



500-275^{Q&As}

Securing Cisco Networks with Sourcefire FireAMP Endpoints
(SSFAMP)

Pass Cisco 500-275 Exam with 100% Guarantee

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

<https://www.passapply.com/500-275.html>

100% Passing Guarantee
100% Money Back Assurance

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

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





QUESTION 1

Which information does the File Trajectory feature show?

- A. the time that the scan was run
- B. the name of the file
- C. the hosts on which the file was seen and points in time where events occurred
- D. the protocol

Correct Answer: C

QUESTION 2

When discussing the FireAMP product, which term does the acronym DFC represent?

- A. It means Detected Forensic Cause.
- B. It means Duplicate File Contents.
- C. It means Device Flow Correlation.
- D. It is not an acronym that is associated with the FireAMP product.

Correct Answer: C

QUESTION 3

Which tool can you use to query the history.db file?

- A. Curl
- B. FireAMP_Helper.vbs
- C. cscript
- D. SQLite

Correct Answer: D Question Set 1

QUESTION 4

How many days\'' worth of data do the widgets on the dashboard page display?

- A. the previous 5 days of data
- B. the previous 6 days of data



- C. the previous 7 days of data
- D. the number of days you set in the dashboard configuration

Correct Answer: C

QUESTION 5

Which question should be in your predeployment checklist?

- A. How often are backup jobs run?
- B. Are any Linux servers being deployed?
- C. Who are the users of the hosts on which you will deploy?
- D. Which applications are installed on the hosts on which you will deploy?

Correct Answer: D

QUESTION 6

What is the first system that is infected with a particular malware called?

- A. Patient Zero
- B. Source
- C. Infector
- D. Carrier

Correct Answer: A

QUESTION 7

File information is sent to the Sourcefire Collective Security Intelligence Cloud using which format?

- A. MD5
- B. SHA-1
- C. filenames
- D. SHA-256

Correct Answer: D

QUESTION 8



The FireAMP connector monitors the system for which type of activity?

- A. Vulnerabilities
- B. Enforcement of usage policies
- C. File operations
- D. Authentication activity

Correct Answer: C

QUESTION 9

In a FireAMP Private Cloud installation, which server does an administrator use to manage connector policy and view events?

- A. opadmin..com
- B. console..com
- C. cloud..com
- D. aws..com

Correct Answer: B

QUESTION 10

The Accounts menu contains items that are related to FireAMP console accounts. Which menu allows you to set the default group policy?

- A. Audit Log
- B. Users
- C. Applications
- D. Business

Correct Answer: D

[Latest 500-275 Dumps](#)

[500-275 PDF Dumps](#)

[500-275 Exam Questions](#)