Certification Exam Guide

SALESFORCE CERTIFIED IDENTITY AND ACCESS MANAGEMENT DESIGNER

Spring'18

CONTENTS

ABOUT THE SALESFORCE CERTIFIED IDENTITY AND ACCESS MANAGEMENT DESIGNER CREDENTIAL

The Salesforce Certified Identity and Access Management Designer credential is designed for Identity professionals who want to demonstrate their knowledge, skills and abilities in assessing identity architecture; designing secure, high-performance access management solutions on the Lightning Platform. The Identity professional is also effective at communicating technical solutions to business and technical stakeholders.

An Identity Professional should be able to do in order to pass the exam:

- Design an identity architecture that may span multiple platforms and include integration and authentication across systems.
- Articulate system design considerations, benefits and recommendations for an identity architecture.
- Apply general identity and access management best practices to Salesforce implementations.

SECTION 1. PURPOSE OF THIS EXAM GUIDE

This Exam Guide is designed to help candidates evaluate their readiness to pass the Salesforce Certified Identity and Access Management Designer exam. This guide provides information about the target audience for the certification exam, recommended training and documentation, and a complete list of exam objectives; all with the intent of helping candidates achieve a passing score. Salesforce highly recommends a combination of on-the-job experience, and self-study to maximize the likelihood of passing the exam.

SECTION 2. AUDIENCE DESCRIPTION: SALESFORCE CERTIFIED IDENTITY AND ACCESS MANAGEMENT DESIGNER

A Salesforce Certified Identity and Access Management Designer is able to assess the environment and requirements to design secure and scalable identity management solutions on the Lightning Platform. The designer has experience designing and implementing complex identity and access management strategies; as well as communicating the solution and design trade-offs to business and technical stakeholders alike.

The Salesforce Certified Identity and Access Management Designer has the following background:

- One year of Identity and Access Management experience
- One year of Salesforce experience with a major component security setup and design
- Two years of Securities Technology experience

Typical job roles may include:

- Enterprise Architect
- Technical Architect
- Security Architect
- Corporate Integration Architect
- Identity Architect

The Salesforce Certified Identity and Access Management Designer candidate has the experience, skills, knowledge, and ability to:

- Describe the configuration requirements of delegated authentication in Salesforce.
- Describe the configuration requirements of SAML in Salesforce.
- Distinguish the difference between Identity Provider Initiated SAML and Service Provider Initiated SAML and when to use each.
- Describe how trust is established between an Identity Provider and a Service Provider.
- Determine the general identity federation capabilities that are available for a given project.
- Explain high-level concepts and flows of OAuth.
- Explain high-level concepts and flows of SAML.

- Explain high-level concepts and flows of OpenID Connect.
- Explain Social Sign-On in the context of Salesforce.
- Explain authentication mechanisms for Communities.
- Identify the cause and resolve common failure conditions for SSO in Salesforce.
- Explain why a solid SSO strategy is important for enterprise security.
- Describe why Two Factor Authentication is important and strategies for implementing it in Salesforce.
- Explain the use of Login Flows.
- Determine the applicable use cases for Identity Connect.
- Describe when to and how to implement App Launcher.
- Determine appropriate user lifecycle management techniques (automated user provisioning, just-in-time provisioning, manual account creation, etc.) for a given project.

A candidate for this exam will likely need assistance to:

- Configure Salesforce to support SSO.
- Configure Salesforce for automated user lifecycle management via user provisioning and Connected Apps.
- Configure Salesforce to support Social Sign-On and Registration.

A candidate for this exam is not expected to know:

- Specific IDP technology capabilities outside of Salesforce

SECTION 3. ABOUT THE EXAM

The Salesforce Certified Identity and Access Management Designer exam has the following characteristics:

- Content: 60 multiple-choice/multiple-select questions* (5 unscored questions will be added)
- Time allotted to complete the exam: 120 minutes (time allows for unscored questions)
- Passing Score: 65%
- Registration fee: USD 400, plus applicable taxes as required per local law
- Retake fee: USD 200, plus applicable taxes as required per local law
- Delivery options: Proctored exam delivered onsite at a testing center or in an online proctored environment. Click here for information on scheduling an exam.
- References: No hard-copy or online materials may be referenced during the exam.
- Prerequisite: None

*Please note that as of November 16, 2017, all Salesforce certification exams will contain five additional, randomly placed, unscored questions to gather data on question performance. The duration of each exam has been evaluated and adjusted to accommodate the inclusion of the unscored questions. These five questions will be in addition to the 60 scored questions on your exam, and will have no impact whatsoever on your score.

