CrowdStrike CCFA

CROWDSTRIKE FALCON ADMINISTRATOR CERTIFICATION QUESTIONS & ANSWERS

Exam Summary – Syllabus – Questions

CCFA

CrowdStrike Certified Falcon Administrator (CCFA)

60 Questions Exam – 80% Cut Score – Duration of 90 minutes

www.VMExam.com

Table of Contents

Know Your CCFA Certification Well:

The CCFA is best suitable for candidates who want to gain knowledge in the CrowdStrike Falcon Platform. Before you start your CCFA preparation you may struggle to get all the crucial Falcon Admin materials like CCFA syllabus, sample questions, study guide.

But don't worry the CCFA PDF is here to help you prepare in a stress free manner.

The PDF is a combination of all your queries like-

- What is in the CCFA syllabus?
- How many questions are there in the CCFA exam?
- Which Practice test would help me to pass the CCFA exam at the first attempt?

Passing the CCFA exam makes you CrowdStrike Certified Falcon Administrator (CCFA). Having the Falcon Admin certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

CrowdStrike CCFA Falcon Admin Certification Details:

Exam Name	CrowdStrike Falcon Administrator
Exam Code	CCFA
Exam Price	$250 USD
Duration	90 minutes
Number of Questions	60
Passing Score	80%
Recommended Training / Books	CCFA Training
Schedule Exam	PEARSON VUE
Sample Questions	CrowdStrike CCFA Sample Questions
Recommended Practice	CrowdStrike Certified Falcon Administrator (CCFA) Practice Test

CCFA Syllabus:

Section	Objectives
User Management	- Determine roles required for access to features and functionality in the Falcon console - Create roles and assign users to roles based on desired permissions - Manage API keys
Sensor Deployment	- Determine prerequisites to successfully install a Falcon sensor on supported operating systems - Analyze the default policies and apply the best practices to prepare workloads for the Falcon sensor - Uninstall a sensor - Troubleshoot a sensor
Host Management and Setup	- Understand how filtering might be used in the Host Management page - Disable detections for a host - Explain the effect of disabling detections on a host - Explain the impact of Reduced Functionality Mode (RFM) and why it might be caused - Find hosts in RFM - Locate inactive sensors - Recall how long inactive sensors are retained - Determine relevant reports specific to host management
Group Creation	- Determine the appropriate group assignment for endpoints and understand how this impacts the application of policies - Apply best practices when managing host groups
Policy Application	- Determine the appropriate prevention policy settings for endpoints and explain how this impacts security posture - Determine the appropriate sensor update policy settings in order to control the update process - Apply roles and policy settings, and track and review Falcon RTR audit logs in order to manage user activity - Understand the functionality of a containment policy - Configure a containment policy for IP address or subnet exclusions that will apply to network

Section	Objectives
	contained hosts based on security workflow requirements - Understand options and requirements to manage quarantined files
Rules Configuration	- Create custom IOA rules to monitor for behavior that is not fundamentally malicious - Interpret business requirements in order to allow trusted activity, resolve false positives and fix performance issues - Assess IOC settings required for customized security posturing and to manage false positives - Understand configurations for CID wide management within General Settings
Dashboards and Reports	- Understand the different types of sensor reports and their use cases - Understand the different audit logs and their use cases
Workflows	- Configure workflows to respond to defined triggers

CrowdStrike CCFA Sample Questions:

Question: 1

Which audit logs are available in the Falcon console for administrative and forensic tracking?

(Choose two)

a) Sensor Kernel Log
b) RTR Audit log
c) Activity Audit Log
d) Application Control Log

Answer: b, c

Question: 2

What does the "Sensor Operational" filter indicate when set in Host Management?

a) Displays only active detections
b) Shows only hosts not in RFM or inactive
c) Groups sensors by policy
d) Filters by sensor version

Answer: b

Question: 3

Which benefits are provided by assigning endpoints to properly structured host groups?

(Choose two)

a) Faster login performance
b) Easier reporting and filtering
c) Consistent policy enforcement
d) Automatic malware removal

Answer: b, c

Question: 4

To ensure rules apply globally across all endpoints in a customer account, administrators must enable _____ management in the General Settings.

a) Regional
b) CID-wide
c) Device group
d) Host-based

Answer: b

Question: 5

When creating a new user role in Falcon, which of the following permissions is required to enable the user to generate API keys?

a) Activity App
b) Hosts Management
c) API Clients and Keys
d) Real Time Response

Answer: c

Question: 6

Which considerations should be made when applying a new prevention policy?

(Choose two)

a) Policy testing on a pilot group
b) Restarting all endpoints
c) Uninstalling existing sensors
d) Reviewing host group priorities

Answer: a, d

Question: 7

Which Falcon platform features assist in locating hosts that may have Reduced Functionality Mode enabled?

(Choose two)

a) Host Management filters using RFM
b) Detection Summary Report
c) Real Time Response session logs
d) RFM column in Host Management table view

Answer: a, d

Question: 8

Which component of a prevention policy controls whether potentially unwanted programs (PUPs) are blocked or allowed?

a) PUP handling
b) Machine learning sensitivity
c) Exploit protection
d) Application control

Answer: a

Question: 9

Which use cases are appropriate for configuring a Falcon workflow?

(Choose two)

a) Forwarding detection data to a SIEM system
b) Updating endpoint hostnames
c) Modifying policy priorities
d) Alerting a SOC team when high-severity detections

Answer: a, d

Question: 10

Which considerations should be made when applying a new prevention policy?

(Choose two)

a) Restarting all endpoints
b) Uninstalling existing sensors
c) Policy testing on a pilot group
d) Reviewing host group priorities

Answer: c, d

Study Guide to Crack CrowdStrike Falcon Admin CCFA Exam:

- Getting details of the CCFA syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the CCFA exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the CrowdStrike provided training for CCFA exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the CCFA sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on CCFA practice tests is must. Continuous practice will make you an expert in all syllabus areas.