Integrating WebSphere Service Registry and Repository with IBM Tivoli Security Policy Manager

Overview

This IBM® Redpapers™ publication describes the built-in integration between IBM WebSphere Service Registry and Repository (WSRR) and IBM Tivoli Security Policy Manager (TSPM), which allows users to author policies in TSPM and attach them to services stored in WSRR.

Product description

IBM Tivoli® Security Policy Manager V7.0 is a standards-based application security solution. It provides centralized application entitlement management, service-oriented architecture (SOA) security policy management, and security as runtime services to strengthen access control for new applications and services, to help improve compliance and to drive operational governance across the enterprise.
Tivoli Security Policy Manager enables application owners and administrators to externalize security and to simplify the management of complex authorization policies for new and existing applications, including customized applications. The benefits include:

- The ability to respond quickly to business changes through centralized application roles, entitlements, and data-level access control
- Improved compliance and security management with roles-, rules-, and attributes-based access control

Tivoli Security Policy Manager also enables enterprise architects and security operations teams to centrally manage and enforce security policies for Web services resources across multiple policy enforcement points, including the WebSphere® DataPower® SOA appliances. The benefits include:

- Reduced manual, inconsistent, and costly administration of security policies at each policy enforcement point
- Operational governance with the ability to delegate and audit all changes to policies

**Value proposition**

Integrating WebSphere Service Registry and Repository with IBM Tivoli Security Policy Manager offers the following benefits:

- It enables organizations to view their services and the policies applicable to those services in one location.
- Any users effected by changes to policies can be notified of these changes by way of the WSRR e-mail notification service.
- It enables, at design time, users to see what services will be affected by changing a policy.

**Key integration features**

When WebSphere Service Registry and Repository integrates with IBM Tivoli Security Policy Manager, a user can discover Web services stored in WSRR and import their Web Service Description Language (WSDL) files into IBM Tivoli Security Policy Manager. Once imported into IBM Tivoli Security Policy Manager, these polices can be authored and attached to these WSDLs. After policy authoring is complete and attached to particular WSDLs, the WSDLs and attached policies can be distributed back to WSRR.
Integration scenarios overview

We describe two scenarios here: The first is where WebSphere DataPower will be used as the policy enforcement point (PEP), and the second is where WebSphere Application Server will be used as the PEP.

Integration scenario 1 overview

JKHL Enterprises, a fictional company, currently has an Account Creation service running in their production environment, and they wish to enhance the security of this service by enforcing a WS-SecurityPolicy with a RequireClientCertificate assertion. The RequireClientCertificate assertion, once enforced, requires all HTTPS clients of the Account Creation service to produce a client certificate before the service can be invoked.

JKHL Enterprises use WSRR as their service repository, and they also use TSPM as the application in which they create all of the WS-SecurityPolicy documents that they require. All consuming applications of the account creation service call a WebSphere DataPower WS-proxy, which is created using the WSRR synchronization feature in WebSphere DataPower.

Integration issues

In this scenario, WSRR is accessed in order to retrieve the AccountCreation service on the WSDL port and to import it into TSPM so that a policy can be authored and attached to it.

Uploading service definitions is explained in Service Lifecycle Governance Using WebSphere Service Registry and RepositoryService Lifecycle Governance with IBM WebSphere Service Registry and Repository V6.3, SG24-7793 and will not be described in this paper.

Creating the WSRR subscription to the AccountCreationV1_0 WSDL service in WebSphere DataPower will not be described in this paper. Creating WSRR subscriptions in WebSphere DataPower is explained in Chapter 4, “Using Web Service Proxy with WebSphere Registry and Repository”, of IBM WebSphere DataPower SOA Appliances Part IV: Management and Governance, REDP-4366

Finally, writing clients that satisfy the new security policy constraints will not be described in this paper
Solution overview

The solution is shown in Figure 1.

This solution is split into several tasks:
1. Import the AccountCreation service WSDL port into TSPM.
2. Create the WS-SecurityPolicy, which asserts RequireClientCertificate.
3. Attach the policy to the AccountCreation service.
4. Publish the attached policy back to WSRR, where WebSphere DataPower will retrieve it during the next synchronization.

Integration scenario 2 overview

JKHL Enterprises currently has an Account Creation service running in their production environment, and they wish to enhance the security of this service by enforcing a WS-SecurityPolicy with a RequireClientCertificate assertion. The RequireClientCertificate assertion, once enforced, requires that all HTTPS clients of the Account Creation service produce a client certificate before the service can be invoked.

JKHL Enterprises uses WSRR as their service repository, and they also have TSPM as the application in which they create all of the WS-SecurityPolicy documents that they require. IBM Tivoli Runtime Security Services client, a component of TSPM, is deployed into JKHL Enterprise’s production environment.
and acts as a Policy Enforcement Point (PEP) to enforce all policies distributed to it.