SECTION 4. RECOMMENDED TRAINING AND REFERENCES

As preparation for this exam, Salesforce recommends a combination of: hands-on experience, training course completion, Trailhead trails, and self-study in the areas listed in the Exam Outline section of this exam guide.

To access the most comprehensive training list, download a copy of our Salesforce Guide to Certification available here.

To enroll in instructor-led courses and launch online training from your Salesforce application, click the **Help & Training** link in the upper right corner of the screen (requires login) and search for the desired courses. Non-Salesforce customers can register for instructor-led courses here.

To review online Documentation, Tip Sheets, and User Guides – search for the topics listed in the Exam Outline section of the exam guide and study the information related to those topics. Documentation, Tip Sheets, and User Guides can also be accessed through **Help & Training.**

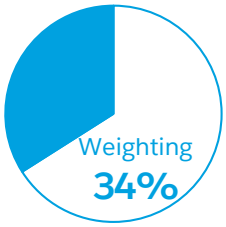
TRAILHEAD TRAILMIX

Check out the official Certification Trailmix for this credential. We have included essential Trailhead learning specifically with you in mind.

SECTION 5. EXAM OUTLINE

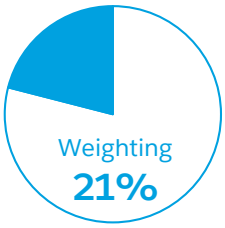
The Salesforce Certified Identity and Access Management Designer exam measures a candidate's knowledge and skills related to the following objectives.

IDENTITY MANAGEMENT CONCEPTS



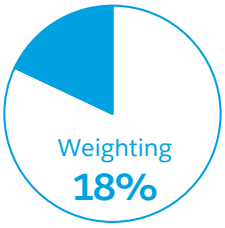
- Describe the role(s) an identity provider and service provider play in an access control solution.
- Describe common methods how trust connections are established between two systems and the methodologies used to describe trust between an identity provider and service provider.
- Given a scenario, articulate whether it is describing an authentication, authorization, or accounting scenario and what Salesforce feature should be used to accomplish the task.
- Given a scenario, recommend the appropriate method for provisioning users in Salesforce and other third party services (SOAP/REST API, SAML JIT, Identity Connect, User Provisioning for Connected Apps, etc.)
- Describe the risks to enterprise security that federated single sign-on solutions aim to address.
- Given a scenario, troubleshoot common points of failure that may be encountered in a single sign-on solution (SAML, OAuth, etc.).

ACCEPTING 3RD PARTY IDENTITY IN SALESFORCE



- Describe the components of an identity management solution where Salesforce is accepting identity from a 3rd party.
- Given a scenario, recommend the appropriate authentication mechanism when Salesforce needs to accept 3rd Party Identity (Enterprise Directory, Social, Community, etc.)
- Given a scenario, recommend the appropriate method of SAML initiation to fulfill the requirements (SP-init, IdP-init.)
- Describe the components of a Delegated Authentication solution.
- Describe the risks of implementing delegated authentication.

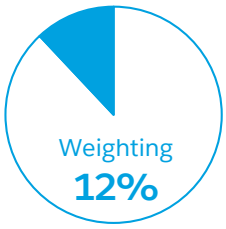
SALESFORCE AS AN IDENTITY PROVIDER



- Given a scenario, determine the most appropriate flow type to recommend when implementing an OAuth solution where Salesforce is providing identity to a 3rd party (E.g. User Agent, Web Server, JWT, etc.)
- Describe the various implementation concepts of OAuth (E.g. scopes, secrets, tokens, refresh tokens, token expiration, token revocation, etc.)

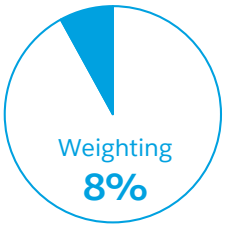
- Describe the role(s) Connected Apps play when Salesforce needs to provide identity to a third party system.
- Given a scenario, recommend the Salesforce technologies that should be used to provide identity to the 3rd party system. (Canvas, Connected Apps, App Launcher, etc.).

ACCESS MANAGEMENT BEST PRACTICES



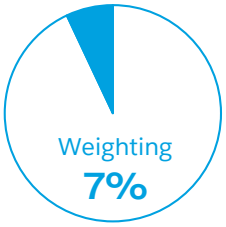
- Describe the risks that Two-Factor Authentication mechanisms aim to mitigate.
- Given a scenario, determine the most appropriate Two-Factor Authentication mechanism for an identity solution.
- Given a scenario, identify the risks and mitigation strategies that session security and Two-Factor Authentication enable (E.g. High Assurance Sessions, 2FA, etc.).

