Module 1: Introduction to Identity and Access Management

- Understand Identity and Access Management concepts.
- Define Identity Management.
- Define Access Management.

Module 2: ForgeRock AM Installation and Configuration

- Configure ForgeRock AM with default settings.
- Set up Tomcat for deployment.
- Deploy the ForgeRock AM war file.

Module 3: LDAP Configuration and Operations

- Provide an overview of LDAP.
- Set up the OpenDJ Directory server configuration.
- Set up the Apache Directory Studio LDAP browser.
- Work with LDAP operations, covering basic operations such as search, create, and modify.

Module 4: Custom Configuration in ForgeRock AM

- Configure ForgeRock AM with custom settings.
- Implement custom configurations using OpenDJ.

Module 5: Authentication Mechanisms in ForgeRock AM

- Describe the authentication mechanism of AM.
- Understand default authentication.
- Identify realm-level authentication settings.
- Change the default authentication process.
- Create various Authentication Modules.
- Create Authentication Chains.
- Implement Multi-Factor Authentication (MFA) with email OTP and ForgeRock Authenticator mobile app.
- Observe various cookies.
- Implement Intelligent Authentication.

Module 6: Authentication Trees in ForgeRock AM

- Understand the Trees within AM.
- Compare tree and chain mechanisms.

- List available nodes.
- Implement various Authentication Trees.
- Increase authentication security with features such as account lockout and risk-based authentication.
- Configure second-factor authentication.

Module 7: User Empowerment through Self-Service

- Configure user self-service features.
- Implement user registration methods.
- Implement forgot username and forgot password methods.

Module 8: Retrieving User Information with REST API

- Use the REST API to connect with ForgeRock AM.
- Retrieve user profile information using REST API Postman.

Module 9: Working with OpenIDM

- Set up OpenIDM.
- Implement user self-service mechanisms.
- Create LDAP connectors.
- Map multiple DataStores.

Module 10: Social Authentication Integration

- Configure social authentication using Google within OpenIDM.
- Configure social authentication using Google within OpenAM.

Module 11: OAuth2.0 Integration

- Discuss different OAuth components.
- Explain the OAuth2.0 Flow.
- Configure AM as an OAuth2.0 authorization server.
- Discuss different types of Grants.
- Configure Authorization Code, Authorization Code with PKCE, Implicit grant, Client Credentials, Resource Owners Password Credentials, and Refresh Token.
- Describe OAuth2 access tokens, refresh tokens, and authorization codes.

Module 12: OIDC1.0 Integration

- Configure AM as an OIDC provider.
- Implement applications with OIDC1.0.

- Test OIDC applications with Postman.
- Difference between the OAuth2.0 and OIDC1.0

Module 13: Clustering and High Availability in ForgeRock AM

- Discuss different deployment models.
- Explore various approaches to providing high availability.

Module 14: SSO with SAML2

- Discuss different authentication flows: SP Initiated SSO, IDP Initiated SSO.
- Discuss different logout flows: SP Initiated SLO, IDP Initiated SLO.
- Configure AM as a SAML2 IDP.
- Configure Salesforce as a SAML2 SP.
- Create and test the Circle of Trust between AM and Salesforce.
- Use the SAML Tracer for testing and troubleshooting the Salesforce SAML connection.