Course Description

AM-421 Revision B.3

Ping Training

training@pingidentity.com

PingAM: Customization and APIs

Ping Identity is starting to rebrand all products and courses under the Ping Identity brand. The content will remain the same and our curriculum developers will continue to prioritize courses that need development.

Description

This course provides a hands-on technical introduction to PingAM (AM), formerly known as ForgeRock® Access Management, APIs and customization use cases. Students examine AM extension points and gain the skills required to extend and integrate an AM deployment in a real-world context. Additionally, students learn to implement various clients that communicate with AM. Further information and guidance can be found in the documentation and knowledge base in the online repositories at: Backstage https://backstage.forgerock.com.

Note: This course revision is based on version 7.3 of PingAM.

Target Audiences

The target audiences for this course include:

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

Objectives

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

- This chapter provides a high-level overview of the PingAM (AM) configuration architecture
- Extend and customize PingAM (AM) authentication processing by using authentication trees and a custom authentication node
- Explore how to use the PingAM (AM) authorization policy sets, polices, and policy evaluation, and create custom policy conditions with Java and scripts
- Explore how to use the PingAM (AM) REST API, in the context of a web client application, for authenticating users with AM and AM authentication trees
- Describe how to extend a web client application with the ability to authenticate and authorize a user by using OAuth 2.0 (OAuth2) for authentication, and implement Open Identity Connect (OIDC) claims by using the scripting API

Prerequisites

The following are the prerequisites for successfully completing this course:

- Completion of the PingAM Essentials course available at:

  https://backstage.forgerock.com/university/forgerock/on-demand/path/TGVhcm5pbmdQYXRoOjI%3D/chapter/Q291cnNlOjE1NzIy

- Knowledge of UNIX/Linix commands
- An understanding of HTTP and web applications
- A basic understanding of how directory servers function
- A basic understanding of REST
- A basic knowledge of Java based environments would be beneficial, but no programming experience is required.

Duration

5 days

Course Contents

Chapter 1: Introducing Customization in PingAM

This chapter provides a high-level overview of the PingAM (AM) configuration architecture, the interfaces through which its

functionality can be accessed, and the way its behavior can be customized or extended.

Lesson 1: Using Extension (Customization) Points

Describe a high-level overview of the AM architecture, the interfaces through which its functionality can be accessed, and the way its behavior can be customized or extended:

- List extension (customization) points of AM
- List customizable AM components
- Quiz questions
- Access the lab environment
- Manage the course application components

Chapter 2: Customizing Authentication

Extend and customize PingAM (AM) authentication processing by using authentication trees and a custom authentication node.

Lesson 1: Authentication With Trees and Nodes: An Introduction

Introduce authentication trees and nodes and how to configure an authentication tree:

- Understand how AM performs authentication
- Describe AM authentication trees and nodes
- Compare tree and chain mechanisms
- Quiz questions
- Create an authentication tree with default nodes
- Test the authentication tree

Lesson 2: Customizing Authentication Trees and Nodes

Prepare a coding build environment and generate a custom authentication node using a Maven archetype:

- Describe custom authentication nodes
- Prepare a build environment
- Generate a custom node with a Maven archetype
- List custom node classes
- Customize node outcomes
- Deploy the custom node
- Modify custom node configuration and logic
- Post-authentication hooks for trees
- Quiz questions
- Create initial custom authentication node source files

- Modify the custom node's implementation to be dynamic
- Deploy and test the custom authentication node
- Test the authentication tree with the custom node

Lesson 3: Developing Scripts With the Scripting API

Introduce scripting, how scripts work, what they can be used for, and how they can be managed through the AM admin UI:

- Understand the basic concepts of scripting
- Understand the scripting environment and the scripting API
- Use the AM admin UI to manage scripts
- Use the REST API to manage scripts
- Develop client and server scripts
- Use decision scripted authentication nodes in trees
- Quiz questions
- Explore client-side scripting with authentication nodes
- Create an authentication tree with client-side and server-side scripts
- Write a server-side script that uses a REST API request

Lesson 4: Migrating Authentication Modules to Trees and Nodes

Describe the design and implementation issues when migrating authentication modules to trees and nodes:

- Describe design principles for trees and nodes
- List design and implementation steps
- Choose node types
- Map files from modules to nodes
- Authentication modules as nodes
- Migrate an LDAP chain to a tree
- Migrate post-authentication plugins
- Handle logout notifications
- Configure redirection URLs
- Implement account lockout
- Link a chain to a tree and return custom failure messages
- Quiz questions
- Reference an article about migrating chains to trees

Chapter 3: Customizing Authorization

Explore how to use the PingAM (AM) authorization policy sets, polices, and policy evaluation, and create custom policy conditions with Java and scripts.

