SALESFORCE CERTIFIED IDENTITY AND ACCESS MANAGEMENT PRACTICE (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://salesforcecertifiediam.examzify.com

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

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

SAMPLE

Table of Contents

Copyright 1

Table of Contents 2

Introduction 3

How to Use This Guide 4

Questions 5

Answers 8

Explanations 10

Next Steps 16

SAMPLE

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.

SAMPLE

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!

SAMPLE

Questions

SAMPLE

1. **Which protocols are commonly associated with Salesforce Identity for SSO?**

   A. POP3, SMTP, and FTP

   B. SAML, OAuth, and OpenID Connect

   C. RTSP, HTTP, and HTTPS

   D. LDAP, RADIUS, and Kerberos

2. **What parameter allows the ability to use the access_token on the Web, including access to Visualforce pages?**

   A. Session ID

   B. Scope

   C. Token

   D. Web Scope

3. **What is recommended before allowing users to log in with SAML assertions?**

   A. Disable the SAML org preference

   B. Test without using a developer edition

   C. Map internal usernames and Salesforce usernames

   D. Use the My Domain feature to prevent direct logins

4. **What are Access Tokens used for in Salesforce?**

   A. Are used to make authenticated requests FOR the user

   B. Must be protected from interception (via Transport Layer Security: TLS)

   C. Have a longer lifetime than authorisation codes

   D. Are a type of OAuth token, known as the Session ID

5. **What does MFA stand for, and why is it important?**

   A. Multi-Factor Authentication; it enhances account security

   B. Multi-Form Acknowledgment; it verifies user actions

   C. Multi-Failure Analysis; it assesses system vulnerabilities

   D. Manual Function Assessment; it requires physical checks

SAMPLE

6. What is the significance of a "Security Token" in Salesforce?

A. A unique code used to verify user identity during API calls or when accessing Salesforce from untrusted networks

B. A backup code for password recovery

C. A method of encrypting sensitive data

D. An identifier for Salesforce subscriptions

7. What is true about the SAML Assertion Flow in Salesforce?

A. Is used when the customer wants to access the web services API in the same way, i.e. using signed assertions

B. OAuth means users can connect to apps

C. Used to make authenticated requests FOR the user

D. Are a type of OAuth token, known as the Session ID

8. What is crucial to include in an SSO configuration for user security across orgs?

A. Shared passwords

B. Master list of usernames

C. Unique Federated ID for each user

D. Public authentication endpoint

9. What type of data do ID Tokens contain in Salesforce?

A. Are encoded as a JSON web token

B. Are signed data structures

C. Contain user ID, time issued and client ID

D. Have a longer lifetime than authorisation codes

10. What does the term "Community User" refer to in Salesforce?

A. Internal users who manage data

B. External users accessing Salesforce through Communities

C. Users who focus on system security

D. Employees accessing Salesforce from remote locations

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which protocols are commonly associated with Salesforce Identity for SSO?

A. POP3, SMTP, and FTP

B. SAML, OAuth, and OpenID Connect

C. RTSP, HTTP, and HTTPS

D. LDAP, RADIUS, and Kerberos

The protocols commonly associated with Salesforce Identity for Single Sign-On (SSO) include SAML, OAuth, and OpenID Connect because these protocols are specifically designed to facilitate secure authentication and authorization across different applications and services. SAML (Security Assertion Markup Language) is widely used for exchanging authentication and authorization data between an identity provider and a service provider, making it ideal for enabling SSO in web applications. It allows users to authenticate once and gain access to multiple applications without needing to log in each time. OAuth is a protocol that allows for secure delegated access, enabling users to grant third-party applications limited access to their resources without sharing their passwords. This protocol supports various use cases, including SSO, by allowing users to authenticate using their existing accounts from identity providers. OpenID Connect builds on top of OAuth, providing an identity layer. It allows clients to verify the identity of the user based on the authentication performed by an authorization server, facilitating SSO by allowing users to log in using credentials from an OpenID provider. Together, these protocols provide comprehensive support for SSO, enhancing user experience by streamlining authentication processes while maintaining security and user privacy.

