CrowdStrike Certified Falcon Administrator (CCFA) Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Sample study guide. For the full version with hundreds of questions, visit: https://crowdstrikefalconadmin.examzify.com

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

Table of Contents

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn’t just about memorization, it’s about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you’re preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You’ll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it’s correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It’s ideal for learners who want to:

- **Practice answering questions under realistic conditions,**
- **Improve accuracy and speed,**
- **Review explanations to strengthen weak areas, and**
- **Approach the exam with greater confidence.**

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn’t about getting every question right the first time, it’s about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let’s begin.

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here’s how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don’t just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There’s no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

Questions

1. **In RTR roles, which role is synonymous with having no rights?**

   A. Read Only

   B. Script Admin/writer

   C. Full Admin

   D. Act.Resp.

2. **What must be running for Web Proxy Automatic Discovery (WPAD) to work during Sensor Deployment?**

   A. DHCP Client

   B. DNS Client

   C. Network Store Interface

   D. Web Proxy Service

3. **To minimize false positives for required applications, what can be created?**

   A. Network security groups

   B. ML Exclusions

   C. Firewall rules

   D. Incident reports

4. **How are prevention policies configured in CrowdStrike?**

   A. Only updated manually

   B. Through a static set of rules

   C. Based on aggressiveness scale for detections and preventions

   D. Automatically linked to sensor updates

5. **Which cloud behavior indicates the sensor is installed on the host during RFM?**

   A. Regular monitoring reports.

   B. Heartbeat signals to the cloud.

   C. Active shutdown notifications.

   D. Error reporting to the dashboard.

6. **Which role in Prevent Roles allows viewing and managing remediation actions?**

   A. **Detections Exceptions Manager**

   B. **Quarantine Manager**

   C. **Falcon Analyst**

   D. **Remediation Manager**

7. **Where are sensor install logs located if the installation is initiated by a user?**

   A. **%LOCALAPPDATA%\Temp**

   B. **%TEMP%\CrowdStrike**

   C. **%USERPROFILE%\Logs**

   D. **%SYSTEMROOT%\Logs**

8. **When deploying sensors on hosts using proxies, which protocol is important to enable?**

   A. **HTTP AutoProxy**

   B. **WinHTTP AutoProxy**

   C. **FTP Proxy**

   D. **Socks Proxy**

9. **In a containment policy, whom can change the containment status?**

   A. **System Administrator**

   B. **Falcon Security Lead**

   C. **Falcon Investigator**

   D. **Falcon Analyst**

10. **How are prevention policy settings typically determined?**

    A. **By random selection**

    B. **Based on business requirements**

    C. **By system settings**

    D. **According to user preferences**

Answers

1. **A**
2. **A**
3. **B**
4. **C**
5. **B**
6. **D**
7. **A**
8. **B**
9. **B**
10. **B**

Explanations

1. In RTR roles, which role is synonymous with having no rights?

A. Read Only

B. Script Admin/writer

C. Full Admin

D. Act.Resp.

The "Read Only" role is designed to provide users with the ability to view data without making any modifications or changes to it. This role is synonymous with having no rights because users assigned this role can access information but lack the permissions to perform any actions that could alter the system or data. Therefore, they can only observe and analyze the current state of the environment without impacting its functionality or security. In contrast, the other roles grant varying levels of access and permission. For instance, "Script Admin/writer" allows users to create and execute scripts, while "Full Admin" provides complete control over the settings, configurations, and actions within the system, enabling users to modify a wide range of elements. Additionally, the "Act.Resp." role focuses on active response capabilities, which allows users to take specific actions based on threat events. Thus, the "Read Only" role stands out as the one that strictly limits user interaction with the system, aligning it with the idea of having no rights.

2. What must be running for Web Proxy Automatic Discovery (WPAD) to work during Sensor Deployment?

A. DHCP Client

B. DNS Client

C. Network Store Interface

D. Web Proxy Service

For Web Proxy Automatic Discovery (WPAD) to function effectively during Sensor Deployment, it is essential for the DHCP Client to be running. WPAD is a method that allows web clients to locate and automatically configure web proxy settings. This is typically achieved through the use of DHCP or DNS services. In the case of DHCP, the DHCP Client is responsible for receiving IP address configurations from a DHCP server, which can include options that aid in the WPAD process. When the DHCP Client is active, it can retrieve the necessary configurations related to proxy settings, allowing the client device to automatically identify and use the appropriate web proxy without manual setup. While DNS Client could potentially play a role in resolving proxy settings if they are provided via DNS, the primary mechanism for WPAD when it comes to automatic discovery is predominantly linked to the DHCP protocol. The Network Store Interface and Web Proxy Service relate to different aspects of network management and proxy management, respectively, and are not directly involved in the fundamental function of WPAD. Hence, the presence of the DHCP Client is crucial for the successful implementation of WPAD during Sensor Deployment.

