Fortinet

Exam Questions FCP_FMG_AD-7.4

FCP - FortiManager 7.4 Administrator

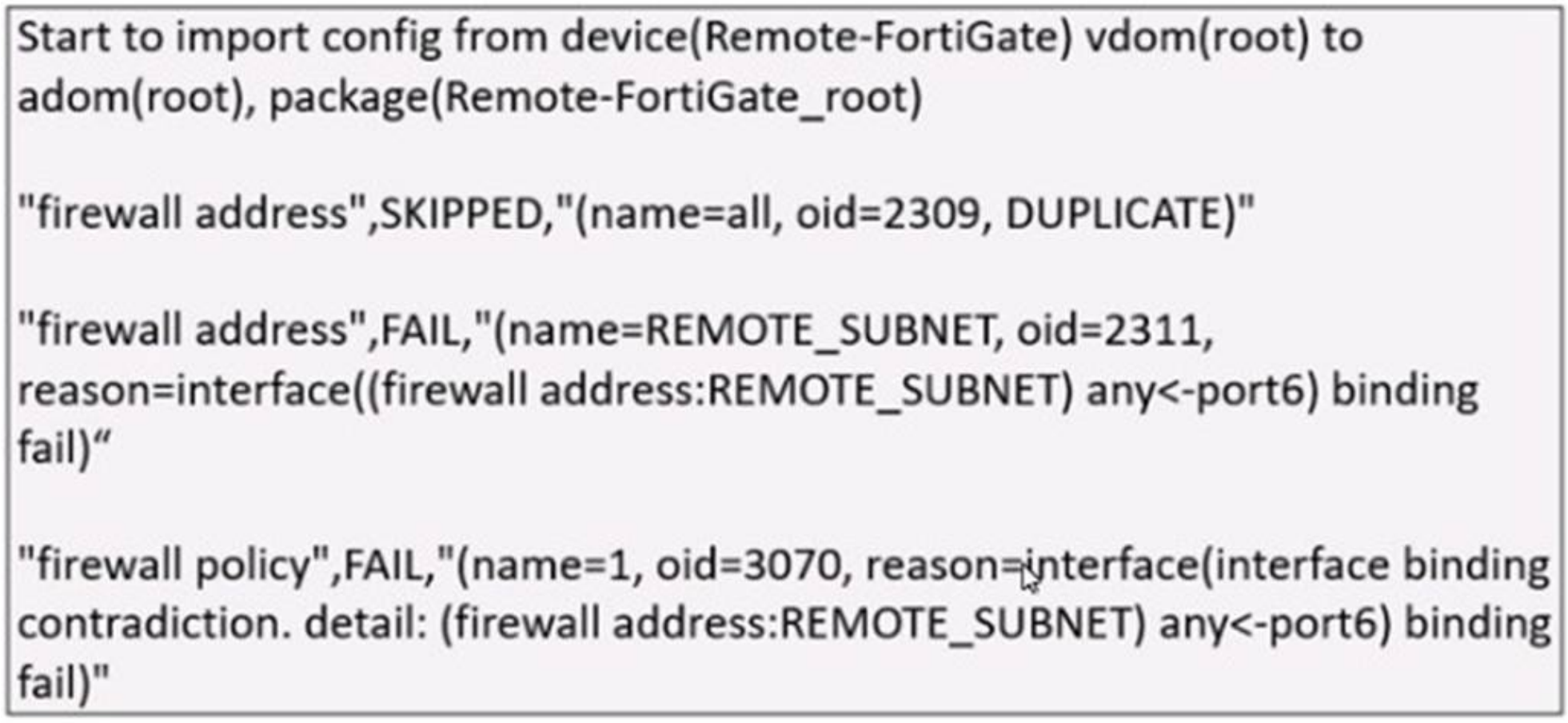
NEW QUESTION 1
Which two items does an FGFM keepalive message include? (Choose two.)

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

Answer: CD

Explanation:
The FortiGate-FortiManager (FGFM) protocol is used for communication between a FortiGate device and FortiManager. Thekeepalive messagesare essential for maintaining communication and monitoring the health of the FortiGate devices connected to FortiManager. These messages provide important status information about the device. Here are the items included in an FGFM keepalive message:
? A. FortiGate IPS version
? B. FortiGate license information
? C. FortiGate configuration checksum
? D. FortiGate uptime

NEW QUESTION 2
Refer to the exhibit which shows the Download Import Report.



Why is FortiManager failing to import firewall policy ID 1?

A. Policy ID 1 is configured from the interface any to port6. FortiManager rejects the request to import this policy because the any interface does not exist on FortiManager
B. Policy ID 1 for this managed FortiGate already exists on FortiManager in the policy package named Remote-FortlGate.
C. Policy ID 1 has an address object that already exists in the ADOM database with any as the interface association, and conflicts with the address object interface association locally on FortiGate.
D. Policy ID 1 does not have the ADOM Interface mapping configured on FortiManager.

