ForgeRock Access Management Core Concepts (AM-400)

This structured course comprises a mix of instructor-led lessons and demonstrations with plenty of lab exercises to ensure an opportunity to fully understand each of the topics covered. It provides students with a strong foundation for the design, installation, configuration, and administration of a ForgeRock® Access Management (AM) solution. The objective of the course is to present the core concepts of access management, demonstrate the many features of AM, and provide hands-on experience that allows students to implement a full solution based on real-life use cases, including many ready-to-use features.
Note: Revision B.1 of this course is built on version 6.5 of ForgeRock AM.

Target Audiences

This course is aimed at those responsible for overseeing various aspects of a successful deployment of ForgeRock AM. This includes, but is not limited to, those with the following responsibilities:

- System Integrators
- System Consultants
- System Architects
- System Developers
- System Administrators

Objectives

Upon completion of this course, you should be able to:

- Implement default authentication with AM
- Configure web agents to control access
- Enable user self-service self-registration basic flow
- Configure intelligent authentication with trees
- Configure an identity store
- Retrieve user information with REST
- Configure policies to control access
- Extend entitlements using step-up authentication and transactional authorization
- Configure AM as an OIDC provider and an UMA authorization server
- Demonstrate OAuth2, OIDC, and UMA2 flows
- Configure social authentication with Google
- Customize AM themes for end-user pages
- Investigate the need to harden AM security
- Install, upgrade, and maintain an AM solution
- Discuss AM clustering
- Configure AM as a SAML2 entity

Prerequisites

The following are the prerequisites to successfully completing this course:

- Knowledge of Unix/Linux commands and text editing
- An appreciation of HTTP and web applications

- A basic appreciation of how directory servers function
- A basic understanding of REST
- A basic knowledge of Java based environments would be beneficial. Programming experience is not required.

Course Contents

Chapter 1: Performing Basic Configuration

Lesson 1: Implementing Default Authentication

- Describe how to use AM to manage default authentication using cookies
- Implement default authentication with AM
- Understand the need for and the use of realms
- Implement separation of admins and users using realms
- Observe the function of cookies

Lesson 2: Protecting a Website

- List and describe AM authentication clients
- Describe web agent main functionality
- Implement policy enforcement using web agents
- Analyze the am-auth-jwt cookie

Lesson 3: Empowering Users Through Self-Service

- Describe the main capabilities of user self-service
- Configure user self-service self-registration basic flow

Chapter 2: Implementing Intelligent Authentication

Lesson 1: Extending Authentication Functionality

- Describe the authentication mechanisms of AM
- List the available nodes
- Compare tree and chain mechanisms
- Identify realm-level authentication settings
- Use the authentication tree designer and ForgeRock's Marketplace
- Create and test an authentication tree containing an LDAP Decision node
- Use the recording tool for troubleshooting

Lesson 2: Retrieving User Information

- Understand the use of an identity store
- Explain the distinction between identity store and credentials store
- Implement user-specific features on the website
- Retrieve user profile information using REST

Lesson 3: Increasing Authentication Security

- Discuss the need to increase authentication security
- Implement account lockout
- Configure risk-based authentication
- Configure second-factor authentication
- Demonstrate push notification authentication

Chapter 3: Controlling Access Using Authorization

Lesson 1: Controlling Access

- Describe how AM manages entitlements through authorization
- Define policy components
- Explain how AM evaluates policies
- Implement access control policies on a website

Lesson 2: Extending Entitlements

- Define session upgrade
- Describe and implement step-up authentication
- Describe and implement transactional authorization
- Tighten access for the rest of the website

Chapter 4: Extending Services Using OAuth 2.0-Based Protocols

Lesson 1: Integrating Low-Level Devices with OAuth 2.0 (OAuth2)

- Explain why OAuth2 protocol can be used to integrate various devices
- Discuss OAuth2 players and their roles
- Describe OAuth 2 access tokens, refresh tokens, and authorization codes
- List OAuth2 grants
- Configure AM as an OAuth2 authorization server
- Demonstrate OAuth2 device flow

Lesson 2: Integrating Mobile Applications with OpenID Connect 1.0 (OIDC)

- Explain how OIDC leverages an OAuth2 handshake to provide authentication and data sharing
- List OIDC grants
- Configure AM as an OIDC provider
- Observe the OIDC authorization grant profile

Lesson 3: Sharing Resources with UMA 2.0 (UMA2)

- Describe how UMA2 enriches OAuth2 to allow resource sharing
- Implement AM as an UMA2 authorization server and demonstrate resource sharing

Lesson 4: Implementing Social Authentication

- Explain how AM can delegate authentication to social media
- Configure social authentication using Google

Chapter 5: Preparing for Production

Lesson 1: Customizing AM End User Pages

- Describe the user interface areas that can be customized
- Theme the end user interface for a realm

Lesson 2: Hardening AM Security

- Highlight the areas where security needs hardening
- Adjust default settings
- Set up administration privileges
- Manage secrets
- Use a Hardware Security Management (HSM) secret store to sign OIDC ID token

Lesson 3: Administering an AM Solution

- Introduce the administration tools available
- Install Amster
- Export and explore configuration with Amster
- Identify tools to troubleshoot issues
- Record debugging information
- Outline the main features of audit logging
- List the available monitoring tools
- Discuss the areas that need tuning

Lesson 4: Installing and Upgrading AM

- Plan an AM installation
- Install a single instance of AM using the wizard
- Describe the bootstrap process
- Upgrade an AM instance using the wizard

Lesson 5: Clustering AM

- Discuss approaches to providing high availability
- Explain how to scale a deployment
- Add a server to a cluster using CTS-based sessions
- Modify the cluster to use client-based sessions
- Discuss deployment approaches

Chapter 6: Federating Across Entities Using SAML v.2 (SAML2)

Lesson 1: Implementing Single Sign-On Using SAML2

- Discuss federation entities and flows
- Explain the SSO flow from the Identity Provider (IdP) point of view
- Examine SSO between Service Provider (SP) and IdP and across SPs

Lesson 2: Delegating Authentication Using SAML2

- Explain the SSO flow from the SP point of view

- Describe the metadata content and use
- Configure AM as a SAML2 SP