Integration issues

In this scenario, WSRR will be accessed to retrieve the AccountCreation service on the WSDL port and to import it into TSPM so that a policy can be authored and attached to it.

Uploading the service definitions is explained in *Service Lifecycle Governance Using WebSphere Service Registry and Repository* Service Lifecycle Governance with IBM WebSphere Service Registry and Repository V6.3, SG24-7793 and will not be described in this paper.

Finally, writing clients that satisfy the new security policy constraints will not be described in this paper.

Solution overview

The solution is shown in Figure 2.

![Figure 2 Scenario 2 overview](image)

This solution is split into several tasks:
1. Import the AccountCreation service on the WSDL port into TSPM.
2. Create the WS-SecurityPolicy, which asserts RequireClientCertificate.
3. Attach the policy to the AccountCreation service.
4. Publish the attached policy back to WSRR and distribute the policy to the PEP installed on the WebSphere Application Server instance where AccountCreation service is deployed.

**Performing the solutions**

Both solutions contain several common steps, which will only differ when publishing the new policy to the policy enforcement point or WSRR.

**Common steps**

Whether you are implementing scenario 1 or scenario 2, the first step is to create a reference to the WSRR instance in IBM Tivoli Security Policy Manager. Perform these steps:

1. Configure a secure communication between TSPM and WSRR.

   Before adding a WSRR instance as a Service Registry in IBM Tivoli Security Policy Manager, you must create a secure communication channel for data exchange between IBM Tivoli Security Policy Manager and WSRR.

   a. Import the signer certificate for the WSRR system into the trust store, as shown in Figure 3 on page 7.

      i. Log in to the WebSphere Application Server administration console of the instance that hosts IBM Tivoli Security Policy Manager and select Security → SSL certificate and key management.

      ii. Click Key stores and certificates.

      iii. Click NodeDefaultTrustStore.

      iv. Click Signer certificates.

      v. Click Retrieve from port.

      vi. Compete the Host, Port (the secure administration port of the WebSphere Application Server instance hosting the WSRR) and Alias fields.

      vii. Click Retrieve signer information.
Figure 3  Retrieving the signer certificate for WSRR

viii. Click **OK** and save the configuration.
b. Export the LPTA key to a file and transfer it to the WSRR system, as shown in Figure 4.

i. In the WebSphere Application Server administration console of the instance that hosts IBM Tivoli Security Policy Manager, select **Security → Secure administration, applications and infrastructure**.

ii. Click **Authentication mechanisms and expiration**.

iii. Navigate to the Cross-cell sign-on area of the Configuration tab. Enter the password for the key file that contains the LPTA key and a full qualified path name for the key file.

iv. Click **Export keys**.

v. Click **OK**.

---

**Figure 4  Export LPTA to a file**
vi. Move the file to the file system of the WSRR system.

c. Log in to the WebSphere Application Server administration console of the
instance that hosts WSRR.

d. Import the signer certificate for the IBM Tivoli Security Policy Manager into
the trust store, as shown in Figure 5.

i. Select **Security → SSL certificate and key management**.

ii. Click **Key stores and certificates**.

iii. Click **NodeDefaultTrustStore**.

iv. Click **Signer certificates**.

v. Click **Retrieve from port**.

vi. Complete the Host, Port (the secure administration port of the
WebSphere Application Server instance hosting the IBM Tivoli Security
Policy Manager) and Alias fields.

vii. Click **Retrieve signer information**.

![SSL certificate and key management](image)

**Figure 5   Retrieving the signer certificate for IBM Tivoli Security Policy Manager**

viii. Click **OK** and save the configuration.
e. Import the LPTA key from the IBM Tivoli Security Policy Manager, as shown in Figure 6.

**Note:** These instructions are for WSRR hosted on a WebSphere Application Server V7.0 instance.

i. Select **Security → Global Security**.

ii. Click **LPTA**.

iii. Navigate to the Cross-cell single sign-on area. Enter the password for the key file that contains the LPTA key and the fully qualified path name for the key file.

iv. Click **Import Keys**.

v. Click **OK** and save the configuration.

f. Restart the WebSphere Application Server instance hosting WSRR.

g. Restart the WebSphere Application Server instance hosting IBM Tivoli Security Policy Manager.
2. Add a WSRR instance as a Service Registry in IBM Tivoli Security Policy Manager. This will allow IBM Tivoli Security Policy Manager to discover services in WSRR.
   a. Select Tivoli Security Policy Manager → IT Environment → Service Registries.
   b. Click Add....
   c. Select IBM WebSphere Service Registry and Repository as the registry and click Next.
   d. Complete the Name, Host, Bootstrap port (the bootstrap port of the WebSphere Application Server instance hosting the WSRR), Registry username (this user must be an administrator in WSRR) and Confirm registry password fields, as shown in Figure 7.
   e. Click Finish.
f. A success message appears, as shown in Figure 8.