SALESFORCE IDENTITY



- Given a scenario, recommend the most appropriate Salesforce license type(s) to support the identity requirements.
- Describe the role(s) Identity Connect plays in an Identity Management solution.

COMMUNITY (PARTNER AND CUSTOMER)



- Describe the capabilities for customizing the registration experience for external communities (E.g. Branding options, self-registration, communications, etc.).

SECTION 6. SAMPLE EXAM QUESTIONS

The following questions are representative of those on the Salesforce Certified Identity and Access Management Designer exam. These questions are *not* designed to test your readiness to successfully complete the certification exam, but should be used to become familiar with the types of questions on the exam. The actual exam questions may be more or less difficult than this set of questions.

1. Universal Containers (UC) uses Google Apps for email and is the first application all of its users go to when they start their day. UC would also like to use Salesforce's App Launcher capability to access other applications, such as Workday, SAP, and Concur. UC would like its users to only use one set of credentials.

   Which system's credentials should UC use?

   Choose one answer

   A. Salesforce
   B. SAP
   C. Google Apps
   D. Workday

2. Universal Containers (UC) has chosen to implement a hub-and-spoke Salesforce org strategy where a subset of users in the hub org should be able to access resources in any of the spoke orgs. The IT team at UC has decided they would like to manage users in the hub org and automatically create those users in the spoke orgs, as needed, to reduce administrative burden. They will configure the hub org as an Identity Provider and use SAML to authenticate users in the spoke orgs.

   What is the recommended solution for automatically creating users in the spoke orgs?

   Choose one answer

   A. Use an IdP-initiated SAML flow and Custom SAML JIT Provisioning to create users in the spoke orgs.
   B. Use an IdP-initiated SAML flow and Salesforce SAML JIT Provisioning to create users in the spoke orgs.
   C. Use the Salesforce REST API to create users in the spoke orgs when they are created in the hub org.
   D. Use Identity Connect to provision users in the spoke orgs when they try to log in from the hub org.

3. What are three advantages of implementing a federated Single Sign-on solution?

   Chose three answers

   A. Reduced IT help desk costs due to fewer password resets.
   B. Centralized provisioning and de-provisioning of users.
   C. All Service Provider credentials will be synchronized.
   D. Users cannot access Salesforce with Salesforce credentials.
   E. Increased adoption of applications by end users.

4. Which three attributes can be used to represent the identity of the user when Salesforce is acting as a Service Provider in a SAML configuration?

   Choose three answers

   A. Salesforce User ID
   B. Salesforce Username
   C. Federation ID
   D. User Email Address
   E. User Full Name

5. Universal Containers (UC) has acquired Global Shipping (GS) and the IT integration teams have been tasked with merging GS's Salesforce org into UC's Salesforce org. UC had been using Active Directory Federation Services (ADFS) as a SAML IdP for Salesforce with no multifactor authentication capabilities, while GS had been using a third-party IdP with a tightly coupled software-based one-time password generator for Two-factor authentication.

   The CIO of UC would preferably like the new org to continue to use ADFS as the IdP due to budget cutbacks, but would like to maintain the multifactor authentication capabilities GS is used to for Salesforce. The CIO is open to options.

   What is the recommended solution the Architect should recommend to the CIO?

   Choose one answer

   A. Enhance and use the existing software-based one-time password generator and continue to use ADFS as the IdP.
   B. Continue to use ADFS as the IdP and enable native Salesforce Two-factor Authentication for the UC org.
   C. Replace ADFS with the IdP from GS and expand the use of the existing software-based one-time password generator.
   D. Find a less expensive IdP on the AppExchange that has multifactor capabilities and use for all UC and GS users.

SECTION 7. ANSWERS TO SAMPLE EXAM QUESTIONS

1. C
2. A
3. A, B, E
4. A, B, C
5. B

SECTION 8. MAINTAINING A CERTIFICATION

One of the benefits of holding a Salesforce credential is always being up to date on new product releases. Our release exams are designed to ensure you have the latest information you need to be a successful Salesforce Certified expert.

Bookmark these useful resources for maintaining your credentials:

- Maintenance Exam Due Dates
- Credential Status Request Overview
- Overall Maintenance Requirements

Don't let your hard-earned credential expire! Once you earn the credential, if you do not complete all maintenance requirements by the due date, your credential will expire, or in some cases, become suspended. For more information, click here.

ABOUT TRAILHEAD

Trailhead is your path into the Salesforce economy. It's the fun way to learn the skills you need to transform your company, earn credentials that grow your career, and connect with a global movement of Trailblazers to continue learning together.