-1 to HQ-NGFW-2 due to the memory-failover-threshold condition. The priority setting does not explain this result here, because override is disabled , and flip-timeout governs subsequent memory-based failovers, not the initial trigger. (Fortinet Document Library)

=========

NEW QUESTION: 15

Refer to the exhibit.

FortiManager cluster settings



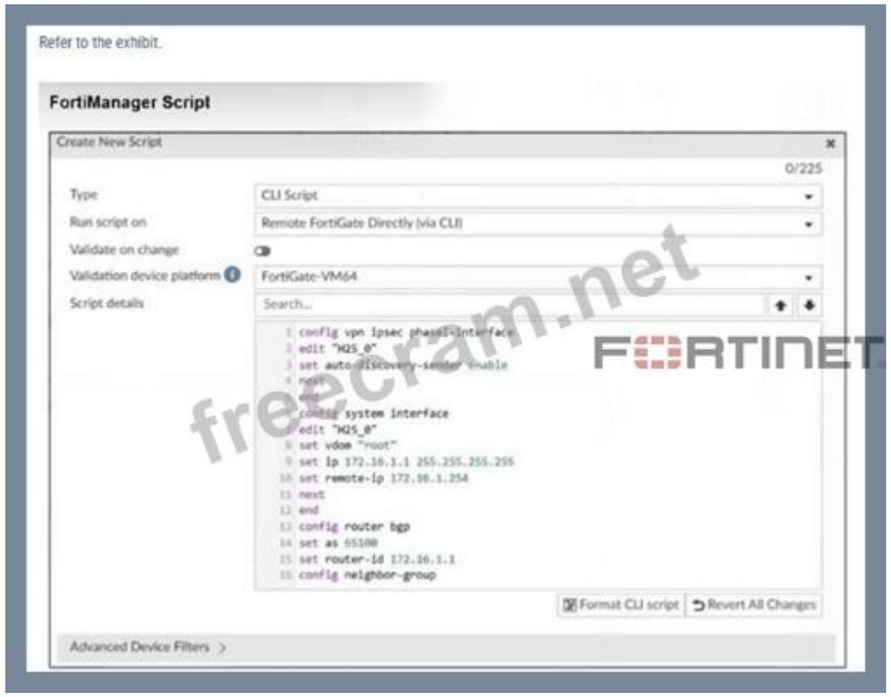
If the monitored interface for the primary FortiManager device fails, what must you do to maintain high availability (HA)?

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: (SHOW ANSWER)
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: 16
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: (SHOW ANSWER)
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: 17
Refer to the exhibit.

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: 18
Refer to the exhibit.

Which two statements about the configuration shown in the exhibit are true? Choose two answers.
A. An administrator can lock the Local-FortiGate_root policy package.
B. The administrator created a snapshot of the Remote-FortiGate policy package.
C. The FortiManager ADOM workspace mode is set to normal.
D. The FortiManager is in workflow mode.
Answer: (SHOW ANSWER)

The exhibit shows Remote-FortiGate with a green closed lock icon , which indicates a locked policy package . The FortiManager 7.6 Administrator Study Guide states: "Policy locking is available in workspace normal and per-ADOM modes" and "Policy locking allows administrators to work on and lock a single policy package instead of locking the whole ADOM." This confirms that a package such as Local-FortiGate_root can also be locked, so A is correct.
B is incorrect because the study guide and lab guide describe snapshots as ADOM revisions , not policy package snapshots: "An ADOM revision creates a snapshot of the policy and object configuration for the ADOM." D is incorrect because in workflow mode, sessions and approval are required before installation. The exhibit shows a normal save/lock state, not a workflow session state.
=========

NEW QUESTION: 19
An administrator is copying a system template profile between ADOMs by running the following command:
execute fmprofile export-profile ADOM 3547 /tmp/Backup_File
output dump to file: [/tmp/Backup_File]
Where does this command export the system template profile from?
A. FortiManager /tmp/Backup_File folder
B. FortiManager ADOM policy database
C. ADOM device database
D. FortiManager configuration backup file
Answer: (SHOW ANSWER)
The FortiManager 7.6 Administrator Study Guide states under Copying System Templates Between ADOMs: "The first step is to export the system template from the original ADOM with the execute fmprofile export-profile command" and shows the output file being written to /tmp/Training , described as "File copied in FortiManager tmp folder." The key point is that the command exports the system template profile from the original ADOM , while
/tmp/Backup_File is only the destination path on FortiManager where the exported file is stored. The same study guide also defines system templates as a "subset of model device configuration-system-level settings" , which means they belong to the device-level side of the ADOM , not the policy database.
So the export source is the ADOM device database , and the file is saved afterward in the FortiManager /tmp folder.

NEW QUESTION: 20
An administrator upgrades FortiManager with workspace mode per ADOM enabled to the latest version but notices that the ADOM versions did not change.
Why were the ADOMs not upgraded?

