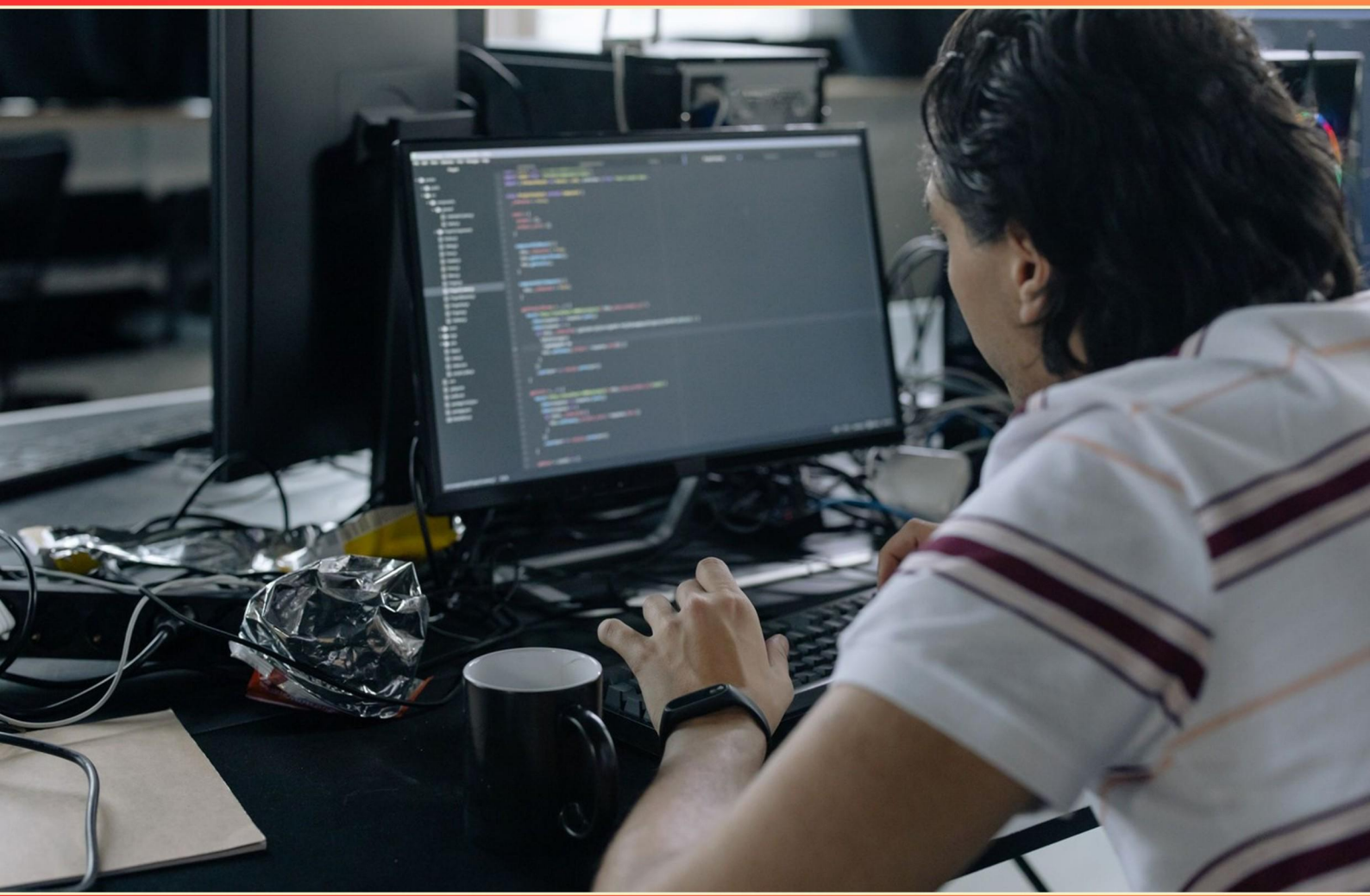
SISE IMPLEMENTING AND CONFIGURING CISCO IDENTITY SERVICES ENGINE PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://siseciscoidentityservicesengine.examzify.com

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. **Which protocol is primarily used for managing network devices securely within Cisco ISE?**