2. What parameter allows the ability to use the access_token on the Web, including access to Visualforce pages?

A. Session ID

B. Scope

C. Token

D. Web Scope

The ability to use an access token on the web, particularly for accessing Visualforce pages, is indeed associated with the concept of "Web Scope." This parameter specifies that the access token can be used in a web context, enabling applications to work seamlessly with web resources, such as Visualforce pages. In this scenario, the Web Scope is vital as it grants the necessary permissions and capabilities for web-based interactions. It facilitates the secure use of tokens beyond mobile or non-web environments, ensuring that web applications can leverage them appropriately. The importance of distinguishing web-centric scopes cannot be overstated, especially in the context of integrations and accessing Salesforce's offerings through web interfaces. The other options pertain to different aspects of Salesforce's identity and access management. Session IDs, for example, are specifically tied to user sessions and do not inherently provide the same scope for web interactions as the Web Scope does. Similarly, while "Scope" and "Token" are essential elements in the OAuth framework, they do not specifically refer to web use in the same way that Web Scope does.

SAMPLE

3. What is recommended before allowing users to log in with SAML assertions?

A. Disable the SAML org preference

B. Test without using a developer edition

C. Map internal usernames and Salesforce usernames

D. Use the My Domain feature to prevent direct logins

Allowing users to log in with SAML assertions is an important step in implementing secure identity management. The recommended practice of using the My Domain feature helps ensure that login processes are managed correctly and securely. By enabling My Domain, an organization can create a custom domain name that enhances control over user logins and makes certain features, such as SAML, work smoothly. It prevents direct logins to the Salesforce default domain, which protects against potential security vulnerabilities and ensures that all user access goes through the configured login pages where SAML assertions can be validated appropriately. While other considerations like disabling SAML org preferences or mapping usernames are important in a broader context, the My Domain feature specifically aligns with best practices for securely managing user access through SAML. It focuses on enabling features that enhance security and control over user authentication processes.

4. What are Access Tokens used for in Salesforce?

A. Are used to make authenticated requests FOR the user

B. Must be protected from interception (via Transport Layer Security: TLS)

C. Have a longer lifetime than authorisation codes

D. Are a type of OAuth token, known as the Session ID

Access Tokens in Salesforce are primarily used to make authenticated requests on behalf of the user. They essentially carry the necessary information to access a protected resource, such as user data or API endpoints, after the user has been authenticated and authorized. By using an Access Token, an application can interact with Salesforce APIs securely and access resources that the user has granted permission to. This makes option A the correct answer. Option B is not the primary purpose of Access Tokens but is indeed essential for ensuring the security of the token and maintaining the confidentiality of the information it carries. Option C is incorrect because Access Tokens generally have a shorter lifetime compared to authorization codes. Access Tokens are designed to be short-lived to reduce the risk of unauthorized access. Option D is not accurate as Access Tokens are not the same as Session IDs. Access Tokens are a type of OAuth token that is specifically used for accessing resources, while Session IDs are used for maintaining a user's session in Salesforce.

SAMPLE

5. What does MFA stand for, and why is it important?

A. Multi-Factor Authentication; it enhances account security

B. Multi-Form Acknowledgment; it verifies user actions

C. Multi-Failure Analysis; it assesses system vulnerabilities

D. Manual Function Assessment; it requires physical checks

Multi-Factor Authentication (MFA) is a security mechanism that requires users to provide two or more verification factors to gain access to a resource, such as an application or online account. The importance of MFA lies in its ability to significantly strengthen account security by adding additional layers of protection beyond just a username and password. With MFA, even if an attacker is able to obtain a user's password through phishing or other means, they would still need the additional authentication factors to access the account. These factors can include something the user has (like a smartphone with an authentication app), something the user knows (like a password), or something the user is (like a fingerprint). This multi-layered approach reduces the likelihood of unauthorized access, making it a critical component of modern security practices. Other options, while they may pertain to security and verification in some contexts, do not accurately describe the widely recognized concept of MFA, nor do they convey its significance in enhancing security protocols in today's digital environment. Thus, MFA remains a foundational element in safeguarding user accounts and sensitive data.

6. What is the significance of a "Security Token" in Salesforce?

A. A unique code used to verify user identity during API calls or when accessing Salesforce from untrusted networks

B. A backup code for password recovery

C. A method of encrypting sensitive data

D. An identifier for Salesforce subscriptions

A "Security Token" in Salesforce plays a critical role in verifying user identity, especially during API calls or when accessing Salesforce from untrusted networks. It adds an extra layer of security by functioning as a unique code that works in conjunction with the user's password. When a user attempts to log in to Salesforce from a network that the system does not recognize, such as a public Wi-Fi connection, the security token ensures that the access attempt is safe and authorized. This mechanism is particularly important in safeguarding sensitive data and preventing unauthorized access. Users must append their security token to their password when they log in through the API, thus confirming that they are legitimate users attempting to access their accounts, even in less secure environments. In contrast, other options do not accurately represent the role of a security token. While backup codes for password recovery or data encryption methods are important, they do not relate to the functionality of a security token. Similarly, identifying subscriptions is unrelated to user authentication and access management, which is the primary purpose of the security token within Salesforce.