Answer: A

Explanation:
? Option A: Policy ID 1 is configured from the interface any to port6. FortiManager rejects the request to import this policy because the any interface does not exist on FortiManager.This is the correct answer. FortiManager fails to import firewall policy ID 1 because it cannot map the "any" interface to a valid interface in its ADOM database. The error indicates that there is a binding failure due to an interface mismatch.
Explanation of Incorrect Options:
? Option B: Policy ID 1 for this managed FortiGate already exists on FortiManager in the policy package named Remote-FortiGateis incorrect because the error is related to interface mapping, not a duplicate policy ID.
? Option C: Policy ID 1 has an address object that already exists in the ADOM database with any as the interface association and conflicts with the address object interface association locally on FortiGateis incorrect because the error specifies an interface issue, not an address object conflict.
? Option D: Policy ID 1 does not have the ADOM Interface mapping configured on FortiManageris incorrect because the error directly mentions a binding failure due to the "any" interface.
FortiManager References:
? For more information, refer to the "Device Manager" section and "Configuration Import and Mapping" in the FortiManager Administration Guide.

NEW QUESTION 3
Which output is displayed right after moving the ISFW device from one ADOM to another?
A)

```
FortiManager # diagnose dvm device list ISFW
--- There are currently 4 devices/vdoms managed ---
--- There are currently 4 devices/vdoms count for license ---

TYPE            OID    SN                HA      IP              NAME            ADOM     IPS                FIRMWARE
fmgfaz-managed  325    FGVM010000077646  -       10.0.1.200      ISFW            ADOM74   6.00741 (regular)  7.0 MR4 (2463)
                |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; conn: up
                |- vdom:[3]root flags:0 adom:ADOM74 pkg:[unknown]ISFW
```

B)

```
FortiManager # diagnose dvm device list ISFW
--- There are currently 4 devices/vdoms managed ---
--- There are currently 4 devices/vdoms count for license ---

TYPE            OID    SN                HA      IP              NAME            ADOM     IPS                FIRMWARE
fmgfaz-managed  325    FGVM010000077646  -       10.0.1.200      ISFW            ADOM74   6.00741 (regular)  7.0 MR4 (2463)
                |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: autoupdated; conn: up
                |- vdom:[3]root flags:1 adom:ADOM74 pkg:[out-of-sync]ISFW
```

C)

```
FortiManager # FortiManager # diagnose dvm device list ISFW
--- There are currently 4 devices/vdoms managed ---
--- There are currently 4 devices/vdoms count for license ---

TYPE            OID    SN                HA      IP              NAME            ADOM     IPS                FIRMWARE
fmgfaz-managed  325    FGVM010000077646  -       10.0.1.200      ISFW            ADOM74   6.00741 (regular)  7.0 MR4 (2463)
                |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: installed; conn: up
                |- vdom:[3]root flags:0 adom:ADOM74 pkg:[never-installed]
```

