Infrastructure Series

TechDoc

WebSphere Message Broker / IBM Integration Bus

WS-Security & WS-RM (Reliable Messaging) Using Policy Sets for SOAP Nodes (Administration)

Author(s): Glen Brumbaugh

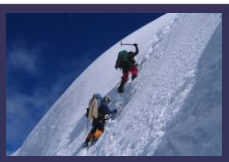

Table of Contents

Introduction

Document Version

This document describes how to configure and use Policy Sets with Message Broker SOAP nodes. The Message Flow nodes that use Policy Sets are:

- SOAPInput 
- SOAPReply 
- SOAPRequest 
- SOAPAsyncRequest 
- SOAPAsyncResponse 

Policy Sets contain WS-Security (Web Security XML specification) and WS-RM (Web Reliable Messaging XML specification) specifications. This document should apply to any version of the Message Broker product that supports these Message Flow nodes. The contents of this document have been specifically verified on the following production versions:

- WebSphere Message Broker v7.0.0.2
- IBM Integration Bus v9.0.0.0

This documentation has been created and maintained by:

- Glen Brumbaugh

This documentation has been reviewed by:

- Glen Brumbaugh

This documentation was last updated:

- Version 1.0 March 2015

Product Naming History

The product currently known as IBM Integration Bus has been through a number of different product names during its several decade long evolution. The product was originally developed by the New Era of Networks (NEON) Corporation and was marketed and resold by IBM. IBM completely redesigned and rebuilt the product and released their own in-house developed product beginning with version 2.0. The product has had the following names and version numbers:

- MQSeries Integrator (MQSI) Version 1.0 – 2.0
- WebSphere MQSeries Integrator Version 2.1
- WebSphere Business Integration Message Broker (WBIMB) V5.0
- WebSphere Message Broker (WMB) Version 6.0 - 8.x
- IBM Integration Bus (IIB) Version 9.0 - 10.0

For the remainder of this document, the product will be referred to as "*Message Broker*". This is both for historical reasons and to signify that this documentation applies to both the WMB and IIB product versions.

Product Component Terminology

With the Version 9.0 product rename (to IBM Integration Bus), several key product architectural components were given new names; while continuing to fill virtually the same role they had previously filled. This documentation will continue to refer to the "old" names because the information documented here refers to both the old and new product versions.

The old and corresponding new names are as follows:

- Message Broker → Now called "Integration Node" (Beginning with v9.0)
- Execution Group → Now called "Integration Server" (Beginning with v9.0)
- Message Flow → Still called "Message Flow"

Message Broker Policy Sets

Overview

Policy Sets are containers for two different Web Service policy types. These Web Service policy types are:

- WS-Security (Security)
- WS-RM (Reliable Messaging)

A Web Service Policy is specified in an XML container. There are separate XML containers for each of the WS-Security and WS-RM specifications. A Policy Set "Binding" is associated with a Policy Set and contains information that is specific to the platform or environment in which the Policy Set will be used. Policy Sets and Bindings are administered from the IBM Integration Explorer (MQExplorer with Message Broker plug-in). Policy Sets and their associated Bindings must be saved and restored together.

Policy Sets can be associated with a Message Flow, a Message Flow node, or both. This association is done in the Broker Archive editor. To support Message Flow association, settings for both *Providers* and *Consumers* are available. These settings map to Message Flow nodes as follows:

- SOAPInput Provider
- SOAPReply Provider

- SOAPRequest Consumer
- SOAPAsyncRequest Consumer
- SOAPAsyncResponse Consumer

In Web Services terminology, Requests and Responses form a Message Exchange Pattern (MEP). A client sends a SOAP Request message to a Web Service provider. The provider, in turn, sends a SOAP Response message to the client. Web Services terminology also defines the "roles" in these interactions. The "Initiator" is the role that sends the initial request message in a MEP. The "Recipient" is the role that processes the initial message in a MEP. The following table summarizes this terminology as it relates to Message Flow Nodes:

Table 1 - SOAP Nodes and their Roles

	Message Broker Point of View (PoV)			
Node	**Request**	**Response**	**Initiator**	**Recipient**
SOAP Input	Inbound Msg		External Client	SOAP Input Node
SOAP Reply		Outbound Msg	External Client	SOAP Reply Node
SOAP Request	Outbound Msg	Inbound Msg	SOAP Request Node	External Client
SOAP Async Request	Outbound Msg		SOAP Async Rqst	External Client
SOAP Async Response		Inbound Msg	SOAP Async Rspnce	External Client

Default Objects

When a Message Broker is created, a default Policy Set and its Binding is created. The names of these default objects are as follows:

- WSS10Default (Policy Set for WS-Security; Request messages contain Username token)
- WSRMDefault (Policy Set for WS-RM; no associated Binding)
- WSS10Default (Binding; refers to WSS10Default Policy Set, not to WSRMDefault!)

