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

Study Guide

Everything you need from our exam experts!

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. Don't worry about getting everything right, 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, and take breaks to retain information better.

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.

7. Use Other Tools

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 terms of roles, what does the term "prevent roles" refer to?**

   A. Roles dedicated to user training and support

   B. Roles with specific access limitations for security management

   C. Roles that only manage financial aspects of the organization

   D. Roles that focus on documentation and support tasks

2. **Which version of TLS must be enabled for Falcon on commercial cloud clients?**

   A. TLS 1.0 or later

   B. TLS 1.1 or later

   C. TLS 1.2 or later

   D. SSL 3.0

3. **Which command is used to uninstall a sensor on a Windows offline host?**

   A. CsUninstallTool.exe

   B. falconctl uninstall

   C. apt-get purge falcon-sensor

   D. yum remove falcon-sensor

4. **Which command can verify if the sensor is connected to the CrowdStrike cloud?**

   A. netstat.exe -f

   B. ping -c 4

   C. tracert

   D. status.txt

5. **When using exclusion patterns, what should you ensure about paths that include spaces?**

   A. Eliminate spaces to create efficient patterns

   B. Include the spaces within the pattern

   C. Avoid using spaces altogether

   D. Use underscores instead of spaces

6. In what format does the Remote Access Graph show connections?

A. A tabular format listing user-specifc data

B. A numeric report of connections made per hour

C. An interactive graph showing user and host connections

D. A textual summary of connection history

7. Which command argument should be included when installing Falcon for Virtual Desktop Infrastructure (VDI)?

A. VDI=0

B. VDI=2

C. VDI=1

D. VDI=3

8. What is the recommended installation method for Falcon on a Mac?

A. Direct download from the website

B. Using an MDM to sync profiles

C. Via command line only

D. Through an installer package

9. Which recommendation is suggested for the default policy in sensor update management?

A. Use auto settings for flexibility

B. Select a static version for stability

C. Disable uninstall protection to streamline updates

D. Apply changes immediately without testing

10. What must be verified when checking **SSL/TLS settings for proper CrowdStrike functionality?**

A. TLS v1.2 / SSL v3

B. Only enable TLS v1.0

C. Disable all SSL and TLS protocols

D. Use self-signed certificates

Answers

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

Explanations

1. In terms of roles, what does the term "prevent roles" refer to?

A. Roles dedicated to user training and support

B. Roles with specific access limitations for security management

C. Roles that only manage financial aspects of the organization

D. Roles that focus on documentation and support tasks

The term "prevent roles" refers to roles with specific access limitations for security management. This concept emphasizes the importance of security roles within an organization that are designed to prevent unauthorized access or actions. The essence of preventive roles is to ensure that individuals in these positions have carefully controlled access to the systems, tools, or data they manage, enabling the enforcement of security policies and protocols designed to minimize risks. By implementing these roles, organizations can mitigate potential security threats and breaches, creating a structured environment where access is granted based on the principle of least privilege. This principle ensures that individuals only have permissions necessary to perform their job functions, ideally reducing the attack surface for potential breaches. In contrast, roles focused on user training and support, managing financial aspects, or handling documentation and support tasks do not primarily revolve around security management and do not encapsulate the concept of 'prevent roles.' These roles play essential functions within the organization but do not focus specifically on access limitations and security protocols needed to prevent unauthorized actions or access.

2. Which version of TLS must be enabled for Falcon on commercial cloud clients?

A. TLS 1.0 or later

B. TLS 1.1 or later

C. TLS 1.2 or later

D. SSL 3.0

TLS (Transport Layer Security) is a cryptographic protocol designed to provide secure communication over a computer network. For Falcon on commercial cloud clients, enabling TLS 1.2 or later is essential. This version of the protocol offers enhanced security features and mitigates vulnerabilities present in earlier versions. TLS 1.2 supports stronger encryption algorithms and provides a more secure framework for data transmission, which is critical for protecting sensitive information in environments that could be targeted by cyber threats. Moreover, many regulatory standards and compliance requirements recommend or mandate the use of TLS 1.2 or newer versions to ensure data integrity and confidentiality. Earlier versions of TLS, like 1.0 and 1.1, while still functional, have known flaws and are often discouraged in favor of TLS 1.2. SSL 3.0 is even older and has significant security vulnerabilities that make it unsuitable for modern secure communication. Therefore, enabling TLS 1.2 or later is the best practice and requirement for maintaining a secure environment in your Falcon deployment on commercial cloud clients.

3. Which command is used to uninstall a sensor on a Windows offline host?

A. CsUninstallTool.exe

B. falconctl uninstall

C. apt-get purge falcon-sensor

D. yum remove falcon-sensor

The command used to uninstall a sensor on a Windows offline host is CsUninstallTool.exe. This tool is specifically designed for use in Windows environments and allows for the removal of the CrowdStrike Falcon sensor even when the host is not connected to the Internet. It is a crucial utility for system administrators managing offline machines that still require security management and remediation. In this context, other commands listed are not applicable for uninstalling a sensor on a Windows offline host. For instance, the command falconctl uninstall is utilized on online systems to manage sensor configurations, while apt-get purge falcon-sensor and yum remove falcon-sensor are commands intended for Linux-based environments, which operate under different package management systems and are not relevant for Windows systems. Thus, the CsUninstallTool.exe command stands out as the appropriate choice for the task at hand.

