Course Description

IG-430 Revision A

ForgeRock University

training@forgerock.com

ForgeRock® Identity Gateway Deep Dive

Description

The aim of this course is to showcase the key features and capabilities of the versatile and powerful edge security solution with the ForgeRock® Identity Gateway (IG) environment. It provides the student with the knowledge and confidence to manage their own environment. It is accepted that this course is not able to demonstrate all the features and capabilities of IG. Further information and guidance can be found in the documentation and knowledge base documents in the online repositories at: Backstage https://backstage.forgerock.com.

Note: Revision A of this course is based on version 7.2 of IG.

Target Audiences

The target audiences for this course include:

- ForgeRock Identity Gateway Administrators
- Technical users who work with Identity Gateway

Objectives

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

- Integrate and protect web applications, APIs, legacy applications, and microservices with ForgeRock® Identity Platform (Identity Platform) by using IG
- Add authentication to the ForgeRock Entertainment Company (FEC) solution, using ForgeRock® Identity Cloud (Identity Cloud) or ForgeRock® Access Management (AM) as the access manager, OpenID Connect (OIDC) provider, and Security Assertion Markup Language (SAML2) identity provider

- Demonstrate how to use IG to manage access to a website using Identity Cloud (or AM) policies and policies with advice
- Protect a REST API with IG and extend IG functionality with scripting
- Highlight various areas that must be taken into account when preparing IG for a production environment. Topics discussed include auditing, monitoring, tuning, security, and deployment

Prerequisites

The following are the prerequisites for successfully completing this course:

- Completion of the ForgeRock® Identity Gateway Essentials course available at:

  https://www.forgerock.com/support/university/forgerock-university/forgerock-identity-gateway-essentials

Duration

5 days

Course Contents

Chapter 1: Integrating Applications With IG

Integrate and protect web applications, APIs, legacy applications, and microservices with Identity Platform by using IG.

Lesson 1: Introducing IG

Introduce IG and discuss scenarios for protecting web applications, APIs, and legacy applications:

- Introduce IG
- Describe IG features
- Compare IG with policy agents
- Explore IG integration with web applications
- Describe IG integration with OIDC and SAML
- Explore IG policy enforcement and second-factor authentication (2FA)
- Describe IG protection of APIs
- Access your CloudShare VM
- Examine the lab environment
- Access the FEC and DVD4U websites

Lesson 2: Fronting a Website With IG

Configure IG to listen for secure connections, operate in development mode, and be a reverse proxy in front of the FEC website:

- Examine the IG configuration structure
- Describe required IG configuration
- Configure IG for secure connections
- Configure IG routes
- Creating and managing routes in IG Studio
- Protect a website by using IG Studio
- Upgrade a route to use WebSockets
- Configure IG for development mode and TLS connections
- Protect the FEC website with IG by using IG Studio
- Manage routes in IG Studio and examine IG log files

Lesson 3: Routing Requests and Responses

Configure IG to route requests depending on external conditions, and use various filters and handlers to process requests and responses within a route:

- Describe the IG object model
- Examine objects available in routes
- Retrieve context data and configure sessions
- Route requests depending on conditions
- Describe route handlers
- Manage requests and responses with a route handler
- Process requests and responses with filters
- Create a route to allow access to a public area of FEC
- Add a page not found route
- Create a route to access the legacy DVD4U application
- Add password replay for the DVD4U application

Lesson 4: Configuring IG Logging and Capturing Route Communication

Introduce decorators, capture information in the IG logs information using the `CaptureDecorator`, and retrieve credentials from a file with a `FileAttributesFilter`:

- Manage IG logs
- Introduce Decorators
- Configure route activity logs
- Capture inbound and outbound communication

- Retrieve credentials from a file
- Observe requests and responses in IG logs
- Test different capture configuration settings
- Centralize IG logging configuration
- Modify the DVD4U route to get credentials from a file
- Use Logback configuration for troubleshooting

Chapter 2: Configuring Agentless Single Sign-On

Add authentication to the FEC solution, using Identity Cloud or AM as the access manager, OIDC provider, and SAML2 identity provider.

