Implementing web services security using user name tokens with policy sets in IBM Integration Bus

Suraj Kumar May 27, 2015

This tutorial describes how to configure policy sets, policy set bindings, and security profile services while using IBM® Integration Bus as a web service consumer to invoke web services secured by Web Services Security (WS-Security) user name tokens.

Introduction

An IBM Integration Bus (hereafter called Integration Bus) application can participate in a web services environment as a service requester, a service provider, or both. Web Services Security is a set of enhancements to SOAP messaging that provides user authorization and authentication, message integrity, and message confidentiality. This tutorial shows you how to implement WS-Security authentication in message flows using Integration Bus SOAP nodes and policy sets. You will learn how to configure policy sets, policy set bindings, and SecurityProfile services while using Integration Bus as a web service consumer to invoke web service secured by WS-Security user name tokens. Version 9 of Integration Bus provides an Eclipse-based graphical user interface, Integration Bus Explorer, that is used to define policies and policy sets.

Create a policy set

Policy sets and bindings are the artifacts that Integration Bus uses to define and configure WS-Security requirements for web services based nodes such as SOAPInput, SOAPReply, SOAPRequest, SOAPAsyncRequest, and SOAPAsyncResponse. A policy set is a container where you define the WS-Security policy types. You use a policy set and policy set bindings editor in Integration Bus Explorer to configure the following aspects of WS-Security:

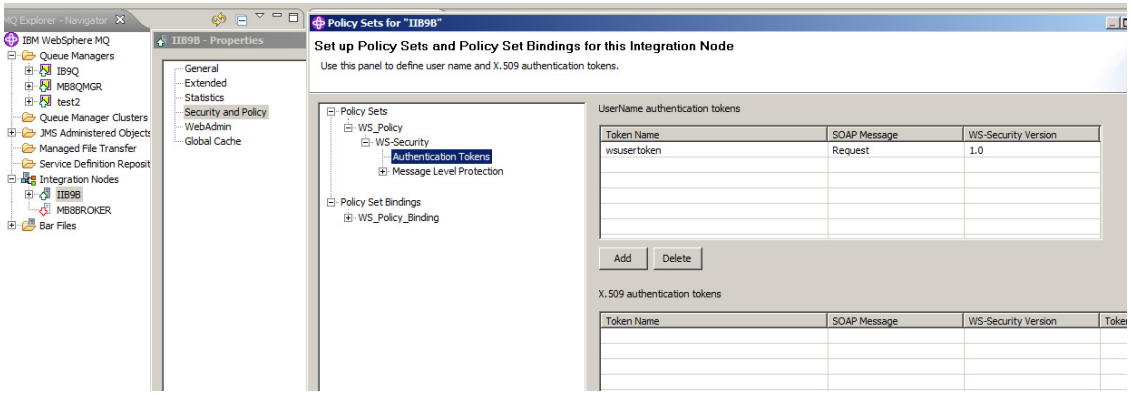
- Authentication
- Confidentiality
- Integrity
- Expiration

A policy set binding contains information specific to security features employed in an installation and has to be associated with a policy set. In this tutorial, policy sets and bindings are created for authentication using user name tokens.

To create a policy set, do the following:

1. Open **Integration Bus Explorer**, right-click the **Integration Node** and select **Properties**.
2. On the **Properties** dialog, select **Security > Policy Sets**.
3. Select **Policy Sets > Add** to add a new policy set on the "Set up Policy Sets and Policy Set Bindings for this Integration Node" dialog. Rename it as `WS_Policy`.
4. Select the newly created policy set and click on **Add WS-Security**.
5. Expand **WS-Security** and highlight **Authentication Tokens** on the left. In the "UserName authentication tokens" section, add a new token name on the right.
6. Rename the token name as `wsusertoken`. Choose SOAP Message as **Request** and WS-Security Version as **1.0** as shown in Figure 1.
7. Click **Finish** to save the policy set, WS_Policy.