D)

```
FortiManager # diagnose dvm device list ISFW
--- There are currently 4 devices/vdoms managed ---
--- There are currently 4 devices/vdoms count for license ---

TYPE            OID    SN                HA      IP              NAME            ADOM     IPS                FIRMWARE
fmgfaz-managed  325    FGVM010000077646  -       10.0.1.200      ISFW            ADOM74   6.00741 (regular)  7.0 MR4 (2463)
                |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: installed; conn: up
                |- vdom:[3]root flags:0 adom:ADOM74 pkg:[imported]ISFW
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

Explanation:
When a FortiGate device, like the ISFW (Internal Segmentation Firewall), is moved from one ADOM to another in FortiManager, the status of the device in the new ADOM will temporarily show some level of inconsistency or unknown state until the ADOM fully syncs and integrates the device.
In the provided options, we are analyzing the FortiManager diagnose dvm device list output for the ISFW device.
Explanation of the Outputs:
? Option A:
? Option B:
? Option C:
? Option D:
Conclusion:
The output that is displayedimmediately after movingthe ISFW device from one ADOM to another isOption A, where the package status is still unknown (pkg: [unknown]) because FortiManager has not yet fully synchronized the device's configuration in the new ADOM.

NEW QUESTION 4
Exhibit.

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

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

A. You can validate administrator login attempts through external servers.
B. The same administrator can lock more than one ADOM at the same time.
C. Two or more administrators can make configuration changes at the same time, in the same ADOM.
D. Concurrent read-write access to an ADOM is disabled.

Answer: BD

Explanation:
The configuration shown in the exhibit sets theworkspace-mode to normal. The workspace mode in FortiManager defines how configuration changes and administrative tasks are handled, specifically regarding locking and collaboration in ADOMs (Administrative Domains).
Understanding the workspace modes:
? Normal Mode:In this mode, only one administrator at a time can lock and edit an ADOM. The changes made by one administrator must be completed and saved before another administrator can make changes. It prevents concurrent read-write access within the same ADOM.
? Workflow Mode:This mode allows multiple administrators to work on different tasks within the same ADOM, but changes still need to be approved before being committed.
Explanation of Options:
? A. You can validate administrator login attempts through external servers.
? B. The same administrator can lock more than one ADOM at the same time.
? C. Two or more administrators can make configuration changes at the same time, in the same ADOM.
? D. Concurrent read-write access to an ADOM is disabled.

NEW QUESTION 5
What will be the result of reverting to a previous revision version in the revision history?

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

Answer: C

Explanation:
? Option C: It will modify the device-level database.This is correct. Reverting to a previous revision version in the revision history affects the device-level database by restoring it to the state saved in the selected revision. This ensures that any changes made after the selected revision are discarded, and the device configuration is returned to the earlier state.
Explanation of Incorrect Options:
? Option A: It will install configuration changes to managed devices automaticallyis incorrect because reverting a revision does not automatically push changes to the devices; it merely reverts the configuration on the FortiManager.
? Option B: It will tag the device settings status as Auto-Updateis incorrect because "Auto-Update" is not a status related to the revision history mechanism.
? Option D: It will generate a new version ID and remove all other revision history versionsis incorrect as reverting to a previous revision does not delete all other versions; it creates a new revision point for tracking.
FortiManager References:
? Refer to the "Revision Management" section in the FortiManager Administration Guide, which provides an overview of how revisions are managed and utilized for restoring configurations.

NEW QUESTION 6
Refer to the exhibit.

An administrator is about to add the FortiGate device to FortiManager using the discovery process.
FortiManager is operating behind a NAT device, and the administrator configured the FortiManager NATed IP address under the FortiManager system administration settings.
What is the expected result?

A. During discover
B. FortiManager uses only the FortiGate serial number to establish the
C. During discovery, FortiManager sets both the FortiManager NATed IP address and NAT device IP address on FortiGate.
D. During discover
E. FortiManager sets the NATed device IP address on FortiGate.
F. During discovery, FortiManager sets the FortiManager NATed IP address on FortiGate.

Answer: D

Explanation:
When adding a FortiGate device to FortiManager that is operating behind a NAT device, and the FortiManager NATed IP address is configured under the system administration settings, FortiManager will set the FortiManager NATed IP address on the FortiGate device during the discovery process. This ensures that the FortiGate knows how to reach the FortiManager through the NAT device.
Options A, B, and C are incorrect because:
? Ais incorrect because the discovery process also requires knowing the NATed IP to establish a connection, not just the serial number.
? Bis incorrect because FortiManager does not set the NAT device's IP address on the FortiGate.
? Cis incorrect because it implies that the NAT device IP is set on FortiGate, which is not the expected outcome.
FortiManager References:
? Refer to FortiManager 7.4 Administrator Guide: Device Discovery and Management with NAT.

NEW QUESTION 7
An administrator wants to create a policy on an ADOM that is in backup mode and install it on a FortiGate device in the same ADOM. How can the administrator perform this task?

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

Answer: B

Explanation:
To create and install a policy on a FortiGate device in an ADOM (Administrative Domain) that is in backup mode, the administrator must use a FortiManager script. This is because backup mode restricts direct configuration changes, and scripts can be used to push specific configuration changes without altering the ADOM mode.
Options A, C, and D are incorrect because:
? A requires the ADOM to be in normal or advanced mode to create policies directly in the Policy & Objects section.
? C suggests disabling offline mode, which is irrelevant to the backup mode configuration.
? D implies changing the ADOM mode, which is unnecessary if using a script to perform the task.
FortiManager References:
? Refer to FortiManager 7.4 Administrator Guide: Working with ADOMs and Using Scripts for managing policies in backup mode.

NEW QUESTION 8
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 120.6m  0.0   1.5   0:00.00 S fclinkd
```

What percent 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. 2.9
B. 3.1
C. 1.5
D. 4.1

Answer: A

Explanation:
In the exhibit, the FortiManager CLI output displays the results of thetopcommand, which shows system processes, CPU usage, and memory (RAM) usage. We are specifically looking for the process responsible for downloading theweb and email filter databases from the public FortiGuard servers. This process is typically handled by thefgdlinkd process.
Key information from the output:
? Thefgdlinkdprocess is listed with aPID of 1463.
? The%MEMcolumn shows that this process is using2.9%of the available RAM.
Evaluation of Options:
? A. 2.9: This iscorrect. Thefgdlinkdprocess, which handles the web and email filter database downloads, is using2.9%of the available memory, as indicated in the%MEMcolumn.

? B. 3.1: This is incorrect. The3.1%memory usage belongs to thefwmsvrdprocess, not the fgdlinkd process.
? C. 1.5: This is incorrect. The1.5%memory usage belongs to thefclinkdprocess, not the fgdlinkd process.
? D. 4.1: This is incorrect. The4.1%memory usage belongs to thefgdsvrprocess, not the fgdlinkd process.

NEW QUESTION 10
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

FCP_FMG_AD-7.4 Practice Exam Features:

* FCP_FMG_AD-7.4 Questions and Answers Updated Frequently

* FCP_FMG_AD-7.4 Practice Questions Verified by Expert Senior Certified Staff

* FCP_FMG_AD-7.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCP_FMG_AD-7.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year