NSE5_EDR-5.0 Q&As

Fortinet NSE 5 - FortiEDR 5.0

Pass Fortinet NSE5_EDR-5.0 Exam with 100% Guarantee

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

https://www.geekcert.com/nse5_edr-5-0.html

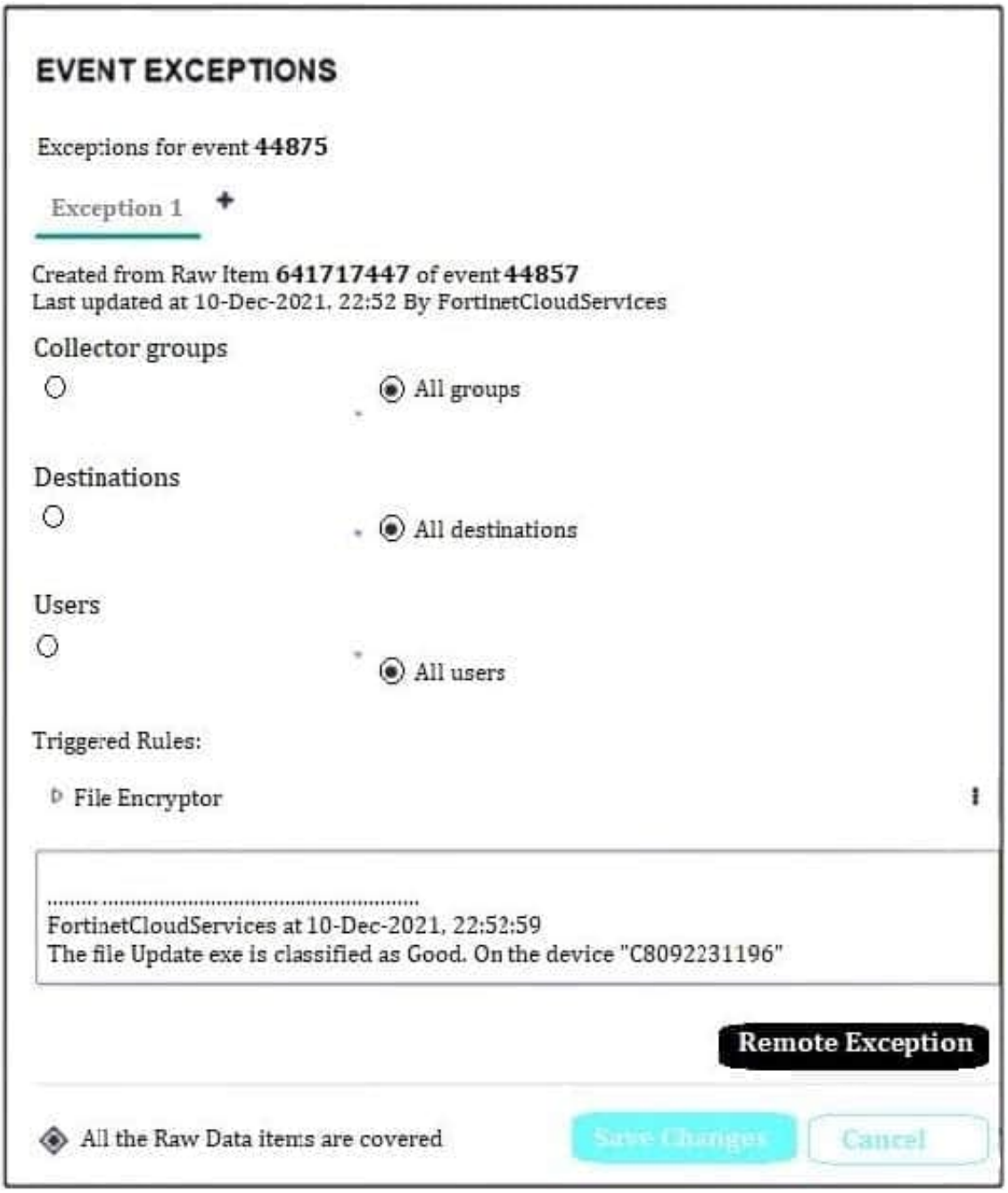
100% Passing Guarantee
100% Money Back Assurance

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

Refer to the exhibit.



Based on the event exception shown in the exhibit which two statements about the exception are true? (Choose two)

A. A partial exception is applied to this event

B. FCS playbooks is enabled by Fortinet support

C. The exception is applied only on device C8092231196

D. The system owner can modify the trigger rules parameters

Correct Answer: AC

QUESTION 2

Which statement is true about the flow analyzer view in forensics?

A. It displays a graphic flow diagram.

B. Two events can be compared side-by-side.

C. It shows details about processes and sub processes.

D. The stack memory of a specific device can be retrieved

Correct Answer: A

QUESTION 3

When installing a FortiEDR collector, why is a `Registration Password\\' for collectors needed?

A. To restrict installation and uninstallation of collectors

B. To verify Fortinet support request

C. To restrict access to the management console

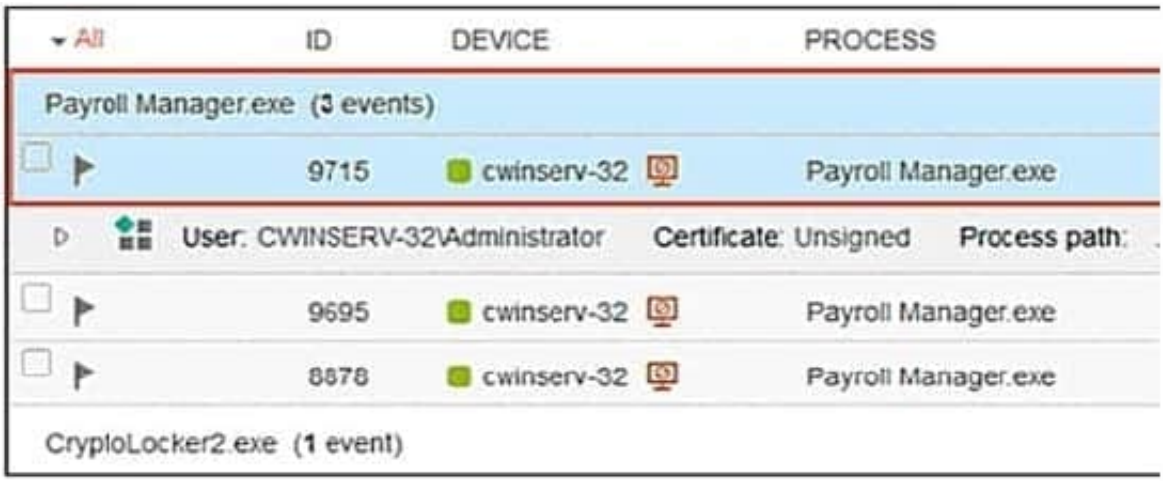
D. To verify new group assignment

Correct Answer: A

QUESTION 4

Refer to the exhibit.

The exhibit shows an event viewer.



What is true about the Payroll Manager.exe event?

A. An event has not been handled by a console admin

B. An event has been deleted

C. A rule assigned action is set to block but the policy is in simulation mode

D. An event has been handled by the communication control policy

Correct Answer: C

QUESTION 5

What is true about classifications assigned by Fortinet Cloud Sen/ice (FCS)?

A. The core is responsible for all classifications if FCS playbooks are disabled

B. The core only assigns a classification if FCS is not available

C. FCS revises the classification of the core based on its database

D. FCS is responsible for all classifications

Correct Answer: C