   A. SSH

   B. RADIUS

   C. HTTPS

   D. IPSec

2. **Which option is considered a TACACS+ configuration option in Cisco ISE?**

   A. TACACS+ version

   B. Management User Name

   C. Observation node to which the client connected

   D. Shared Secret

3. **Which three of the following are steps that should be taken as part of planning for Profiler usage?**

   A. Ensure that guest access is configured properly.

   B. Enable pxGrid services globally.

   C. Identify endpoints that require device identification.

   D. Configure 802.1X and MAB authentication policies for profiling.

4. **Which section of the RADIUS live log details report shows all events processed by Cisco ISE during the endpoint session lookup?**

   A. A. Overview

   B. B. Authentication Details

   C. C. Results

   D. D. Steps

5. **What are 'User Defined Attributes' in Cisco ISE used for?**

   A. To create user groups based on sales performance

   B. To customize additional user information for policy enforcement

   C. To track user login times

   D. To determine hardware specifications of user devices

6. What type of policies can be created in Cisco ISE?

A. Only network security policies

B. Access policies, authorization policies, and profiling policies

C. General IT policies across all devices

D. Hardware inventory policies

7. What effect does dynamic adjustment of access permissions have in Cisco ISE?

A. It creates user accounts automatically

B. It enhances network traffic speeds

C. It ensures compliance with security policies

D. It prevents all unauthorized users from accessing the network

8. How does Cisco ISE protect sensitive information during transmission?

A. By using basic text encoding for data

B. By employing encryption protocols such as SSL/TLS

C. By restricting access to sensitive information

D. By implementing lower-quality encryption for faster performance

9. Which menu path will display a table to inspect RADIUS events in real time from the Cisco ISE GUI?

A. A. Context Visibility > Endpoints

B. B. Policy > Policy Sets

C. C. Operations > RADIUS live log

D. D. Context Visibility > Users

10. Which Cisco TrustSec feature uses EAP-FAST to authenticate devices and negotiates IEEE 802.1AE encryption?

A. A. Endpoint Admission Control

B. B. security group

C. C. Network Device Admission Control

D. D. SGT

Answers

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

Explanations

1. Which protocol is primarily used for managing network devices securely within Cisco ISE?

A. SSH

B. RADIUS

C. HTTPS

D. IPSec

The most suitable protocol for managing network devices securely within Cisco Identity Services Engine (ISE) is SSH (Secure Shell). SSH is a cryptographic network protocol that provides a secure channel over an unsecured network in a client-server architecture, allowing for encrypted communication between devices. In the context of Cisco ISE, SSH is frequently employed to manage switches, routers, and other network devices securely. This is essential for the protection of administrative tasks and access, ensuring that commands sent to network devices remain confidential and are resistant to eavesdropping or man-in-the-middle attacks. Other options may serve different purposes in networking: - RADIUS (Remote Authentication Dial-In User Service) is primarily used for authentication, authorization, and accounting (AAA) services rather than direct management access. - HTTPS (Hypertext Transfer Protocol Secure) is used for secure communication over a computer network, particularly for web interfaces and APIs, but it is not specifically designed for device management in the same way SSH is. - IPSec (Internet Protocol Security) is a set of protocols used to secure Internet Protocol (IP) communications by authenticating and encrypting each IP packet in a communication session. It is more associated with securing end-to-end connections rather than managing devices directly. Therefore, SSH

2. Which option is considered a TACACS+ configuration option in Cisco ISE?

A. TACACS+ version

B. Management User Name

C. Observation node to which the client connected

D. Shared Secret

The correct option regarding TACACS+ configuration in Cisco Identity Services Engine (ISE) is the TACACS+ version. This choice is fundamental in establishing how the TACACS+ protocol functions within an ISE environment. Different versions of TACACS+ may introduce distinct features or modifications in behavior, meaning that specifying the correct version is crucial for ensuring compatibility and functionality between Cisco ISE and the devices that will be communicating with it using TACACS+. While management user names and shared secrets are indeed part of the TACACS+ configuration, they are specific parameters rather than overarching configuration options such as the version itself. The management user name is essential for authentication processes but does not influence the protocol's operational characteristics. Similarly, the shared secret is critical for securing the communication between the TACACS+ server and the client, but again, it does not dictate how the protocol itself operates, unlike the version number, which defines the underlying protocol mechanics. The observation node, which refers to the ISE node that a client connects to for monitoring purposes, is not a TACACS+ configuration parameter at all. Therefore, focusing on the version highlights a key aspect of TACACS+ configuration that is essential for proper integration within the Cisco ISE framework.