3. To minimize false positives for required applications, what can be created?

A. Network security groups

B. ML Exclusions

C. Firewall rules

D. Incident reports

Creating ML Exclusions is an effective way to minimize false positives for required applications. Machine Learning (ML) algorithms used in threat detection can sometimes misidentify benign applications or behaviors as malicious, leading to false positives. By establishing ML Exclusions, you inform the system to disregard certain applications or behavioral patterns during its analysis, thereby allowing legitimate applications to run without being flagged as potential threats. This helps maintain operational integrity and reduces unnecessary alerts while ensuring that the security posture remains strong. While other options, such as network security groups, firewall rules, and incident reports, serve important roles in a security framework, they are not specifically aimed at minimizing false positives in the way that ML Exclusions are. Network security groups can manage access and control traffic flows, firewall rules are set to block or allow certain types of traffic, and incident reports are used for documenting security events but do not directly influence the algorithmic classification of applications. Therefore, the establishment of ML Exclusions specifically targets the challenge of minimizing false detections related to trusted applications.

4. How are prevention policies configured in CrowdStrike?

A. Only updated manually

B. Through a static set of rules

C. Based on aggressiveness scale for detections and preventions

D. Automatically linked to sensor updates

Prevention policies in CrowdStrike are configured based on an aggressiveness scale for detections and preventions. This approach allows administrators to tailor the level of sensitivity in threat detection and response to fit the specific needs and risk tolerance of their environment. By leveraging this scale, organizations can determine how aggressively they want the Falcon platform to react to potential threats, thereby facilitating the balance between security and usability. The aggressiveness scale enables administrators to adjust settings dynamically based on their operational requirements, which can change over time. This means that rather than relying on a static set of rules or manual configurations, the system provides flexibility that adapts to evolving threats and organizational needs. The ability to customize aggression levels also reflects an understanding of the varied nature of threats and the importance of context in cybersecurity measures. This method of configuring policies is more efficient and effective in dealing with the complexities of modern cybersecurity threats than merely using static rules or depending solely on manual updates.

5. Which cloud behavior indicates the sensor is installed on the host during RFM?

A. Regular monitoring reports.

B. Heartbeat signals to the cloud.

C. Active shutdown notifications.

D. Error reporting to the dashboard.

The indication that a sensor is installed on the host during Real-Time Monitoring Framework (RFM) is represented by heartbeat signals to the cloud. Heartbeat signals are essential for maintaining communication between the sensor installed on the host and the CrowdStrike cloud service. These signals provide consistent updates about the status of the host, ensuring that the sensor is actively engaged and operational. Regular intervals of these heartbeat signals confirm that the sensor is functioning and able to relay data back to the cloud in real-time, reflecting the ongoing health and activity of the endpoint. In contrast, regular monitoring reports can provide insights into security metrics or trends but do not specifically confirm the presence of a sensor. Active shutdown notifications may inform administrators about host shutdown events but do not indicate ongoing sensor activity. Error reporting to the dashboard can highlight issues or anomalies but, like reports, does not serve as direct evidence of the sensor's active installation. Therefore, heartbeat signals are the most direct indication of the sensor's presence and functionality on the host during RFM.

6. Which role in Prevent Roles allows viewing and managing remediation actions?

A. Detections Exceptions Manager

B. Quarantine Manager

C. Falcon Analyst

D. Remediation Manager

The role that allows viewing and managing remediation actions is the Remediation Manager. This role is designed specifically to oversee the remediation process, which includes the assessment of threats and the implementation of necessary actions to mitigate those threats. The Remediation Manager is equipped with the necessary permissions to view current incidents, track the status of remediations, and execute the actions required to resolve issues identified by the system. This role is critical in maintaining the security posture of an organization as it ensures that threats are not only detected but also effectively managed. Individuals in this role collaborate with other stakeholders, often using insights from detection and monitoring tools to inform their remediation strategies. Having a dedicated role for remediation actions helps prevent overlaps and confusion in responsibilities, thereby streamlining the response to security incidents. In contrast, other roles, while important, do not focus primarily on remediation actions. For instance, the Detections Exceptions Manager may work on setting exceptions for certain detections but does not manage the actual remediation processes. The Quarantine Manager handles the quarantine of detected threats but is not responsible for the entire remediation scope. The Falcon Analyst examines and analyzes incidents but may not directly engage with remediation actions in the same comprehensive manner as the Remediation Manager.