Lesson 1: Customizing Authorization

Explore the AM authorization framework and the concepts central to it, such as policy sets (applications), policies, and the policy evaluation flow:

- Understand the policy concepts in AM
- Identify the situation when a custom condition is needed
- Customize policy evaluation with a plugin and an Entitlement Condition class
- Implement a scripted condition
- Quiz Questions
- Explore the ContactList REST APIs and policy design
- Create resource types and a policy set
- Write a policy condition checking for maintenance mode
- Modify the policy condition script to provide additional information

Chapter 4: Customizing With REST Clients

Explore how to use the PingAM (AM) REST API, in the context of a web client application, for authenticating users with AM and AM authentication trees.

Lesson 1: Using the REST API

Introduce the AM REST services and the Common REST API, how to invoke REST services from a JavaScript application, and how to configure CORS in AM:

- Describe AM REST API services and the Common REST API
- Understand the Common REST API
- Explore REST API sorting, versioning, and status codes
- Use AM services from a browser-based application
- Enable CORS
- Quiz questions
- Study the ContactList application architecture
- Configure the CORS filter in AM
- Create a login service that uses AM authentication

Lesson 2: Authenticating With REST

Implement authentication and logout in a client application with the AM REST API either using a simple (header-based) approach or a more complex approach, where the server may request additional information from the client using callbacks:

- Review authentication and introduce RESTful authentication
- Implement authentication with the simple REST API
- Implement authentication with the full REST API
- Describe callback types available in AM
- Handle session upgrade and logout with the REST API
- Implement RESTful token and session management
- Use REST to manage identities
- Manage realms with the REST API
- Lesson Quiz
- Implement a fully functional AM-based authentication in ContactList
- Modify the login service to use the authentication tree

Lesson 3: Working With RESTful User Self-Service APIs

Discuss how a browser-based application can use the self-service API to perform operations on behalf of the user such as registration, password reset, and displaying the user dashboard:

- Describe the self-service REST API
- Configure AM for self-service
- Implement password reset with REST
- Self-register a user via REST
- Lesson quiz
- Prepare AM for the password reset functionality
- Examine the password reset protocol
- Extend ContactList with a password reset feature

Lesson 4: Authorizing With REST

Demonstrate how the AM REST API policy management and evaluation works, and how it can be utilized to protect resources that are either actual URLs or other entities like actions:

- Understand how to use the policy engine to protect resources other than URLs
- Describe the policy management REST API
- Describe the policy evaluator REST API
- Implement fine-grained authorization using policies and the REST API
- Lesson quiz
- Prepare AM for ContactList authorization
- Extend the backend to use the authorization REST API
- Extend the front-end application to use AM

Chapter 5: Federating With OAuth2

Describe how to extend a web client application with the ability to authenticate and authorize a user by using OAuth 2.0 (OAuth2) for authentication, and implement Open Identity Connect (OIDC) claims by using the scripting API.

Lesson 1: Implementing OAuth2 Custom Scopes

Discuss how PingAM (AM) supports the standard OAuth2 and OIDC protocols, including JSON Web Tokens (JWT):

- Understand OAuth2 and use its HTTP endpoints
- Examine the flow of the OAuth2 Authorization Code grant type
- Understand OIDC and use its HTTP endpoints
- Examine the flow of the OIDC Authorization Code grant type
- Understand the scope validation mechanism and customize its default behavior
- Use the Scripting API to customize the handling of OIDC claims
- Set up the OAuth2/OIDC service in AM
- Study and complete the ContactListTokenResponseTypeHandler code
- Enable OAuth2 federation in the ContactList front-end
- Turn ContactList RESTful backend into an OAuth2 resource server