Lesson 1: Implementing Authentication with the SSO Filter

Implement authentication for websites with the single sign-on (SSO) filter by using IG to interact with Identity Cloud or AM as the authentication server, to ensure access to non-public content requires authentication:

- Create a route by using the IG Studio Freeform Designer
- Configure Identity Cloud or AM as a service
- Describe how to use the SSO Filter
- Retrieve user data from the authentication provider
- Configure IG as an HTTPS client
- Create a route with the IG Studio Freeform Designer
- Redirect requests to AM for authentication
- Configure IG for client-side HTTPS
- Access properties in SSO token context
- Retrieve user profile data for display in a web page
- Store information in an IG HTTP session
- Configure capture decorators in Freeform Designer

Lesson 2: Configuring CDSSO for the Legacy Application

Configure cross-domain single sign-on (CDSSO) to support applications located in different domains, by using the `CrossDomainSingleSignOnFilter`:

- Describe the CDSSO Filter
- Configure the CDSSO Filter Solution
- Configure CDSSO redirect endpoints
- Integrate the legacy application with CDSSO
- Create a new route to protect DVD4U with CDSSO and AM
- Update the DVD4U route to automatically log in the authenticated user
- Prepare the Identity Cloud tenant

- Protect the DVD4U and FEC websites using CDSSO with Identity Cloud

Lesson 3: Performing SSO With IG as an OIDC Relying Party

Configure IG to operate as an OIDC client (relying party) to offer potential subscriber users access to the trial sections and immediate access to promotional content of the website by using their Gmail account:

- Describe basic OIDC concepts
- Configure IG as an OIDC client
- Examine the flow of OIDC redirects for authentication and consent
- Explore the flow of OIDC callbacks and data injection
- Configure an OIDC relying party route
- Examine the OIDC relying party solution

Lesson 4: Providing SSO with IG as a SAML2 SP

Configure IG to act as a SAML2 service provider (SP), enabling an application to be SAML2-compliant:

- Authenticate with a SAML2 IdP
- Describe the use of the SAML federation handler
- Describe the use of the dispatch handler
- Describe the SAML2 implementation flow
- Set up SAML2 configuration files for IG
- Configure a SAML2 route for the trial section
- Examine the SAML2 solution (optional)

Chapter 3: Controlling Access with IG as Policy Enforcement Point

Demonstrate how to use IG to manage access to a website using Identity Cloud (or AM) policies and policies with advice.

Lesson 1: Implementing Authorization With a Policy Enforcement Filter

Configure IG to manage access to a website by evaluating policies configured in Identity Cloud (or AM) and using a `PolicyEnforcementFilter`:

- Describe the use of the Policy Enforcement Filter
- Illustrate the use of the Policy Enforcement Filter
- Configure a policy enforcement point (PEP) route for the premium section of FEC
- Examine the PEP solution (optional)

Lesson 2: Providing Step-Up Authentication and Transactional Authorization

Illustrate how IG handles step-up authentication and transactional authorization policy advices with Identity Cloud (or AM):

- Describe step-up authentication
- Illustrate how IG handles step-up authentication
- Describe transactional authorization
- Illustrate how IG handles transactional authorization
- Configure a PEP route for the on demand and profile sections of FEC
- Examine the profile solution (optional)
- Examine the on-demand solution (optional)

Chapter 4: Protecting a REST API

Protect a REST API with IG and extend IG functionality with scripting.

Lesson 1: Configuring IG as an OAuth2 Resource Server

Configure IG to act as an OAuth2 resource server that protects a REST API:

- Describe the use of the OAuth2 resource server filter
- List access token resolvers
- Validate certificate-bound access tokens
- Observe the flow with the token introspection resolver
- Prepare the OAuth2 solution to protect the FEC REST API
- Configure IG to protect the FEC REST APIs
- Examine the REST API solution (optional)

Lesson 2: Extending Functionality With Scripts

Log information on context, implement dynamic scopes to manage access to resources, and refine allowed access using script-based objects in IG:

- Describe the scripting functionality for extending IG
- Explore scriptable objects
- Examine dynamic scopes solution
- Describe OAuth2 token swapping in IG
- Configure a scriptable filter to log the content of the OAuth2 context
- Configure a dynamic scopes script
- Configure a scriptable filter to retrieve the correct favorite list

Chapter 5: Preparing for Production with IG

Highlight various areas that must be taken into account when preparing IG for a production environment. Topics discussed include auditing, monitoring, tuning, security, and deployment.

Lesson 1: Auditing, Monitoring, and Tuning an IG Solution

Prepare IG for a production environment by considering auditing, monitoring, tuning, security, and deployment topics:

- Describe the audit framework
- Excluding sensitive data from audit logs
- Accessing the Common REST API monitoring endpoint
- Decreasing the number of requests through caching

Lesson 2: Developing an Awareness of Security Questions With IG

Develop awareness of best practices, describe `JwtSessions`, examine common secrets, and manage request rates and throttling:

- Discuss IG best practices regarding security
- Examine the common secrets
- Explore secret store types
- Describe throttling
- Create common secret stores
- Configure throttling

Lesson 3: Deploying IG

Explore how to deploy IG into a production context by using property value substitution and clustering:

- Describe property value substitution
- Set up multiple IG instances
- Integrate configuration tokens in the solution
- Deploy a second IG instance