

NSE4_FGT-7.2^{Q&As}

Fortinet NSE 4 - FortiOS 7.2

Pass Fortinet NSE4_FGT-7.2 Exam with 100% Guarantee

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

https://www.leads4pass.com/nse4_fgt-7-2.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 does not want to report the logon events of service accounts to FortiGate. What setting on the collector agent is required to achieve this?

- A. Add the support of NTLM authentication.
- B. Add user accounts to Active Directory (AD).
- C. Add user accounts to the FortiGate group fitter.
- D. Add user accounts to the Ignore User List.

Correct Answer: D

Reference: <https://community.fortinet.com/t5/Support-Forum/Collector-Agent-and-problem-getting-login-info/m-p/95481>

QUESTION 2

Which of the following conditions must be met in order for a web browser to trust a web server certificate signed by a third-party CA?

- A. The public key of the web server certificate must be installed on the browser.
- B. The web-server certificate must be installed on the browser.
- C. The CA certificate that signed the web-server certificate must be installed on the browser.
- D. The private key of the CA certificate that signed the browser certificate must be installed on the browser.

Correct Answer: C

QUESTION 3

You have enabled logging on a FortiGate device for event logs and all security logs, and you have set up logging to use the FortiGate local disk. What is the default behavior when the local disk is full?

- A. No new log is recorded after the warning is issued when log disk use reaches the threshold of 95%.
- B. No new log is recorded until you manually clear logs from the local disk.
- C. Logs are overwritten and the first warning is issued when log disk use reaches the threshold of 75%.
- D. Logs are overwritten and the only warning is issued when log disk use reaches the threshold of 95%.

Correct Answer: C

config log disk setting

set diskfull [overwrite | nolog]

Action to take when disk is full. The system can overwrite the oldest log messages or stop logging when the disk is full. (default --> overwrite)

config log memory global-setting

set full-first-warning-threshold {integer}

Log full first warning threshold as a percent. (default --> 75) Reference:

<https://docs.fortinet.com/document/fortigate/7.2.5/cli-reference/421620/config-log-disk-setting>

<https://docs.fortinet.com/document/fortigate/7.2.5/cli-reference/418620/config-log-memory-global-setting>

Logs are overwritten and the first warning is issued when log disk use reaches the threshold of 75%.

This is true because this is the default behavior of FortiGate when logging to the local disk. The local disk is the internal storage of FortiGate that can be used to store event logs and security logs. When the local disk is full, FortiGate will

overwrite the oldest logs with the newest ones, and issue warnings at different thresholds of disk usage. The first warning is issued when log disk use reaches 75%, the second warning is issued when log disk use reaches 85%, and the final

warning is issued when log disk use reaches 95%. The administrator can configure these thresholds and the action to take when the disk is full using the CLI command config log disk setting1

QUESTION 4

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

- A. The RPF check is run on the first sent packet of any new session.
- B. The RPF check is run on the first reply packet of any new session.
- C. The RPF check is run on the first sent and reply packet of any new session.
- D. RPF is a mechanism that protects FortiGate and your network from IP spoofing attacks.

Correct Answer: AD

Reference: <https://www.programmersought.com/article/16383871634/>

QUESTION 5

Which of the following are valid actions for FortiGuard category based filter in a web filter profile ui proxy-based inspection mode? (Choose two.)

- A. Warning
- B. Exempt
- C. Allow
- D. Learn

Correct Answer: AC

[NSE4_FGT-7.2 PDF Dumps](#)

[NSE4_FGT-7.2 Practice
Test](#)

[NSE4_FGT-7.2 Study Guide](#)