Handling Policy Sets and Bindings

Policy Sets and their Bindings are each handled as a separate Configurable Service. These Configurable Services are as follows:

- PolicySets
- PolicySetBindings

Defining Configurable Services

A Policy Set Configurable Service is defined using the following command:

- mqsicreateconfigurableservice *Broker* -c PolicySets -o *NewPolicySet*

A Policy Set Binding Configurable Service is defined using the following command:

- mqsicreateconfigurableservice *Broker* -c PolicySetBIndings -o *NewPolicySetBinding*

Importing Policy Sets and Bindings

Once the necessary Configurable Service objects have been defined, Policy Sets and their Bindings may be imported into the named Configurable Services. This is accomplished by using the *mqsichangeproperties* command. Note that a Policy Set may contain multiple policies (e.g. WS-Security and WS-RM). The *mqsichangeproperties* command can only handle one policy at a time. Thus it may take multiple executions of this command to completely import a Policy Set.

The following commands can be used to import Policy Sets and their Bindings.

- mqsichangeproperties *Broker* -c PolicySets -o *ExistingPolicySet* -n WS-Security -p *PolicySetSecurityFile*.xml
- mqsichangeproperties *Broker* -c PolicySets -o *ExistingPolicySet* -n WS-RM -p *PolicySetRMFile*.xml
- mqsichangeproperties *Broker* -c PolicySetBIndings -o *ExistingPolicySetBinding* -n WS-Security -p *PolicySetBIndingsSecurityFile*.xml
- mqsichangeproperties *Broker* -c PolicySetBIndings -o *ExistingPolicySetBinding* -n WS-RM -p *PolicySetBIndingsRMFile*.xml

Once the Policy Set and its Bindings have been imported, the Binding must be re-linked with its associated Policy Set. This is done using the following command:

- mqsichangeproperties *BrokerName* -c PolicySetBindings -o *ExistingPolicySetBinding* -n associatedPolicySet -v *ExistingPolicySet*

Note that the Execution Group must be stopped and restarted before these changes can take effect.

Display the linkage between Policy Sets and Bindings

The Policy Set associated with a specific Binding can be displayed using the following command:

- mqsireportproperties *Broker* -c PolicySetBindings -o *ExistingPolicySetBinding* -n associatedPolicySet

Note that this is a property of the Binding and not the Policy Set! The Binding for a Policy Set cannot be determined by querying the Policy Set; it must be determined by querying the Binding.

Exporting Policy Sets and Bindings

Policy Sets and Bindings can be exported from the Message Broker. This is accomplished by using the *mqsireportproperties* command. Note that a Policy Set may contain multiple policies (e.g. WS-Security and WS-RM). The *mqsireportproperties* command can only handle one policy at a time. Thus it may take multiple executions of this command to completely export a Policy Set. The following commands can be used to import Policy Sets and their Bindings.

- mqsireportproperties *Broker* -c PolicySets -o *ExistingPolicySet* -n WS-Security -p *PolicySetSecurityFile*.xml
- mqsireportproperties *Broker* -c PolicySets -o *ExistingPolicySet* -n WS-RM -p *PolicySetRMFile*.xml
- mqsireportproperties *Broker* -c PolicySetBindings -o *ExistingPolicySetBinding* -n WS-Security -p *PolicySetBindingSecurityFile*.xml
- mqsireportproperties *Broker* -c PolicySetBindings -o *ExistingPolicySetBinding* -n WS-RM -p *PolicySetBindingRMFile*.xml

Relating Policy Sets and Bindings to Message Flows and Nodes

Policy Sets and Bindings can be related either to an individual Message Flow or to a specific Node within a Message Flow. Policy Sets and Bindings relating to a specific node will override any settings specified at the Message Flow level. The relationship between Policy Sets / Bindings and Message Flows / Nodes is made within the Broker Archive (BAR) file editor. This editor is available within both the Message Broker Toolkit and the Integration Explorer (MQExplorer).