A. The administrator did not run the database integrity check before performing the upgrade.
B. FortiManager does not automatically upgrade ADOMs after a firmware upgrade.
C. A FortiManager process task is stuck and blocking the ADOM upgrade, so the administrator must fix it.
D. A user had all ADOMs locked before the upgrade, which stopped them from being upgraded.
Answer: (SHOW ANSWER)
The correct answer is B . The FortiManager 7.6 Administrator Study Guide gives the exact extract: "Also note when you upgrade the FortiManager firmware version the existing ADOMs are not automatically upgraded." This directly explains why the administrator saw the FortiManager upgrade complete while the ADOM versions remained unchanged.
The same section also explains that ADOM upgrades are a separate action: "You can upgrade an ADOM in System Settings > ADOMs" and "Can upgrade to one version higher at a time." In addition, the guide recommends: "upgrade all devices first, and then upgrade the ADOM." So the issue is not workspace mode, locked ADOMs, or a stuck task. The ADOMs simply require their own manual upgrade step after the FortiManager firmware upgrade.

NEW QUESTION: 21

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: (SHOW ANSWER)
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: 22
Refer to Exhibit:

Configuration Revision History

Configuration Revision History

View Config | View Install Log | Revision Diff | Retrieve Config | More | Search...

ID	Date & Time	Name	Created by	Installation	Comments
7	2025-03-27 17:07:13	BR1-FGT-1	admin	Installed	
✓ 6	2025-02-26 19:12:28	BR1-FGT-1	student	Revision Revert	Reverted from ID 7 by admin. A new revision ID will be generat
5	2025-02-26 19:03:41	AutoUpdate	AutoUpdate	Revision Revert	Reverted from ID 6 by admin. A new revision ID will be generat
4	2025-02-26 19:03:36	BR1-FGT-1	admin	Revision Revert	Reverted from ID 6 by admin. A new revision ID will be generat
3	2025-02-26 18:53:46	AutoUpdate	AutoUpdate	Auto Updated	Autoretrieve merged config
2	2025-02-26 18:29:53	BR1-FGT-1	admin	Installed	
1	2025-02-26 17:51:22		student	Revision Revert	Reverted from ID 6 by admin. A new revision ID will be generat

1 Selected

Device Revision Diff wizard

Device Revision Diff

Revision ID: 6		Revision ID: 7	
Total	13495	Total	12696
Deleted	805	Added	26
Modified	26	Modified	0

```
12939 config firewall policy
12940 edit 1
12941 set name "Internet"
12942 set uuid 9117420a-8b0c-51ef-f05a-8b1b2297d9de
12943 set action accept
12944 set srcintf "port4"
12945 set dstintf "port2"
12946 set nat enable
12947 set srcaddr "all"
12948 set dstaddr "all"
12949 set schedule "always"
12950 set service "ALL"

12951 next
```

```
12143 config firewall policy
12144 edit 1
12145 set name "Internet"
12146 set uuid 9117420a-8b0c-51ef-f05a-8b1b2297d9de
12147 set action accept
12148 set srcintf "port4"
12149 set dstintf "port2"
12150 set nat enable
12151 set srcaddr "all"
12152 set dstaddr "all"
12153 set schedule "always"
12154 set service "ALL"
12155 set comments "test"
12156 next
```

Save Diff as Script | Show Diff Only | < Previous Diff | Next Diff > | Cancel

An administrator admin used the Configuration Revision History window to revert the FortiGate device configuration to revision ID 6. After running the reinstall policy package, the administrator noticed problems with the firewall policy- they could not see the unset comment on policy ID 1.
Why did FortiManager not remove the comment from policy ID 1 when the administrator ran reinstall policy package?
A. Because the administrator student must install the configuration changes to correctly see the expected results.
B. Because the administrator must import the firewall policies to update the firewall policy package.
C. Because every time the administrator uses the revert config file, they must use the Install Wizard instead of running the reinstall policy package.
D. Because the administrator used the Revision Diff view, which shows what changed, not what will be installed.
Answer: (SHOW ANSWER)
The correct answer is B . The FortiManager 7.6 Administrator Study Guide gives the exact extract:
"Performing a revert operation followed by an installation only reverts device-level changes and does not revert policy packages. To achieve full synchronization, you must run the Import Configuration tool on FortiManager to synchronize the policy package." The guide also states: "After every retrieve, auto-update, or revert operation, you must use Import Configuration to ensure the policy information is synchronized." In the exhibit, the missing unset comment for policy ID 1 is a policy package issue, not just a device-level revert issue. Reinstalling the existing policy package does not automatically rebuild it from the reverted revision. The administrator must import the firewall policies again so the policy package reflects the reverted policy state. That is why the comment was not removed.
=========

