KillTest

質量更高　服務更好

練習題

https://www.killtest.net

一年免費更新服務

Exam : **NSE6_FMG_AD-7.6**

Title : Fortinet NSE 6 - FortiManager 7.6 Administrator

Version : DEMO

1.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: A C
Explanation:
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.

2.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: A E
Explanation:
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.

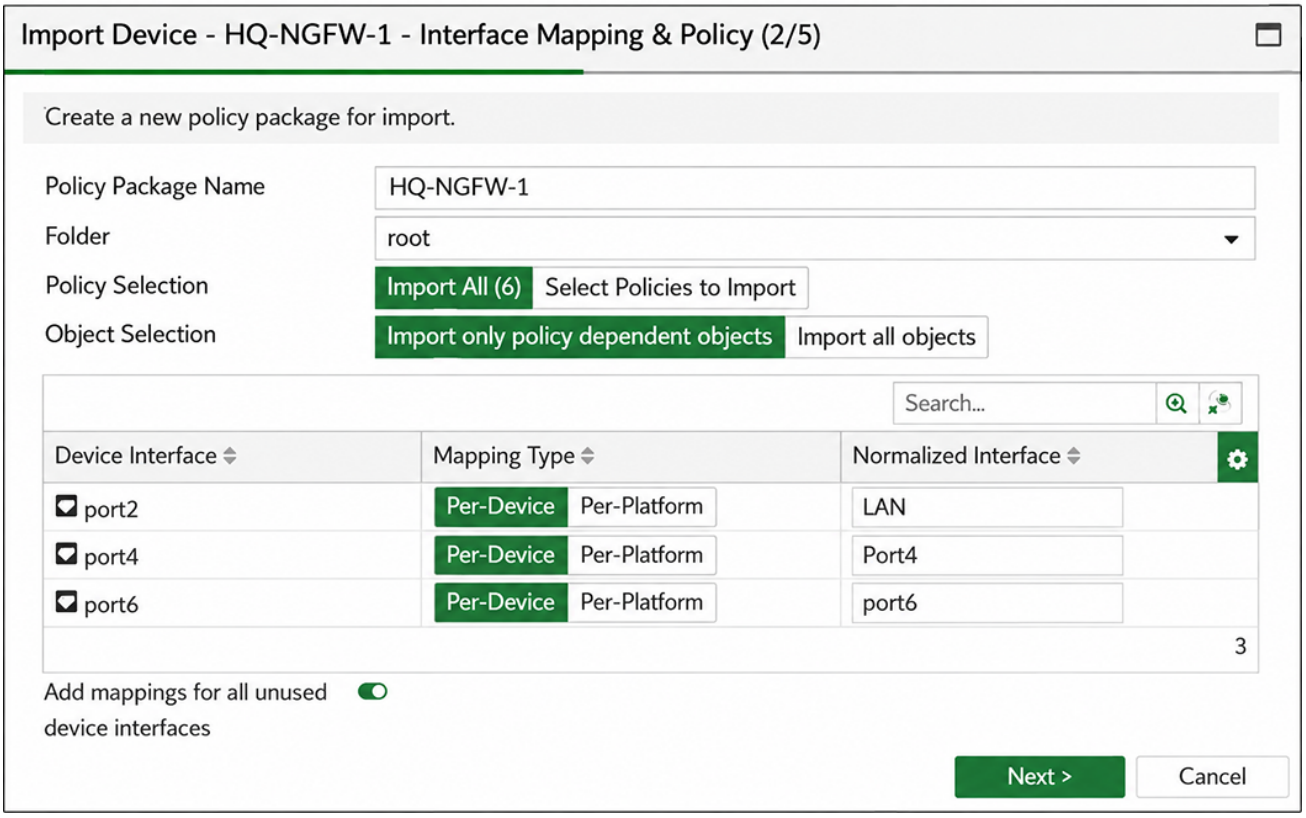
3.While attempting to push a NetFlow configuration script through the FortiManager policy package: an administrator encounters an error stating that an object is unrecognized in line 4.

```
Starting log (Run on database)
config vdom
edit AGEUSR
[line 4] > config sys interface [parameter(s) invalid. detail: object unrecognized]
Failed to commit to DB, reason([line 4] > config sys interface [parameter(s) invalid. detail: object unrecognized]

Running script(NetFlow_Configuration) on DB failed
```

What must the administrator do to successfully apply the NetFlow configuration script and avoid the object unrecognized error?
A. Make sure the user running the script has full access to the VDOM—AGEUSR.
B. Run the script on the device database.
C. Use metadata variables if they use VDOMs in the script.
D. Create a normalized interface on the policy layer before running the script.
Answer: B
Explanation:
The correct answer is B. The error occurs because the script is being run on the policy package database, but the failing command is config sys interface, which is a device-level configuration command, not a policy-layer command. The lab guide gives the exact relationship: “Because the scripts target the device database, first, you will run the scripts against the device database, and then install the scripts on the managed devices” and “The scripts contain configuration changes related to device-level settings.”
By contrast, the lab guide shows Policy Package or ADOM Database scripts being used for firewall objects and policies in a policy package.
So this NetFlow script must be run on the device database, then installed. The issue is not VDOM permissions, metadata variables, or normalized interfaces.

4.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: C
Explanation:
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.

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: C
Explanation:
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.