4. Which command can verify if the sensor is connected to the CrowdStrike cloud?

A. netstat.exe -f

B. ping -c 4

C. tracert

D. status.txt

The command that verifies if the sensor is connected to the CrowdStrike cloud involves checking established network connections. The netstat command, specifically with the -f option, provides a list of active connections and their corresponding remote endpoints, including information about the DNS names associated with those connections. This means that by using this command, an administrator can see if the sensor is successfully communicating with the CrowdStrike cloud, allowing for confirmation of connectivity. In contrast, the other options do not directly provide information about the sensor's connection status with the CrowdStrike cloud. The ping command tests network connectivity to a specific IP address but does not offer direct insights into the specific connections of the CrowdStrike sensor itself. Tracert shows the path that packets take to a destination but doesn't assess the sensor's connection status. Lastly, status.txt is a file generated by the CrowdStrike Falcon sensor that contains various operational details, but it does not actively verify connectivity in real-time like netstat does. Thus, netstat -f is the most suitable command for verifying the sensor's connection status.

5. When using exclusion patterns, what should you ensure about paths that include spaces?

A. Eliminate spaces to create efficient patterns

B. Include the spaces within the pattern

C. Avoid using spaces altogether

D. Use underscores instead of spaces

When working with exclusion patterns in a system like CrowdStrike, it's essential to accurately reflect the file paths as they exist in the operating environment. Including spaces within the path is crucial because many operating systems and applications recognize spaces as significant characters. If spaces are omitted or improperly represented, the exclusion pattern may not match the intended file or directory correctly, potentially leading to unintended results, such as leaving files unprotected or not excluded from scans. Using the correct representation of paths ensures that the system understands the exact location of the files or directories you intend to exclude. This attention to detail helps maintain security and operational integrity by accurately targeting the right elements within the file system.

6. In what format does the Remote Access Graph show connections?

A. A tabular format listing user-specifc data

B. A numeric report of connections made per hour

C. An interactive graph showing user and host connections

D. A textual summary of connection history

The Remote Access Graph presents connections in an interactive graph format that visually represents user and host connections. This visual representation allows administrators to quickly discern patterns, identify anomalies, and analyze the relationships between users and hosts more effectively than standard textual or tabular data would allow. By utilizing an interactive graph, it enables dynamic exploration of the data, where users can manipulate the view to focus on specific aspects, such as particular timeframes or users. This feature is particularly beneficial in cybersecurity, where understanding the flow of connections can assist in detecting unauthorized access or unusual activity within a network.

7. Which command argument should be included when installing Falcon for Virtual Desktop Infrastructure (VDI)?

A. VDI=0

B. VDI=2

C. VDI=1

D. VDI=3

When installing Falcon for Virtual Desktop Infrastructure (VDI), specifying the argument VDI=1 is essential. This command indicates that the installation is tailored for a VDI environment, allowing the Falcon sensor to properly configure itself for the unique characteristics and requirements associated with virtual desktop infrastructures. In a VDI setup, the operating conditions differ from that of traditional endpoint installations, mainly because VDI environments often host multiple user sessions on a single physical machine. Setting the installation argument to VDI=1 ensures that the sensor operates correctly in this environment, optimizing performance and resource utilization while ensuring effective security monitoring. This choice aligns with best practices for deploying Falcon in environments designed for virtual desktops, ensuring comprehensive protection without compromising system performance or user experience.

8. What is the recommended installation method for Falcon on a Mac?

A. Direct download from the website

B. Using an MDM to sync profiles

C. Via command line only

D. Through an installer package

The recommended installation method for Falcon on a Mac is through an MDM (Mobile Device Management) to sync profiles. This method allows for a streamlined installation process across multiple devices, which is particularly advantageous in enterprise environments. By utilizing an MDM, organizations can deploy the Falcon agent efficiently, manage configuration settings, and ensure compliance across all managed devices. MDM also supports the automation of installations and updates, reducing the burden on IT resources and maintaining consistent security protocols throughout the organization. Using an MDM enables centralized control, allowing IT administrators to easily push policies, monitor installations, and track compliance without needing manual intervention for each individual device. This method also enhances security by allowing for consistent application of security policies, profiles, and apps, promoting a more robust and unified security posture across all devices within the organization.

9. Which recommendation is suggested for the default policy in sensor update management?

A. Use auto settings for flexibility

B. Select a static version for stability

C. Disable uninstall protection to streamline updates

D. Apply changes immediately without testing

Selecting a static version for stability in sensor update management is a recommended best practice. This approach ensures that the sensor remains on a known and tested version of the Falcon sensor, decreasing the likelihood of introducing issues that may arise from new updates. Stability is crucial in maintaining the operational integrity of endpoint protection; using a static version helps avoid potential disruptions or vulnerabilities that could occur with automatic updates or newer versions that have not undergone extensive testing in your specific environment. This strategy is especially important for organizations where system reliability is paramount, allowing IT teams to manage and schedule updates based on their individual needs and testing protocols. By prioritizing a static version, organizations can ensure that the security infrastructure remains predictable and controlled, minimizing risks associated with rapid changes.

10. What must be verified when checking **SSL/TLS settings** for proper CrowdStrike functionality?

A. TLS v1.2 / SSL v3

B. Only enable TLS v1.0

C. Disable all SSL and TLS protocols

D. Use self-signed certificates

Verifying the SSL/TLS settings for proper CrowdStrike functionality involves ensuring that TLS v1.2 is enabled, as it is a secure and widely accepted protocol for encrypted connections. Using outdated protocols like SSL v3 or older versions of TLS can expose systems to vulnerabilities and attacks, as these protocols are no longer considered secure. TLS v1.2 offers improved security features, such as stronger encryption algorithms and protection against specific types of attacks, making it essential for maintaining the integrity and confidentiality of data in transit. Ensuring that only TLS v1.2 is in use helps maintain compliance with security best practices and standards, which is crucial for the effective deployment of CrowdStrike services.

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!