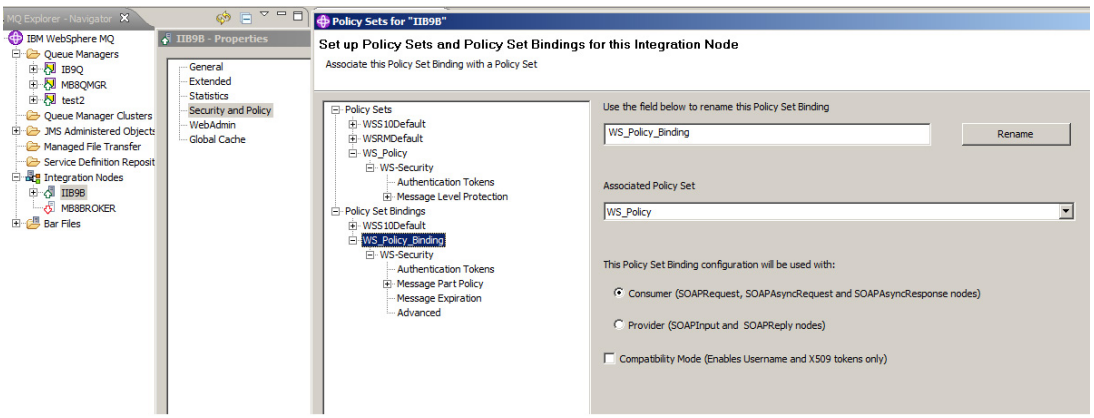
Figure 1. Create a policy set



To create a policy set bindings for a web service consumer, do the following:

1. Right-click the **Integration node**, select **Properties > Security and Policy** and then click **Policy Sets**.
2. Select **Policy Set Bindings** on the left and click **Add** to create a new entry. Rename it to `WS_Policy_Binding` as shown in Figure 2.
3. Select the policy created above, **WS_Policy**, to be associated.
4. Select **Consumer** so that the bindings can be used with web service consumer nodes.
5. Click **Finish** to save the bindings.

Figure 2. Policy set bindings



Create the security profile

The security operations to be executed in an Integration Bus message flow are defined in a security profile. Details regarding the security token propagation, authentication, authorization on the messages flowing through the message flow are specified in the security profile. You can either use the "mqsicreateconfigurableservice" command or Integration Bus Explorer to create the security profile. As the security profile is validated during BAR deployment, you need to create a security profile that defines the security operations that you want to perform before enabling security on a node. Run the following commands shown in Listing 1 to create a security profile. Here, "IIB9B" is used as the integration node.

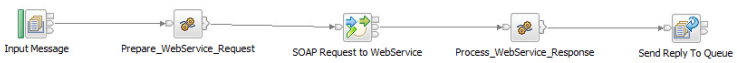
Listing 1. Command to create a security profile

```
mqsisetdbparms IIB9B -n WSSecurityID -u spssuser1 -p spssPa12word
mqsicreateconfigurableservice IIB9B -c SecurityProfiles -o WSSecurityProfile -n "propagation,
idToPropagateToTransport,transportPropagationConfig" -v "TRUE,STATIC ID,WSSecurityID"
```

Create a message flow with SOAP nodes

This tutorial uses "SPSS Job" as the target web service. You will create a sample MQInput based message flow as a web service consumer to invoke the SPSS Service for scoring. The SPSS web service is protected by WS-Security authentication. You will then configure WS-Security for authentication on this message flow using the security profile, policy set, and policy set binding that was created earlier. Define a BAR file to include the above created message flow to deploy on an Integration Bus runtime as shown in Figure 3.

Figure 3. SOAP consumer message flow



The ESQL compute node has been kept simple with fixed values provided to the SPSS service to find the anomaly with the input set of data. Notice that no WS-Security headers are added while drafting the SOAP request message (see Listing 2).