SAMPLE

7. What is true about the SAML Assertion Flow in Salesforce?

A. Is used when the customer wants to access the web services API in the same way, i.e. using signed assertions

B. OAuth means users can connect to apps

C. Used to make authenticated requests FOR the user

D. Are a type of OAuth token, known as the Session ID

The SAML Assertion Flow is specifically designed for scenarios where an application needs to authenticate users using SAML assertions. This flow facilitates secure single sign-on (SSO) experiences, allowing users to access applications without needing to enter their credentials multiple times. The use of signed assertions in this context ensures that the identity provider has securely provided the user's identity and any associated attributes. The correct answer emphasizes the role of signed assertions in providing a method for users to access APIs in a manner consistent with the protocol's security standards. This is particularly relevant in environments where secure communication and user identity verification are critical. The other options, while related to different authentication and authorization contexts, do not accurately describe the SAML Assertion Flow. For instance, the concept of OAuth pertains to a different mechanism for granting access to applications without sharing passwords, and while OAuth can indeed facilitate user connectivity, it operates under a different framework than SAML. Similarly, authenticated requests in general can be made in various ways, but the scope of the SAML Assertion Flow is focused on how identity is asserted and doesn't specifically entail the broader authenticated request capabilities. Additionally, Session IDs are a different type of token compared to SAML assertions, which do not fall under the OAuth token category.

8. What is crucial to include in an SSO configuration for user security across orgs?

A. Shared passwords

B. Master list of usernames

C. Unique Federated ID for each user

D. Public authentication endpoint

Including a unique Federated ID for each user in an SSO configuration is essential for maintaining user security across different organizations. A unique Federated ID allows the identity provider to distinctly recognize and authenticate each user, even if other identifiers, like usernames or email addresses, overlap across systems. This uniqueness is vital to prevent unauthorized access, data breaches, and identity confusion that could arise from shared usernames or passwords across multiple services. Using a unique Federated ID helps ensure that access rights and user attributes are properly managed and that each user's session can be accurately tracked and governed. This setup not only enhances security by providing a clear link between an identity and its corresponding permissions but also facilitates easier auditing and management of user identities across different platforms. While shared passwords, a master list of usernames, or a public authentication endpoint may sound helpful, they do not provide the same level of granularity and security that a unique identifier offers. Shared passwords can lead to vulnerabilities if credentials are exposed; a master list of usernames could become a target for attackers; and public authentication endpoints, while useful for connectivity, do not inherently manage security unless tied to unique identifiers for each user.

SAMPLE

9. What type of data do ID Tokens contain in Salesforce?

A. Are encoded as a JSON web token

B. Are signed data structures

C. Contain user ID, time issued and client ID

D. Have a longer lifetime than authorisation codes

ID Tokens in Salesforce contain critical information about the user and the context of authentication. Specifically, they include the user ID, the time the token was issued, and the client ID. This data is essential for identifying the user and securely communicating their identity to the application. The user ID helps the application recognize whom the token corresponds to, while the issuance time is important for assessing the validity and freshness of the token. The client ID ties the authentication to a specific application, ensuring that the identity being represented is part of an allowed entity within the Salesforce ecosystem. While other aspects of ID tokens, such as their encoding or their signed nature, are important, the fundamental purpose of the ID Token revolves around conveying user identity and related metadata, making this option the most directly relevant.

10. What does the term "Community User" refer to in Salesforce?

A. Internal users who manage data

B. External users accessing Salesforce through Communities

C. Users who focus on system security

D. Employees accessing Salesforce from remote locations

The term "Community User" in Salesforce specifically refers to external users who access Salesforce through Communities. Communities in Salesforce are designed to extend the functionality of the Salesforce platform to external users, such as customers, partners, or any stakeholders who need to interact with your business. These users typically have limited access compared to internal users and can access shared data, collaborate on projects, or create cases, all while remaining within the defined boundaries and permissions set up by the organization. This access is typically managed through community licenses, which provide a tailored user experience focused on the needs of these external users. The other options represent different user categories that do not specifically pertain to the concept of Community Users. Internal users managing data refers to users with full access within the company, not the external collaboration aspect emphasized by Community Users. Users focusing on system security is a role that may exist but is not specific to external community interactions. Finally, employees accessing Salesforce remotely do not define Community Users, since they are usually internal employees who have full access to the company's Salesforce instance.

SAMPLE

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://salesforcecertifiediam.examzify.com

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

SAMPLE