NEW QUESTION: 23
An administrator has a FortiGate-HQ device with VDOMs-root, HR and Facilities, currently managed under the FortiManager ADOM-Site1. They try to move VDOM HR to the FortiManager ADOM-Site2, but it does not work.
Why is the administrator not able to move FortiGate-HQ VDOM HR to FortiManager ADOM-Site2?
A. The FortiGate-HQ must be managed under the FortiManager ADOM-root to allow moving its VDOMs to different ADOMs.
B. The administrator must delete the FortiGate-HQ device from FortiManager and add it again using the Add Device wizard before moving the VDOM.
C. The administrator must have full access in the device layer of FortiGate-HQ VDOM-root before they can VDOMs to different ADOMs.
D. FortiManager must be in ADOM normal mode, which does not allow VDOMs to be managed separately.
Answer: (SHOW ANSWER)

NEW QUESTION: 24
What can you conclude from the failed installation log shown in the exhibit?

Installation log

A. Policy ID 2 is installed in the disabled state.
B. Policy ID 2 will not be installed.
C. Policy ID 2 is installed without a source address.
D. Policy ID 2 is installed without the remote user student.
Answer: (SHOW ANSWER)
The correct answer is D . The lab guide explains that when an installation fails, the installation log shows the commands that the managed device received and accepted, as well as the commands that the managed device did not accept .
From the exhibit, FortiGate accepted the policy creation commands for policy ID 2 such as set srcintf port3, set dstintf port1, set srcaddr all, set dstaddr all, set action accept, and set schedule always. However, the line set users student failed with "entry not found in datasource" and "value parse error before ' student ' " .
That shows the user reference was not accepted, while the rest of the policy commands were processed.
Therefore, policy ID 2 is still created, but without the remote user student . This rules out A , B , and C .
=========

NEW QUESTION: 25
Which two statements about the integrity of databases on FortiManager are correct? Choose two answers.
A. Scheduled backups run database integrity commands automatically.
B. The diagnose dvm check-integrity command attempts to fix a corrupted file system.
C. The diagnose cdb check adom-integrity command can correct issues related to locked devices.

D. You should fix all database integrity issues before performing a script.
E. Not following the correct upgrade path may cause inconsistencies in the databases.
Answer: (SHOW ANSWER)
The correct answers are A and E . The study guide explicitly states under Database Integrity that scheduled backups "Automatically executes database integrity commands" and "Does not automatically make corrections" . That exactly verifies A .
It also states in Best Practices-Database Integrity: "Always follow the proper upgrade path" and "If you don't, it may cause inconsistencies in the database." That exactly verifies E .
B is incorrect because diagnose dvm check-integrity verifies and corrects device manager database issues such as device states, memberships, lock statuses, and duplicate VDOM entries, not a corrupted file system. C is incorrect because locked device status issues are listed under diagnose dvm check-integrity, not diagnose cdb check adom-integrity. D is not a stated FortiManager best practice in the uploaded guide.

NEW QUESTION: 26
Which is recommended when you are managing a high volume of logs in your network?
A. Forward logs from FortiAnalyzer to FortiManager daily.
B. Add and manage FortiAnalyzer from FortiManager.
C. Store logs on FortiManager and use FortiView.
D. Enable advanced ADOM mode on FortiManager.
Answer: (SHOW ANSWER)

NEW QUESTION: 27
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: 28
Refer to the exhibit.

```
FortiManager # diagnose dvm device list
--- There are currently 6 devices/vdoms managed ---
--- There are currently 6 devices/vdoms count for license ---

TYPE            OID    SN               HA      IP             NAME          ADOM     IPS                  FIRMWARE        HW_GenX
fmgfaz-managed  188    FGVM02TM24013504 -       100.65.1.111   BR1-FGT-1     My_ADOM  7.0 MR6 (3401)  N/A
                |- STATUS: dev-db: not modified; conf: in sync; cond: pending; dm: installed; conn: up; template:[modified]default
                |- vdom:[3]root flags:0 adom:My_ADOM pkg:[imported]BR1-FGT-1
```


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, updating policy and device-level database.

C. The latest revision history for the managed FortiGate does match the FortiManager policy database.

D. The system template default will override device-level database configurations.

Answer: C,D (LEAVE A REPLY)

The output shows dev-db: not modified; conf: in sync, which means the device-level database is aligned with the latest revision history , so A is false . The study guide explains that "Synchronized / Auto-update:

The latest revision history configuration entry ... is aligned with the configuration on FortiGate," and dev-db: not modified indicates the device-level settings are not changed on FortiManager.

For the policy layer, the output shows pkg:[imported]BR1-FGT-1. The study guide states "Imported:

indicates that a policy package was successfully imported for a managed device," so the policy package in FortiManager matches what was imported from the managed device context, making C correct.

D is also correct because the lab guide explicitly says "All Provisioning Templates applied on FortiGate devices have precedence over any configuration you apply on the device layer of the FortiManager."

NEW QUESTION: 29

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.