

Fortinet NSE 5FortiManager 7.2

Fortinet NSE5 FMG-7.2

Version Demo

Total Demo Questions: 2

Total Premium Questions: 23

Buy Premium PDF

<https://passqueen.com>

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Administration	4
Topic 2, Device management	6
Topic 3, Policy and objects	8
Topic 4, Install configuration changes	3
Topic 5, Provisioning FortiGate devices	1
Topic 6, Troubleshooting	1
Total	23

QUESTION NO: 1

Which two statements regarding device management on FortiManager are true? (Choose two.)

- A. FortiGate devices in HA cluster devices are counted as a single device.
- B. FortiGate in transparent mode configurations are not counted toward the device count on FortiManager.
- C. FortiGate devices in an HA cluster that has five VDOMs are counted as five separate devices.
- D. The maximum number of managed devices for each ADOM is 500.

ANSWER: A C

Explanation:

FortiManager uses logical managed-device accounting for FortiGate high-availability deployments. A FortiGate HA cluster is managed as one cluster entity rather than as separately managed primary and secondary members. This lets an administrator perform policy-package assignment, configuration installation, revision management, and monitoring at the cluster level while preserving the cluster's operational relationship. Therefore, the statement that FortiGate devices in HA cluster devices are counted as a single device is correct.

Virtual domains affect this accounting because FortiManager manages configuration and policy scope per VDOM. Each VDOM is treated as a separately managed logical FortiGate context for device-count purposes. Consequently, when an HA cluster has five VDOMs, the cluster contributes five managed-device contexts to the relevant device count. This is why the statement that FortiGate devices in an HA cluster that has five VDOMs are counted as five separate devices is also correct. These rules are important when planning FortiManager capacity and licensing for multi-VDOM deployments, particularly where clusters consolidate several administrative or tenant contexts. Fortinet documents FortiManager device administration and managed-device behavior in the [FortiManager 7.2 Administration Guide](#); product capacity information is also available in the [FortiManager product documentation](#).

QUESTION NO: 2

An ADOM is operating in workspace mode. Administrator A has locked the ADOM and is editing a policy package. Administrator B must make an urgent change to the same ADOM but cannot modify its policy objects.

What should Administrator B do?

- A. Wait for Administrator A to release the ADOM lock, then lock the ADOM.
- B. Create a second policy package with the same name in the ADOM.
- C. Install the current policy package to release the ADOM lock.
- D. Change the ADOM mode to normal mode while Administrator A is editing.

ANSWER: A

Explanation:

Administrator B must obtain the ADOM lock before making changes. In workspace mode, the lock prevents concurrent administrators from changing the same ADOM database and creating conflicting edits. Administrator A can commit or discard the current workspace changes and release the lock, after which Administrator B can lock the ADOM and make the required change. Creating another administrator account or installing the policy package does not bypass the workspace lock.