3. Which three of the following are steps that should be taken as part of planning for Profiler usage?

A. Ensure that guest access is configured properly.

B. Enable pxGrid services globally.

C. Identify endpoints that require device identification.

D. Configure 802.1X and MAB authentication policies for profiling.

Identifying endpoints that require device identification is a crucial step in planning for Profiler usage within Cisco Identity Services Engine (ISE). This step directly impacts how effectively the Profiler can work to classify and profile devices in your network. By knowing which devices need to be identified, an organization can tailor its strategies to ensure that these devices are appropriately monitored and regulated. Profiling helps in maintaining security and compliance by giving visibility into the types of devices connecting to the network. Understanding which endpoints are critical for identification allows network administrators to set up necessary policies and configurations that can enhance their overall security posture. This tailored approach aids in efficient device management and consistent application of policies relevant to different device types. While other choices relate to different aspects of set-up and configuration, they do not focus on the specific need for device identification as an initial step. Therefore, identifying these endpoints is foundational for effectively implementing profiling capabilities in ISE.

4. Which section of the RADIUS live log details report shows all events processed by Cisco ISE during the endpoint session lookup?

A. A. Overview

B. B. Authentication Details

C. C. Results

D. D. Steps

The section of the RADIUS live log that shows all events processed by Cisco ISE during the endpoint session lookup is the Steps section. This section provides a detailed chronological account of the individual actions or steps that Cisco ISE took while handling the RADIUS request. In the Steps section, you can observe how ISE processed the authentication request, including the checks performed against various identity stores, policies that were applied, and any decision-making logs that occurred as part of the session lookup. It outlines the flow of operations during the session, making it easier for administrators to troubleshoot issues or understand the specific actions taken during the authentication process. The Overview section typically provides a high-level summary rather than the nitty-gritty details of the processes that took place. The Authentication Details section focuses more on the specific authentication method used and its outcome, while the Results section provides final outcomes of the authentication attempt without venturing into the series of events that occurred during processing. Therefore, the Steps section is where one would look for an in-depth analysis of the session lookup events.

5. What are 'User Defined Attributes' in Cisco ISE used for?

A. To create user groups based on sales performance

B. To customize additional user information for policy enforcement

C. To track user login times

D. To determine hardware specifications of user devices

User Defined Attributes in Cisco Identity Services Engine (ISE) serve the primary purpose of customizing additional user information that can be leveraged for policy enforcement within the ISE framework. Organizations often have unique requirements for how they manage and apply rules to user access, and these attributes allow administrators to extend the existing user data model beyond the default options. By defining custom attributes, organizations can tailor access policies to reflect their specific operational needs, facilitating more granular control over what resources users can access based on various criteria, such as roles, departments, or other significant information. This can enhance security by ensuring that policies are closely aligned with the organization's requirements. The other options highlight various functions that do not align with the purpose of User Defined Attributes in ISE. For instance, creating user groups based on sales performance or tracking login times pertains more to management and auditing functions rather than to customizing attributes for policy enforcement. Likewise, determining hardware specifications of user devices revolves around device profiling rather than user attributes, which are specifically concerned with identity and user characteristics.

6. What type of policies can be created in Cisco ISE?

A. Only network security policies

B. Access policies, authorization policies, and profiling policies

C. General IT policies across all devices

D. Hardware inventory policies

The answer focuses on the range of policy types that can be created within Cisco Identity Services Engine (ISE). Cisco ISE is known for its robust policy framework that allows for granular control over access and authorization based on a variety of criteria. Access policies are foundational in Cisco ISE, as they define the level of access a user or device is granted based on their identity, role, location, and the device they're using. These policies may incorporate attributes such as user group membership or device type, enabling tailored access that enhances network security. Authorization policies are another crucial component. They determine what resources a user or device can access once their identity has been verified. This can involve restrictions or permissions at multiple levels, ensuring that users only have access to resources that are appropriate for their roles. Profiling policies serve to identify and categorize devices connecting to the network. This information is vital for determining appropriate access rights and for visibility into network usage. By profiling endpoints, Cisco ISE can apply pertinent security policies based on device type, operating system, or specific attributes. This range of policy types—access, authorization, and profiling—demonstrates the comprehensive capabilities of Cisco ISE in enforcing security across a network, making these policies integral to the effective functioning of the service