The relationship between the Web Policy types and Message Flows and their nodes are described as Broker Archive (BAR) properties. The properties that may be specified are as follows:

Message Flow Properties

- Provider Policy Set
- Provider Policy Set Bindings
- Consumer Policy Set
- Consumer Policy Set Bindings

Message Flow Node Properties

- Policy Set
- Policy Set Bindings

Configuring WS-Security properties

WS-Security policy types and their associated Bindings are configured through multiple Policy Set and Binding editors in the Integration Explorer (MQExplorer). The Policy Set editors describe:

- The authentication mechanism used (e.g. Username, X.509 certificate, etc.)
- Authentication mechanism specifics (e.g. Cipher suite used for X.509 certificates)
- How security will be used (e.g. encryption and/or authentication)
- Message integrity (e.g. hashing)

The Bindings editors describe the specific details of the mechanisms defined in the Policy Set.

Authentication and Tokens – Policy Set

Authentication mechanisms to be used in the Message Flow are described in the Policy Set (WS-Security specification). There are multiple authentication mechanisms that can be specified. These include:

- Username
- Kerberos Ticket
- X.509 Certificate
- SAML (Security Assertion Markup Language)
- LTPA (Lightweight Third-Party Authentication)

The Policy Set only defines the types of mechanisms that will be used. Zero or more instances of each of these authentications types may be defined. Each instance defined is called a “token” and assigned a “Token Name”. The mapping of a “Token Name” to a specific instance (e.g. User Name or X.509 certificate) is performed in the Binding file.

Authentication and Tokens – Binding

Specifics about the security defined in the Policy Set are defined in the Binding. Specific details include:

- Specific User Names
- Specific X.509 specific certificates (specified by label/alias or Distinguished Name)
- Truststore processing (specific Truststore or “Any”)

Configuring WS-RM properties

Messaging delivery behavior is described in the Policy Set (WS-RM specification). The behavior that can be specified includes:

- Message delivery sequence (FIFO or other)
- Message expiration
- Message parts to be encrypted

Best Practices

- **XML File Names:** There can potentially be a number of different Policy Set and Binding files. All of these files will have an ".xml" file extension. Since Policy Set and Binding files need to be related to one another, a naming approach that relates one or more Binding files to its associated Policy Set file is required. It is recommended that these two groups of files begin with the same character string so that they sort together. After this common beginning, the Binding files should be further named so that their relationship to a Message Flow or Node can easily be determined.

References

- IBM – Knowledge Center – IIB – v9.0 – Setting up Message Flow Security
  http://www-01.ibm.com/support/knowledgecenter/api/content/SSMKHH_9.0.0/com.ibm.etools.mft.doc/ap04170_.htm

- IBM – Knowledge Center – IIB – v9.0 – Policy Sets
  http://www-01.ibm.com/support/knowledgecenter/api/content/SSMKHH_9.0.0/com.ibm.etools.mft.doc/ac60110_.htm

- IBM – Knowledge Center – IIB – v9.0 – Exporting Policy Sets
  http://www-01.ibm.com/support/knowledgecenter/api/content/SSMKHH_9.0.0/com.ibm.etools.mft.doc/ac60360_.htm

- IBM – Knowledge Center – IIB – v9.0 – Importing Policy Sets
  http://www-01.ibm.com/support/knowledgecenter/api/content/SSMKHH_9.0.0/com.ibm.etools.mft.doc/ac60370_.htm

- IBM – Knowledge Center – IIB – v9.0 – Associate Policy Sets & Bindings with Message Flows
  http://www-01.ibm.com/support/knowledgecenter/api/content/SSMKHH_9.0.0/com.ibm.etools.mft.doc/ac60120_.htm

- IBM – Knowledge Center – IIB – v9.0 – Policy Sets & Bindings Editor
  http://www-01.ibm.com/support/knowledgecenter/api/content/SSMKHH_9.0.0/com.ibm.etools.mft.doc/ab60180_.htm

- IBM – Knowledge Center – IIB – v9.0 – WS-Security
  http://www-01.ibm.com/support/knowledgecenter/api/content/SSMKHH_9.0.0/com.ibm.etools.mft.doc/ac55630_.htm