z/OS V2.5 IBM Education Assistant

Solution Name: z/OSMF JWT support

Solution Element(s): z/OSMF Core

Agenda

- Trademarks
- Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Upgrade & Coexistence Considerations
- Installation & Configuration
- Summary
- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.
- Additional Trademarks:
  - None.

Objectives

z/OSMF supports the use of JWT tokens, as follows:

- The z/OSMF server returns a JWT token after the user authenticates with the z/OSMF server
- The z/OSMF-provided JWT token can be decrypted by a remote web application with or without requiring a connection to the z/OSMF server.
- The z/OSMF-provided JWT token can be used to access z/OSMF REST services, similar to the use of LTPA tokens.

Overview

- Who (Audience)
  - System administrator
- What (Solution)
  - The z/OSMF server returns a JWT token after the user authenticates with the z/OSMF server
- Wow (Benefit / Value, Need Addressed)
  - The z/OSMF-provided JWT token can be decrypted by a remote web application with or without requiring a connection to the z/OSMF server.
  - The z/OSMF-provided JWT token can be used to access z/OSMF REST services, similar to the use of LTPA tokens. .

Usage & Invocation (1)

How to enable JWT function on z/OSMF server To enable the JWT function on z/OSMF server, do the following:

1. Copy the file server_override.xml from <product_dir>/defaults/servers/zosmfServer/ to < user_dir >/configuration

   Where:

   - <product_dir> is the z/OSMF product directory. By default, this is /usr/lpp/zosmf
   - < user_dir > is the z/OSMF data directory. By default, this is /global/zosmf

2. Set the permissions to 755 for the file server_override.xml in < user_dir >/configuration. For example: chmod 755 < user_dir >/configuration/server_override.xml

3. Restart the z/OSMF server.

As a result, the JWT support is enabled with default values. Usually, the default values are sufficient for most installations.

Usage & Invocation (2)

How to configure the JWT settings for the z/OSMF server :

JWT Single Sign On:

In the server_override.xml file, locate the following statement. Here, you specify the settings for configuring JWT Single Sign On.

<jwtSso cookieName="jwtToken" jwtBuilderRef="zOSMFBuilder" includeLtpaCookie="true" useLtpaIfJwtAbsent="true" />

Parameter	Type	Default value	Description
cookieName	string	jwtToken	Name of the cookie that is used to store the JWT token.
jwtBuilderRef	A reference to top level jwtBuilder element (string).	zOSMFBuilder	A reference to the JWT Builder configuration element in server.xml that describes how to build the JWT token.
includeLtpaCookie	boolean	true	After successful authentication with a JWT token, include an LTPA cookie in addition to the JWT cookie. z/OSMF requires it to be TRUE.
useLtpaIfJwtAbsent	boolean	true	If the JWT cookie is missing, attempt to process an LTPA cookie if it is present. z/OSMF requires it to be TRUE.

Usage & Invocation (3)

How to configure the JWT settings for the z/OSMF server :

JWT builder:

In the server_override.xml file, locate the following statement. Here, you can specify the elements and attributes that are used to build the JWT token.

<jwtBuilder id="zOSMFBuilder" issuer="zOSMF" keyAlias="DefaultzOSMFCert.IZUDFLT" expiresInSeconds="${izu.ltpa.expiration}"/>

Parameter	Type	Default value	Description
id	string	zOSMFBuilder	This ID is used to identify the JWT builder.
issuer	string	zOSMF	The issuer information.
keyAlias	string	DefaultzOSMFCert.IZUDFLT	A key alias name that is used to locate the private key for signing the token with an asymmetric algorithm. This value should be the certificate label value.
expiresInSeconds	A period of time with second precision	${izu.ltpa.expiration}	Indicates the token expiration time in seconds. z/OSMF requires JWT token expiration time be equal to LTPA token expiration time, so use one variable to set it. This value can be set by the statement SESSION_EXPIRE in parmlib.

Usage & Invocation (4)

How to configure the JWT settings for the z/OSMF server :

MicroProfile:

JWT token In the server_override.xml file, locate the following statement, which is used to configure the MicroProfile JWT token:

<mpJwt id="myMpJwt" issuer="zOSMF" jwksUri="https://${izu.jwks.hostname}:${izu.https.port}/jwt/ibm/api/zOSMFBuilder/jwk" />

Parameter	Type	Default value	Description
id	string	myMpJwt	The unique ID.
issuer	string	zOSMF	The issuer information. It should be the same value with the issuer value in Builder.
jwksUri	string	https://${izu.jwks.hostname}:${izu.https.port}/jwt/ibm/api/zOSMFBuilder/jwk	Specifies a JSON Web Key service URL.

Interactions & Dependencies

- Software Dependencies
  - Liberty 19.0.0.1 and above
- Hardware Dependencies
  - N/A
- Exploiters
  - Zowe

Upgrade & Coexistence Considerations

- To exploit this solution, all systems in the Sysplex must be at the new z/OS level:

  No
- List any toleration/coexistence APARs/PTFs.

  N/A
- List anything that doesn't work the same anymore.

  N/A
- Upgrade involves only those actions required to make the new system behave as the old one did.

  N/A
- Coexistence applies to lower level systems which coexist (share resources) with latest z/OS systems.

  N/A

Installation & Configuration

- List anything that a client needs to be aware of during installation and include **examples** where appropriate - clients appreciate these:
  - Are any APARs or PTFs needed for enablement? PH12143
  - What jobs need to be run? N/A
  - What hardware configuration is required? N/A
  - What PARMLIB statements or members are needed? N/A
  - Are any other system programmer procedures required? N/A
  - Are there any planning considerations? N/A
  - Are any special web deliverables needed? N/A
  - Does installation change any system defaults? N/A

Summary

- The following z/OS V2R5 z/OSMF JWT support item has been explained:
  - z/OSMF JWT support

Appendix

- To reference more detailed information about z/OSMF JWT support, please refer to z/OSMF Configuration Guide