Listing 2. ESQL to prepare the SOAP request message

```
CREATE COMPUTE MODULE Invoke_SPSS_Service_Compute
 CREATE FUNCTION Main() RETURNS BOOLEAN
 BEGIN

    DECLARE soapenv NAMESPACE 'http://schemas.xmlsoap.org/soap/envelope/';

  -- Body Elements
  SET OutputRoot.SOAP.Body.ns200:getScore.ns57:scoreRequest.(XMLNSC.Attribute) id='TM_Anomaly';
  SET OutputRoot.SOAP.Body.ns200:getScore.ns57:scoreRequest.ns57:requestInputTable.(XMLNSC.Attribute)
 name='Table 1';
  SET OutputRoot.SOAP.Body.ns200:getScore.ns57:scoreRequest.ns57:requestInputTable.ns57:requestInputRow.
(XMLNSC.Attribute)reserved='?';
  DECLARE rowRef REFERENCE TO
 OutputRoot.SOAP.Body.ns200:getScore.ns57:scoreRequest.ns57:requestInputTable.ns57:requestInputRow;

  DECLARE iter,countOfProps INTEGER;
  Set iter=1;
```

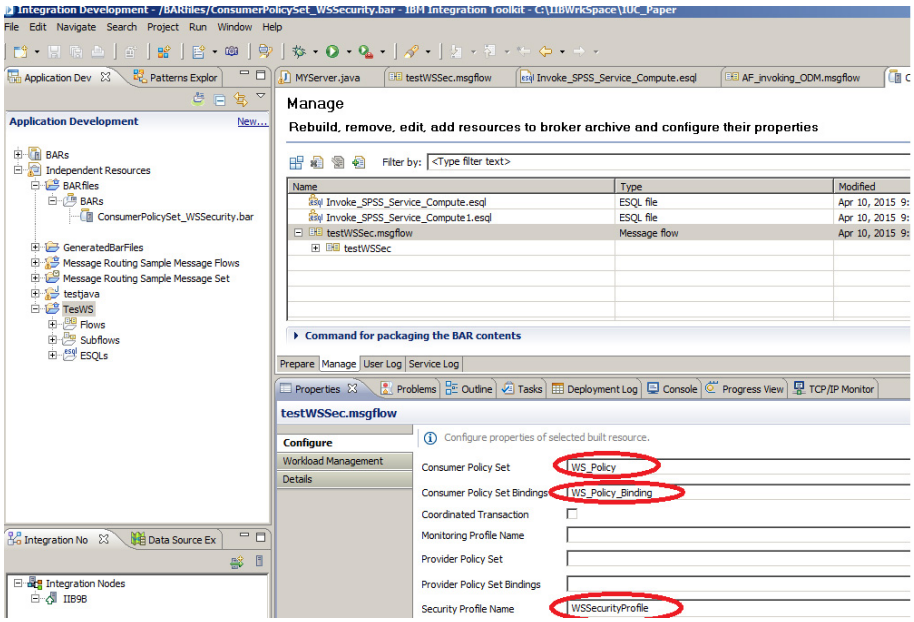
```
  SET countOfProps = CARDINALITY(InputRoot.XMLNSC.request.params[]);
  WHILE (iter <= countOfProps) DO
   SET rowRef.ns57:input[iter].(XMLNSC.Attribute)name=InputRoot.XMLNSC.request.params[iter].name;
   SET rowRef.ns57:input[iter].(XMLNSC.Attribute)value=InputRoot.XMLNSC.request.params[iter];
   SET iter=iter+1;
  END WHILE;

  DECLARE spssBaseURL CHARACTER;
  SET spssBaseURL=InputLocalEnvironment.Variables.spss.URL;
  SET OutputLocalEnvironment.Destination.SOAP.Request.Transport.HTTP.WebServiceURL='http://localhost:5541/
scoring/services/Scoring.HttpV2';

  RETURN TRUE;
 END;

END MODULE;
```

Associate the policy with a message flow

The policy and security profile is set on the message flow used to make the outbound web service call. This is done by overriding the message flow properties in the BAR file editor. These can also be set at the SOAPRequest node, which overrides the properties set at the message flow level. The following properties are updated (Figure 4):

- Update the policy set to **WS_Policy**.
- Update the policy set bindings to **WS_Policy_Binding**.
- Update the security profile to **WSSecurityProfile**.

