

AAA, OAuth, and OIDC in IBM DataPower V7.5

WE753 (Classroom)

ZE753 (Self-paced)

Course description

This course teaches you the developer skills that are required to configure and implement authentication and authorization support within your IBM DataPower Gateway V7.5 services.

A common requirement for DataPower services is to authenticate the sender of a message, and authorize that sender to request the message’s behavior. The AAA action within DataPower provides the basics of the “authenticate, authorize, and audit” support.

OAuth is an authorization framework that defines a way for a client application to access server resources on behalf of another party. It provides a way for the user to authorize a third party to their server resources without sharing their credentials. DataPower supports OAuth specifications and protocols, and can provide an OAuth web token service.

OpenID Connect (OIDC) is an authentication layer that runs on top of an OAuth 2.0 authorization framework. DataPower can operate as an OIDC client.

In this course, you learn how to use the configuration options and processing actions to add the AAA support to a service, implement an OAuth 2.0 scenario, and add OIDC support.

Hands-on exercises give you experience working directly with an IBM DataPower gateway. The exercises focus on skills such as configuring a AAA action, configuring a web token service, and creating an OIDC client.

For information about other related courses, see the IBM Training website:

http://www.ibm.com/training

General information

Delivery method

Classroom or self-paced virtual classroom (SPVC)

Course level

ERC 1.0

Product and version

IBM DataPower Gateway Version 7.5.1

Audience

This course is designed for integration developers who configure service policies on IBM DataPower Gateways.

Learning objectives

After completing this course, you should be able to:

* Describe the AAA framework within the IBM DataPower Gateway
* Explain the purpose of each step in an access control policy
* Configure a AAA action to enforce authentication and authorization policies that are in a AAA information file and in an LDAP server
* Describe the OAuth 2.0 framework
* Explain the role that a DataPower gateway performs in an OAuth 2.0 framework
* Configure the DataPower objects that are used for OAuth 2.0 interactions
* Define Social Login
* Describe how to configure Social Login in DataPower
* Configure an OIDC client

Prerequisites

Before taking this course, you should successfully complete course *Essentials of Service Development for IBM DataPower Gateway V7.5* (WE751G) or *Essentials of Service Development for IBM DataPower Gateway V7.5* (ZE751G). You should also be familiar with AAA, OAuth 2.0, and OIDC concepts.

Duration

1 day

Skill level

Intermediate

|  |  |
| --- | --- |
| Classroom (ILT) setup requirements | |
| Processor | Intel Pentium 2.26 GHz or faster |
| GB RAM | 8 |
| GB free disk space | 80 |
| Network requirements | LAN / Internet / Fixed IP |
| Other requirements | The communication link between the student workstations and the DataPower gateway should be approximately 1.5 megabits/sec (“T1” line).The network administrator needs to open the following ports for bidirectional communication between the lab workstations and the DataPower gateway:   * dp\_WebGUI\_port: Port number that is configured on the DataPower gateway from the web GUI interface; usually port 9090 * dp\_xml\_mgmt\_port: Port number that is configured on the DataPower gateway for the XML management interface; usually port 5550 * 12010 - 12309: Ports that students use to access their services on the DataPower gateway; the port range assumes 30 students (xx01x - xx30x) * 389: Port that students and the DataPower gateway use to access the LDAP server that runs on the student image * 9080: Port that students and the DataPower gateway use to access the FLY airlines Booking Service web service that runs on the DataPower gateway * 2068: Port that students and the DataPower gateway use to access the FLY airlines Baggage Service web service that runs on the DataPower gateway * 22: DataPower SSH CLI (Command Line Interface) |

Notes

The following unit and exercise durations are estimates, and might not reflect every class experience. If the course is customized or abbreviated, the duration of unchanged units will probably increase.