7. Where are sensor install logs located if the installation is initiated by a user?

A. %LOCALAPPDATA%\Temp

B. %TEMP%\CrowdStrike

C. %USERPROFILE%\Logs

D. %SYSTEMROOT%\Logs

The sensor install logs are stored in the %LOCALAPPDATA%\Temp directory when the installation is initiated by a user. This location is specifically designated for temporary files that are user-specific. When the CrowdStrike Falcon sensor is installed by a user, the installation process generates logs that provide details about the installation event, any errors encountered, and other relevant information. Storing these logs in the %LOCALAPPDATA%\Temp ensures that they are accessible only to the user who initiated the installation, maintaining a level of privacy and separation from other users on the system. It is important to note that the other options do not accurately reflect the specific storage location for user-initiated sensor install logs. For instance, while %TEMP%\CrowdStrike and %SYSTEMROOT%\Logs are valid directories that may hold various types of log files in different contexts, they do not serve as the designated area for logs produced from user-initiated installations of the CrowdStrike sensor. %USERPROFILE%\Logs is similarly not where these specific installation logs would be found, as it typically pertains to logs generated by user-specific applications or operations that are not related to the installation process of the Falcon sensor.

8. When deploying sensors on hosts using proxies, which protocol is important to enable?

A. HTTP AutoProxy

B. WinHTTP AutoProxy

C. FTP Proxy

D. Socks Proxy

When deploying sensors on hosts using proxies, enabling the WinHTTP AutoProxy protocol is crucial because it allows applications on Windows systems to automatically configure themselves to use a proxy server for HTTP requests. This protocol is designed specifically for Windows environment settings and enables seamless connections for applications that rely on WinHTTP, ensuring that they can communicate securely and efficiently over the network. The WinHTTP AutoProxy feature plays an essential role in managing proxy configurations dynamically. It allows the operating system to retrieve the proxy configuration from a designated URL, facilitating a central management approach for proxy settings across multiple devices. This is particularly useful in enterprise environments where maintaining consistent proxy settings can enhance security and performance.   In contrast, other protocols like HTTP AutoProxy may be less specific to Windows applications or might not provide the same level of integration with the system's networking stack. FTP Proxy and Socks Proxy serve different purposes in network communication and do not provide the same level of automated proxy configuration for Windows hosts as WinHTTP does. Therefore, relying on WinHTTP AutoProxy is particularly appropriate in scenarios where ease of management and integration with Windows architecture are priorities.

9. In a containment policy, whom can change the containment status?

A. System Administrator

B. Falcon Security Lead

C. Falcon Investigator

D. Falcon Analyst

The Falcon Security Lead has the authority to change the containment status in a containment policy. This role typically involves overseeing security operations and managing incidents, which includes the ability to modify the containment status of endpoints based on the threat landscape and the organization's security posture. Being in a leadership position, the Falcon Security Lead has the responsibility to ensure that containment actions align with the broader security strategy and that any changes to containment status are justified based on the analysis of threats and risks. This level of access is crucial for making informed decisions about when to isolate or re-enable endpoints that may pose a security risk, thus helping to mitigate potential threats effectively. Other roles like the System Administrator, Falcon Investigator, and Falcon Analyst may have important functions within the security team, but the specific authority to change containment status is designated to the Falcon Security Lead to ensure that such critical changes are managed effectively and in accordance with organizational policies.

10. How are prevention policy settings typically determined?

A. By random selection

B. Based on business requirements

C. By system settings

D. According to user preferences

Prevention policy settings are typically determined based on business requirements because these policies are designed to align security measures with the operational needs and risk tolerance of an organization. This involves assessing potential threats, compliance obligations, and the specific assets that need protection. By tailoring the prevention policies to business requirements, organizations can ensure that their security posture effectively mitigates risks while supporting overall business functions. Other factors, such as system settings and user preferences, might play a role in the implementation of these policies, but they do not drive the foundational decisions like business requirements do. Decisions based on random selection are not a strategic approach to security management and do not take into account the unique context of each organization.

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we’d love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://crowdstrikefalconadmin.examzify.com

We wish you the very best on your exam journey. You've got this!