

Supporting REST and JOSE in IBM DataPower Gateway V7.5

WE752 (Classroom)

ZE752 (Self-paced)

Course description

This course teaches you the developer skills that are required to configure and implement services that support REST-based traffic and JOSE-based signatures and encryption on the IBM DataPower Gateways (IDG) with firmware version 7.5.1.

The DataPower Gateways allow an enterprise to simplify, accelerate, and enhance the security capabilities of its JSON, XML, web services, and REST deployments. For JSON payloads, DataPower supports digital signatures and encryption that conform to the JSON Object Signing and Encryption (JOSE) specification.

Through a combination of instructor-led lectures and hands-on lab exercises, you learn how to use the configuration options, processing actions, and GatewayScript to support REST-based message traffic. To protect JSON message payloads, you use JSON Web Signature (JWS) and JSON Web Encryption (JWE) actions in the processing policy of a service.

Hands-on exercises give you experience working directly with a DataPower gateway. The exercises focus on skills such as selecting request and response types, using the HTTP method criteria in a matching rule, style sheet and GatewayScript transforms, GatewayScript CLI debugging, signing JSON payloads, and encrypting JSON payloads.

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:

* Add support to DataPower services to support REST applications
* Describe how to integrate with systems by using RESTful services
* Use the DataPower gateway to proxy a RESTful service
* Describe the support for JOSE in IBM DataPower Gateway V7.5
* Describe the JWS and JWE formats for compact and JSON serialization
* Configure JWS Signature and Signature Identifier objects
* Configure a JSON Web Sign action and a JSON Web Verify action to support compact and JSON serialization
* Configure a JSON Web Encrypt action and a JSON Web Decrypt action to support compact and JSON serialization
* Use the jose GatewayScript module to sign, verify, encrypt, and decrypt JSON content

Prerequisites

Before taking this course, you should successfully complete *Essentials of Service Development for IBM DataPower Gateway V7.5* (WE751G). You should also be familiar with basic JavaScript programming and REST and JSON basics.

Duration

1 day

Skill level

Intermediate

|  |  |
| --- | --- |
| Classroom (ILT) setup requirements | |
| Processor | Intel Pentium 2.5 GHz or faster |
| GB RAM | 8 |
| GB free disk space | 50 |
| 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 courses:

* VW712, *JOSE and JOSE Support in IBM DataPower V7.2* (https://www.youtube.com/watch?v=g2O5eat6A60)
* WE712, *JWS and JWE Support in IBM DataPower V7.2*
* WE711, *Accelerate, Secure and Integrate with IBM DataPower V7.1*

Course agenda

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

|  |  |
| --- | --- |
| Unit 1. REST and JSON support for Web 2.0 and mobile applications  Duration: 45 minutes | |
| Overview | DataPower services support mobile and desktop clients that communicate by using a REST pattern and JSON structures. If necessary, the gateway can be configured to convert the REST/JSON request into a SOAP request that an existing web service application requires. This unit covers the capabilities that are built into DataPower that support REST and JSON interactions. |
| Learning objectives | After completing this unit, you should be able to:   * Add support to DataPower services to support REST applications * Describe how to integrate with systems by using RESTful services * Use the DataPower gateway to proxy a RESTful service |

|  |  |
| --- | --- |
| Exercise 1. Using DataPower to implement REST services  Duration: 1 hour and 30 minutes | |
| Overview | This exercise shows you how to use the DataPower gateway to expose web services with JSON data and a REST interface. You learn how to validate JSON input against a JSON schema. The request and response data is transformed between JSON and SOAP by using GatewayScript code, style sheets, and XQuery/JSONiq code. A GatewayScript parses the typical REST URI input parameters and converts them to a SOAP request format. The system log, probe, and CLI debugger are used to observe and debug the configuration. |
| Learning objectives | After completing this exercise, you should be able to:   * Create a service policy to handle JSON and REST requests and responses * Use a GatewayScript to build a SOAP request from HTTP query parameters or JSON * Enable and use the CLI debugger * Define and use style sheet parameters * Convert a SOAP response to a JSON-formatted data structure by using XQuery/JSONiq |

|  |  |
| --- | --- |
| Unit 2. JOSE and JOSE support in IBM DataPower  Duration: 30 minutes | |
| Overview | JOSE is a critical element in providing message integrity and confidentiality in REST and JSON scenarios. This unit examines the rationale for JOSE, reviews the JOSE components, and describes the support within DataPower for JOSE. |
| Learning objectives | After completing this unit, you should be able to:   * Describe why JOSE is needed * List the components of JOSE support that DataPower uses * Describe the JWA, JWK, JWS, and JWE components and their important parameters * Explain JSON serialization and compact serialization * Describe the JWS and JWE formats * List the support within DataPower for JOSE behaviors |