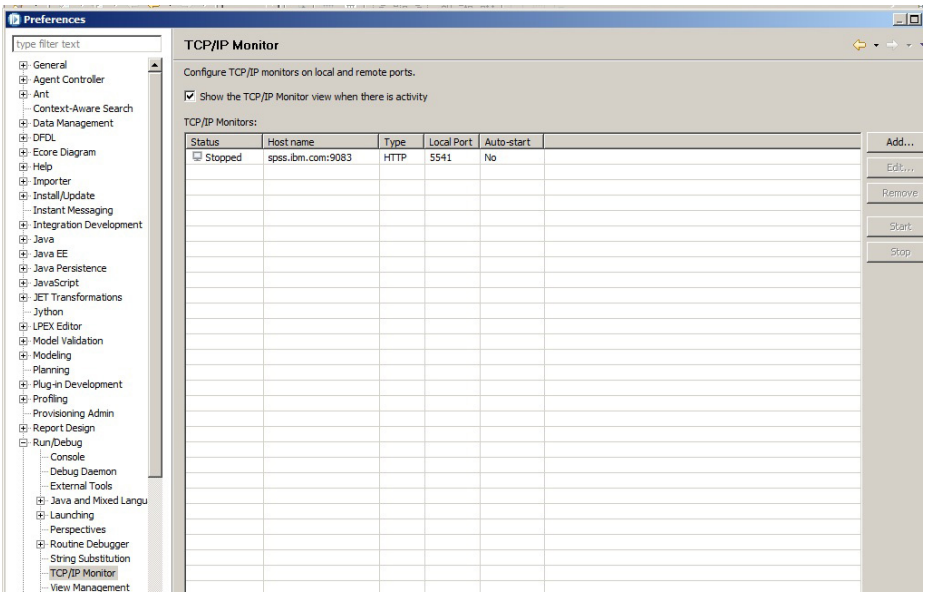
Figure 4. Associate policy sets with SOAP consumer message flow



Run tests to evaluate authentication

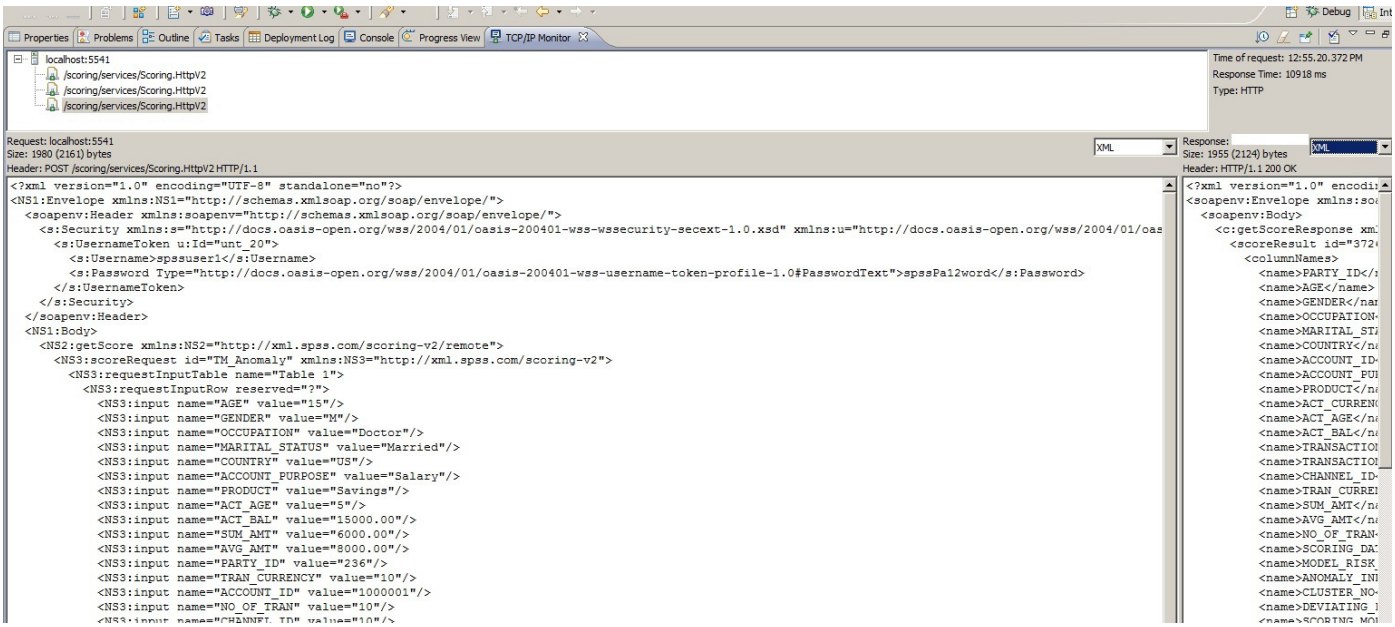
To monitor the outgoing web service request, you can use any network monitoring tool. Here, we are using the TCP/IP Monitor tool provided in the Integration Development toolkit. Create a monitor in the TCP/IP monitor tool and provide an available local port for monitoring. Update the server and port details on the SOAPRequest node's HTTP URL, rebuild the BAR, and deploy it.