7. What effect does dynamic adjustment of access permissions have in Cisco ISE?

A. It creates user accounts automatically

B. It enhances network traffic speeds

C. It ensures compliance with security policies

D. It prevents all unauthorized users from accessing the network

Dynamic adjustment of access permissions in Cisco Identity Services Engine (ISE) plays a crucial role in maintaining compliance with security policies. This functionality allows ISE to evaluate and modify the access rights of users and devices based on their current security posture, role, or context. For example, if a user's device is found to be non-compliant with the organization's security policies—such as having outdated antivirus software or missing security patches—the ISE can dynamically adjust the access control permissions for that device. This might mean limiting the device's access to certain resources or placing it in a remediation VLAN until it meets the required compliance standards. By ensuring that only compliant devices and users can access specific network resources, ISE helps organizations uphold their security policies and mitigate risks. This feature also supports adaptive security models that evolve with the changing threat landscape, promoting a more robust approach to network security management.

8. How does Cisco ISE protect sensitive information during transmission?

A. By using basic text encoding for data

B. By employing encryption protocols such as SSL/TLS

C. By restricting access to sensitive information

D. By implementing lower-quality encryption for faster performance

Cisco Identity Services Engine (ISE) protects sensitive information during transmission by employing robust encryption protocols such as SSL/TLS. These protocols create a secure channel that encrypts the data being sent over the network, ensuring that even if the data is intercepted, it cannot be easily read or manipulated. SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are widely used to secure data transmission over the internet and between network devices, providing confidentiality and integrity during the data exchange process. Utilizing these encryption methods helps to maintain the privacy of sensitive information, such as user credentials and identity attributes. This protection is essential for organizations to prevent unauthorized access and data breaches, particularly in environments where sensitive identity and access management data is being handled. In contrast, basic text encoding provides no security, and restricting access alone does not encrypt the data that is transmitted. Implementing lower-quality encryption could compromise the security in favor of performance, which is not a suitable strategy for protecting sensitive information.

9. Which menu path will display a table to inspect RADIUS events in real time from the Cisco ISE GUI?

A. A. Context Visibility > Endpoints

B. B. Policy > Policy Sets

C. C. Operations > RADIUS live log

D. D. Context Visibility > Users

The correct answer is the option that leads to the Operations > RADIUS live log section in the Cisco ISE GUI. This path is specifically designed for monitoring and inspecting RADIUS events in real time. When you navigate to this section, it provides a detailed view of all RADIUS authentication and accounting messages, allowing administrators to see live data related to user authentications, rejections, and other RADIUS-related activities. In contrast, the other menu paths serve different purposes. For example, Context Visibility > Endpoints focuses on displaying information about devices that have connected to the network, including their roles and attributes, but it does not provide the specific real-time logging of RADIUS events. Similarly, Policy > Policy Sets is used for configuring and managing authentication and authorization policies rather than monitoring real-time event logs. Lastly, Context Visibility > Users provides insights into user activities and profiles but lacks the real-time event logging functionality specific to RADIUS. Therefore, choosing the Operations > RADIUS live log path is essential for effective real-time monitoring of RADIUS events.

10. Which Cisco TrustSec feature uses EAP-FAST to authenticate devices and negotiates IEEE 802.1AE encryption?

A. A. Endpoint Admission Control

B. B. security group

C. C. Network Device Admission Control

D. D. SGT

The correct answer focuses on Network Device Admission Control (NDAC), which plays a vital role in the Cisco TrustSec architecture. NDAC employs the Extensible Authentication Protocol - Fast (EAP-FAST) for authenticating devices on the network. This authentication process is crucial for ensuring that only legitimate and safe devices gain access to network resources. In conjunction with EAP-FAST, NDAC also negotiates IEEE 802.1AE encryption, which is fundamental for securing the communication between the endpoint and the network infrastructure. This encryption ensures that data is transmitted securely, protecting against eavesdropping and tampering. NDAC facilitates a robust security posture by not only authenticating devices but also ensuring they are correctly classified and assigned the appropriate Security Group Tags (SGTs). This adds another layer of security by determining what resources network devices are permitted to access based on their group classifications. This process is central to TrustSec's ability to implement role-based access control and enforce security policies dynamically, providing a more secure and manageable network environment.

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://siseciscoidentityservicesengine.examzify.com

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