CCFA-200 Q&As

CrowdStrike Certified Falcon Administrator

Pass CrowdStrike CCFA-200 Exam with 100% Guarantee

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

https://www.passapply.com/ccfa-200.html

100% Passing Guarantee
100% Money Back Assurance

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

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

QUESTION 1

Which is the correct order for manually installing a Falcon Package on a macOS system?

A. Install the Falcon package, then register the Falcon Sensor via the registration package

B. Install the Falcon package, then register the Falcon Sensor via command line

C. Register the Falcon Sensor via command line, then install the Falcon package

D. Register the Falcon Sensor via the registration package, then install the Falcon package

Correct Answer: C

QUESTION 2

Your organization has a set of servers that are not allowed to be accessed remotely, including via Real Time Response (RTR). You already have these servers in their own Falcon host group. What is the next step to disable RTR only on these hosts?

A. Edit the Default Response Policy, toggle the "Real Time Response" switch off and assign the policy to the host group

B. Edit the Default Response Policy and add the host group to the exceptions list under "Real Time Functionality"

C. Create a new Response Policy, toggle the "Real Time Response" switch off and assign the policy to the host group

D. Create a new Response Policy and add the host name to the exceptions list under "Real Time Functionality"

Correct Answer: C

QUESTION 3

You notice there are multiple Windows hosts in Reduced functionality mode (RFM). What is the most likely culprit causing these hosts to be in RFM?

A. A Sensor Update Policy was misconfigured

B. A host was offline for more than 24 hours

C. A patch was pushed overnight to all Windows systems

D. A host was placed in network containment from a detection

Correct Answer: C

QUESTION 4

In order to exercise manual control over the sensor upgrade process, as well as prevent unauthorized users from

uninstalling or upgrading the sensor, which settings in the Sensor Update Policy would meet this criteria?

A. Sensor version set to N-1 and Bulk maintenance mode is turned on

B. Sensor version fixed and Uninstall and maintenance protection turned on

C. Sensor version updates off and Uninstall and maintenance protection turned off

D. Sensor version set to N-2 and Bulk maintenance mode is turned on

Correct Answer: B

QUESTION 5

The Falcon sensor uses certificate pinning to defend against man-in-the-middle attacks. Which statement is TRUE concerning Falcon sensor certificate validation?

A. SSL inspection should be configured to occur on all Falcon traffic

B. Some network configurations, such as deep packet inspection, interfere with certificate validation

C. HTTPS interception should be enabled to proceed with certificate validation

D. Common sources of interference with certificate pinning include protocol race conditions and resource contention

Correct Answer: B