Figure 5. TCP/IP Monitor tool settings



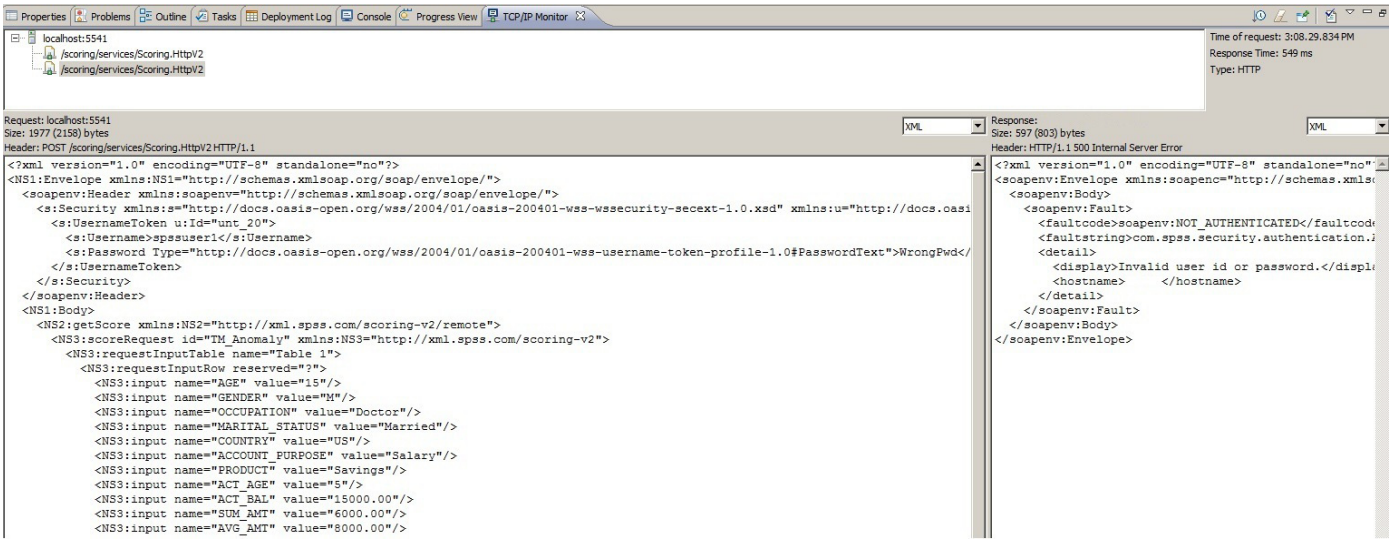
To trigger the message flow, use MQ Explorer to write an XML message to the input queue. The TCP/IP Monitor tool shows the generated web service request with the user name token headers (Figure 6).

Figure 6. Successful run with authentication details in WS-Security headers



If the SecurityProfile has incorrect authentication details, it leads to authentication failure as shown in Figure 7.

Figure 7. Authentication error



You have now verified through the TCP/IP monitor tool that the policy set and security profile set on the message flow have added the required WS-Security authentication headers to the outgoing SOAP request.

Conclusion

This tutorial showed you how to implement WS-Security user name token authentication on a web service consumer message flow using policy sets, policy set bindings, and a security profile. It also explained how to use the TCP/IP monitor tool to verify the WS-Security headers created in a SOAP request.

Related topics

- IBM Integration Bus Knowledge Center
- IBM Integration Bus product family page
- Video: What's new in IBM Integration Bus
- Download IBM Integration Bus Developer Edition
- Follow IBM Integration Bus on Twitter
- IBM Integration Bus forum
- Track IBM Integration Bus user requirements