This course is new, but it includes modules from the following previous course:

* *Accelerate, Secure and Integrate with IBM DataPower v7.1* (WE711G)

Course agenda

|  |
| --- |
| Course introduction  Duration: 15 minutes |

|  |  |
| --- | --- |
| Unit 1. Authentication, authorization, and auditing (AAA)  Duration: 1 hour | |
| Overview | This unit describes the authentication, authorization, and auditing (AAA) framework within the IBM DataPower Gateway. These three facets of security both monitor and restrict access to resources. |
| Learning objectives | After completing this unit, you should be able to:   * Describe the AAA framework within the DataPower Gateway * Explain the purpose of each step in an access control policy * Authenticate and authorize requests with:   + WS-Security Username and binary security tokens   + HTTP Authorization header claims   + Security Assertion Markup Language (SAML) assertions |

|  |  |
| --- | --- |
| Exercise 1. Configuring authentication and authorization in a service  Duration: 45 minutes | |
| Overview | This exercise covers the AAA capabilities of the IBM DataPower Gateway. To enforce client authentication and authorization, access to services is restricted to permitted clients for authorized operations. |
| Learning objectives | After completing this exercise, you should be able to:   * Configure a AAA action to enforce authentication and authorization policies that are in a AAA information file * Configure a AAA action to enforce authentication and authorization policies that are in an LDAP server |

|  |  |
| --- | --- |
| Unit 2. OAuth overview and DataPower implementation  Duration: 45 minutes | |
| Overview | This unit introduces the OAuth 2.0 framework and its DataPower implementation. |
| Learning objectives | After completing this unit, you should be able to:   * Describe the OAuth framework * Describe why OAuth is useful in security scenarios * Describe the OAuth three-legged scenario * Explain the role that a DataPower gateway performs in an OAuth framework * Describe the OAuth configuration options on DataPower: the web token service, the AAA action, the OAuth client profile, and the OAuth client group |

|  |  |
| --- | --- |
| Exercise 2. Defining a three-legged OAuth scenario that uses DataPower services  Duration: 1 hour and 30 minutes | |
| Overview | In this exercise, you define the DataPower objects that are needed to implement a three-legged OAuth scenario: an OAuth client profile, an OAuth client group, a web token service, and a resource server. During the service creation, you create a AAA policy that specifies OAuth. Finally, you test the implementation by invoking a client that runs in a web server. |
| Learning objectives | After completing this exercise, you should be able to:   * Define an OAuth Client Profile and an OAuth Client Group object * Create a AAA policy to support the OAuth protocol * Configure a DataPower web token service * Configure a DataPower implementation of an OAuth resource server |

|  |  |
| --- | --- |
| Unit 3. Social Login support in DataPower  Duration: 45 minutes | |
| Overview | This unit covers how DataPower supports Social Login. |
| Learning objectives | After completing this unit, you should be able to:   * Define Social Login * Describe how to configure Social Login in DataPower * Configure a Social Login Policy object * Configure a JWT Generator and a JWT Validator object * Describe OpenID Connect * Configure an OpenID Connect client in DataPower |

|  |  |
| --- | --- |
| Exercise 3. Implementing an OIDC client  Duration: 1 hour | |
| Overview | In this exercise, you configure and test an OIDC client. |
| Learning objectives | After completing this exercise, you should be able to:   * Configure an OIDC client |

|  |  |
| --- | --- |
| Unit 4. Course summary  Duration: 15 minutes | |
| Overview | This unit summarizes the course and provides information for future study. |
| Learning objectives | After completing this unit, you should be able to:   * Explain how the course met its learning objectives * Access the IBM Training website * Identify other IBM Training courses that are related to this topic * Locate appropriate resources for further study |

For more information

To learn more about this course and other related offerings, and to schedule training, see ibm.com/training

To learn more about validating your technical skills with IBM certification, see ibm.com/certify

To stay informed about IBM training, see the following sites:

IBM Training News: ibm.com/blogs/ibm-training

YouTube: youtube.com/IBMTraining

Facebook: facebook.com/ibmtraining

Twitter: twitter.com/IBMCloudEdu