multisoft
Systems

Salesforce Certified Identity and Access Management Architect Training

COURSE CONTENT

GET IN TOUCH

Multisoft Systems
B - 125, Sector - 2, Noida

(+91) 9810-306-956

info@multisoftsystems.com

www.multisoftsystems.com

About Multisoft

Train yourself with the best and develop valuable in-demand skills with Multisoft Systems. A leading certification training provider, Multisoft collaborates with top technologies to bring world-class one-on-one and certification trainings. With the goal to empower professionals and business across the globe, we offer more than 1500 training courses, which are delivered by Multisoft's global subject matter experts. We offer tailored corporate training; project Based Training, comprehensive learning solution with lifetime e-learning access, after training support and globally recognized training certificates.

About Course

The Salesforce Certified Identity and Access Management Architect training offered by Multisoft Systems is designed to empower professionals aiming to specialize in the intricate mechanisms of identity and access management within the Salesforce platform. This course equips participants with the essential skills and knowledge to effectively design and implement robust identity solutions, manage complex access control scenarios, and navigate Salesforce's extensive security models with confidence.

Module 1: Identity Management Concepts

- ✓ Common authentication patterns and understand the differences between each one.
- ✓ The building blocks that are part of an identity solution (authentication, authorization, & accountability) and how you enable those building blocks using Salesforce features.
- ✓ How trust is established between two systems.
- ✓ Recommend the appropriate method for provisioning users in Salesforce.
- ✓ Troubleshoot common points of failure that may be encountered in a single sign-on solution (SAML, OAuth, etc.)

Module 2: Accepting Third-Party Identity in Salesforce

- ✓ Describe when Salesforce is used as a Service Provider.
- ✓ Recommend the most appropriate way to provision users from identity stores in B2E and B2C scenarios.
- ✓ Recommend the appropriate authentication mechanism when Salesforce needs to accept 3rd Party Identity (Enterprise Directory, Social, Community, etc.).
- ✓ Identify the ways that users can be provisioned in Salesforce to enable SSO and apply access rights.
- ✓ Identify the auditing and monitoring approaches available on the platform, and describe the tools that are available to diagnose IdP issues.

Module 3: Salesforce as an Identity Provider

- ✓ Identify the most appropriate OAuth flow (Web based, JWT, User agent, Device auth flow).
- ✓ Recommend appropriate Scope and Configuration of the connected App for Authorization.
- ✓ The various implementation concepts of OAuth (scopes, secrets, tokens, refresh tokens, token expiration, token revocation, etc.).

- ✓ Recommend the Salesforce technologies that should be used to provide identity to the 3rd party system. (Canvas, Connected Apps, App Launcher, etc.).

Module 4: Salesforce as an Identity Provider

- ✓ A set of requirements, determine the most appropriate methods of multi-factor authentication to use, and the right type of session they should yield.
- ✓ How should you best assign roles, profiles, and permission sets to a user during the SSO process, how would you keep these assignments up to date.
- ✓ Describe what tools you can apply to audit and verify the activity/user during and after login.
- ✓ Identify the configuration settings for a Connected app.

Module 5: Salesforce Identity

- ✓ A set of requirements, identify the role Identity Connect product plays in a Salesforce Identity implementation.
- ✓ Identify if Salesforce Customer 360 Identity fits into a fully developed Customer 360 solution.
- ✓ A set of requirements, recommend the most appropriate Salesforce license type(s).

Module 6: Community (Partner and Customer)

- ✓ The capabilities for customizing the user experience for Experience Cloud (Branding options, authentication options, identity verification self-registration, communications, password reset etc.).
- ✓ A set of requirements, determine the best way to support external identity providers in communities and leverage the right user/contact model to support community user experience.
- ✓ A requirement, understand the advantages and limitations of External Identity solutions and associated licenses.
- ✓ Determine when to use embedded login.