|  |  |
| --- | --- |
| Unit 3. Using the WebGUI to create and verify a JWS  Duration: 30 minutes | |
| Overview | This unit explains the JSON Web Sign and JSON Web Verify actions. These actions in the WebGUI can be used to sign REST and JSON messages, and to verify the signatures within these messages. The unit covers both compact and JSON serialization forms. |
| Learning objectives | After completing this unit, you should be able to:   * Configure a JSON Web Sign action for compact and JSON serialization * Configure a JSON Web Verify action for compact serialization * Configure a JSON Web Verify action that checks a multi-signature JWS * Configure JWS Signature and Signature Identifier objects * Describe the processing flow for verification of a multi-signature JWS |

|  |  |
| --- | --- |
| Exercise 2. Creating and verifying a JWS  Duration: 1 hour | |
| Overview | A JWS is used to sign a payload that is either a JSON object or the URI request parameters in a REST request. This exercise covers the configuration of the JSON Web Sign action to generate a compact serialized JWS and a JSON serialized JWS. As part of this exercise, you also configure the JSON Web Verify action to verify the signature within the JWS. |
| Learning objectives | After completing this exercise, you should be able to:   * Configure a JSON Web Sign action to generate a compact serialized and a JSON serialized JWS * Configure a JSON Web Verify action to verify a compact serialized and a JSON serialized JWS |

|  |  |
| --- | --- |
| Unit 4. Using the WebGUI to create and decrypt a JWE  Duration: 30 minutes | |
| Overview | This unit explains how to encrypt and decrypt message payloads by using the JSON Web Encrypt and JSON Web Decrypt actions. These actions are available in the policy editor of the WebGUI. |
| Learning objectives | After completing this unit, you should be able to:   * Describe the JWE format for compact and JSON serialization * Configure a JSON Web Encrypt action for compact and JSON serialization * Configure a JSON Web Decrypt action for compact serialization * Configure a JSON Web Decrypt action that checks a multi-recipient JWE * Configure JWE Header, JWE Recipient, and Recipient Identifier objects * Describe the processing flow for verification of a multi-recipient JWE |

|  |  |
| --- | --- |
| Exercise 3. Creating and decrypting a JWE  Duration: 1 hour | |
| Overview | A JWE is used to encrypt a payload that is either a JSON object or the URI request parameters in a REST request. This exercise covers the configuration of the JSON Web Encrypt action to generate a compact serialized JWE and a JSON serialized JWE. As part of the exercise, a JSON Web Decrypt is used to decrypt the encrypted payload that is passed in the JWE. The last section of the exercise encrypts a JWS into a JWE, decrypts the JWS that is in the JWE, and verifies the JWS. |
| Learning objectives | After completing this exercise, you should be able to:   * Configure a JSON Web Encrypt action to generate a compact serialized and a JSON serialized JWE * Configure a JSON Web Verify action to verify a compact serialized and a JSON serialized JWS * Encrypt a JWS into the JWE, decrypt the JWE to get the JWS, and verify the JWS |

|  |  |
| --- | --- |
| Unit 5. Using GatewayScript to manipulate a JWS and a JWE  Duration: 30 minutes | |
| Overview | This unit covers the objects and methods that can be used to manipulate a JWS and a JWE. It describes the various GatewayScript classes and methods in the supplied jose module that can be used to create and verify a JWS, and to create and decrypt a JWE. |
| Learning objectives | After completing this unit, you should be able to:   * Describe the components of the jose module * Use the jose module to sign JSON content * Use the jose module to verify JSON signatures * Use the jose module to encrypt JSON content * Use the jose module to decrypt JSON content |

|  |  |
| --- | --- |
| Exercise 4. Using GatewayScript to work with a JWS and a JWE  Duration: 1 hour | |
| Overview | Instead of using the processing actions, you can work with a JWS and a JWE by using the JOSE objects and methods that are available in GatewayScript. In this exercise, you write GatewayScript to create and verify signatures in a JWS, and encrypt and decrypt a JWE. |
| Learning objectives | After completing this exercise, you should be able to:   * Use the JWSHeader, JWSSigner, and JWSVerifier classes to manipulate a JWS * Use the JWEHeader, JWEEncrypter, and JWEDecrypter classes to manipulate a JWE |

|  |  |
| --- | --- |
| Unit 6. 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/training/blog

YouTube: youtube.com/IBMTraining

Facebook: facebook.com/ibmtraining

Twitter: twitter.com/IBMCloudEdu