NSE5_FMG-6.4 Q&As

Fortinet NSE 5 - FortiManager 6.4

Pass Fortinet NSE5_FMG-6.4 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/nse5_fmg-6-4.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

An administrator with the Super_User profile is unable to log in to FortiManager because of an authentication failure message.

Which troubleshooting step should you take to resolve the issue?

A. Make sure FortiManager Access is enabled in the administrator profile

B. Make sure Offline Mode is disabled

C. Make sure the administrator IP address is part of the trusted hosts.

D. Make sure ADOMs are enabled and the administrator has access to the Global ADOM

Correct Answer: C

Explanation: Even if a user entered the correct userid/password, the FMG denies access if a user is logging in from an untrusted source IP subnets. Reference: https://docs.fortinet.com/document/fortimanager/6.0.3/administration-guide/107347/trustedhosts

QUESTION 2

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.

Correct Answer: AC

QUESTION 3

Refer to the exhibit.

An administrator logs into the FortiManager GUI and sees the panes shown in the exhibit.

Which two reasons can explain why the FortiAnalyzer feature panes do not appear? (Choose two.)

A. The administrator logged in using the unsecure protocol HTTP, so the view is restricted.

B. The administrator profile does not have full access privileges like the Super_User profile.

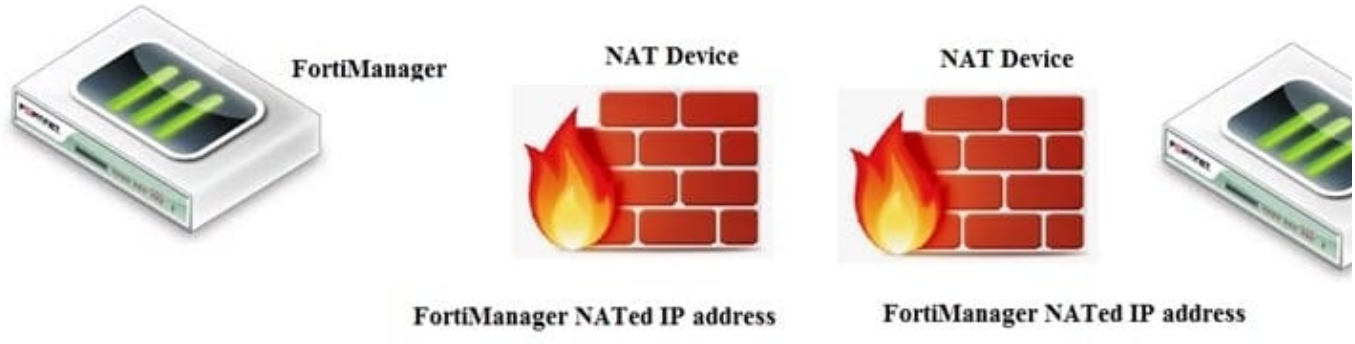
C. The administrator IP address is not a part of the trusted hosts configured on FortiManager interfaces.

D. FortiAnalyzer features are not enabled on FortiManager.

Correct Answer: BD

QUESTION 4

View the following exhibit.



If both FortiManager and FortiGate are behind the NAT devices, what are the two expected results? (Choose two.)

A. FortiGate is discovered by FortiManager through the FortiGate NATed IP address.

B. FortiGate can announce itself to FortiManager only if the FortiManager IP address is configured on FortiGate under

central management.

C. During discovery, the FortiManager NATed IP address is not set by default on FortiGate.

D. If the FCFM tunnel is torn down, FortiManager will try to re-establish the FGFM tunnel.

Correct Answer: AC

Fortimanager can discover FortiGate through a NATed FortiGate IP address. If a FortiManager NATed IP address is configured on FortiGate, then FortiGate can announce itself to FortiManager. FortiManager will not attempt to re-establish the FGFM tunnel to the FortiGate NATed IP address, if the FGFM tunnel is interrupted. Just like it was in the NATed FortiManager scenario, the FortiManager NATed IP address in this scenario is not configured under FortiGate central management configuration.

QUESTION 5

Refer to the exhibit.

Which two statements about the output are true? (Choose two.)

A. The latest revision history for the managed FortiGate does match with the FortiGate running configuration

B. Configuration changes have been installed to FortiGate and represents FortiGate configuration has been changed

C. The latest history for the managed FortiGate does not match with the device-level database

D. Configuration changes directly made on the FortiGate have been automatically updated to device-level database

Correct Answer: AC

STATUS: dev-db: modified; conf: in sync; cond: pending; dm: retrieved; conn: up-dev-db: modified - This is the device setting status which indicates that configuration changes were made on FortiManager.- conf: in sync - This is the sync status which shows that the latest revision history is in sync with Fortigate\\'s configuration.- cond: pending - This is the configuration status which says that configuration changes need to be installed. Most probably a retrieve was done in the past (dm: retrieved) updating the revision history DB (conf: in sync) and FortiManager device level DB, now there is a new modification on FortiManager device level DB (dev-db: modified) which wasn\\'t installed to FortiGate (cond: pending), hence; revision history DB is not aware of that modification and doesn\\'t match device DB. Conclusion:- Revision DB does match FortiGate.- No changes were installed to FortiGate yet.- Device DB doesn\\'t match Revision DB.- No changes were done on FortiGate (auto-update) but configuration was retrieved instead After an Auto-Update or Retrieve:device database = latest revision = FGT Then after a manual change on FMG end (but no install yet):latest

revision = FGT (still) but now device database has been modified (is different). After reverting to a previous revision in revision history:device database = reverted revision != FGT

NSE5_FMG-6.4 PDF Dumps | NSE5_FMG-6.4 Study Guide | NSE5_FMG-6.4 Exam Questions