![Success window](image)

Figure 8  Success window

3. Add a WSRR instance as a policy distribution point.
   This allows IBM Tivoli Security Policy Manager to distribute policies authored and attached to services back to WSRR.
   a. Select **Tivoli Security Policy Manager → IT Environment → Policy Distribution Points**.
   b. Click **Add...**.
   c. Click **Next**.
d. In Policy Distribution Type, select **IBM WebSphere Registry and Repository** and type a name in Policy Distribution Target name field, as shown in Figure 9. Click **Next**.

![Figure 9 Setting the Policy Distribution Target Type](image)

Figure 9 Setting the Policy Distribution Target Type

e. Complete the Host, Port (the bootstrap port of the WebSphere Application Server instance hosting the WSRR), Registry username (has to be an administrator in WSRR) and password fields and click **Next**.

f. Click **Finish**.
g. A success message appears, as shown in Figure 10.

![Image of Figure 10: Adding WSRR as a Policy Distribution Target is successful]

Figure 10  Adding WSRR as a Policy Distribution Target is successful

4. Import the service into IBM Tivoli Security Policy Manager from WSRR.
   a. Select **Tivoli Security Policy Manager** → **Services and Policies** → **Services**.
   b. Click **Add**.
   c. Click **Next**.
   d. From the drop-down menu, select **Web Service** and click **Next**.
   e. Select **Import from a registry** and click **Next**.
   f. Select the name of the WSRR created previously and click **Next**.
   g. Enter * into the Name field and click **Next**.
   h. Enter a different name for the service or accept the name already entered. Click **Next**.
   i. Click **Next**.
   j. Click **Finish**. The service has now been imported into TSPM.

5. Create a policy in IBM Tivoli Security Policy Manager.
   a. Select **Tivoli Security Policy Manager** → **Services and Policies** → **Policies**.
   b. Click **Add**.
c. Select **Message Protection** and **Create a new policy**, as shown in Figure 11, and click **Next**.

![Figure 11 Selecting a policy type](image1)

**Figure 11 Selecting a policy type**

d. Enter `http_token` into the Name field for the policy, as shown in Figure 12. Click **Add**....

![Figure 12 Adding a name to the policy](image2)

**Figure 12 Adding a name to the policy**
e. Select **Supporting Tokens** as the Assertion Type, as shown in Figure 13.

![Figure 13  Selecting the Assertion Type](image)
f. A new set of options are presented. From these options, select **HTTPS Token** from the Type drop-down menu and click **Add**, as shown in Figure 14.
g. Select `requireClientCertificate` from the Mode drop-down menu, as shown in Figure 15, and select the **No Issuer** radio button. Click **Next**.

![Figure 15  Setting the mode](image)

- h. Click **Next**.
- i. Click **Next**.
- j. Click **Save**.

6. Attach the policy to the service.
   a. Select **Tivoli Security Policy Manager → Services and Policies → Policies**.
   b. Select **Security → Message Protection → http_token**.
   c. Select **Web Service/http://jkhl.itso.ibm.com/AccountCreationV1/service\AccountCreationV1_0/AccountCreationV1_0_ProductionPort** from the Services drop-down menu, as shown in Figure 16 on page 19. Click the + button.
Solution 1 specific steps

Perform the following steps to complete solution 1:

1. Prepare TSPM to publish the service with the attached policy back to WSRR.
   b. Click Web Service → http://jkhle.itso.ibm.com/AccountCreationV1/service}AccountCreationV1_0.
   c. Select Policy → Configure Policy.
   d. Click WSRR from the Available Policy Distribution Targets pane and click Add.
e. In Available Policy Decision Points pane, select **DataPower**, as shown in Figure 17.

![Figure 17 Policy configuration](image)

f. Click **Next**.

g. Click **Next**.
h. Click **Finish**.

2. Distribute the policy.

a. Select **Tivoli Security Policy Manager → Services and Policies → Services**.

b. Click **Web Service** → http://jkhle.itso.ibm.com/AccountCreationV1/service}AccountCreationV1_0.

c. Select **Policy → Distribute Policy**.

d. Click **Distribute the latest effective policy**.

e. Click **OK**.
Solution 2 specific steps

Perform the following steps to complete solution 2:

1. Prepare TSPM to publish the service with the attached policy back to WSRR and to the policy distribution target.
   b. Click Web Service → http://jkhle.itso.ibm.com/AccountCreationV1/service}AccountCreationV1_0.
   c. Select Policy → Configure Policy.
   d. Click WSRR from the Available Policy Distribution Targets drop-down menu. Click Add.
   e. Click prodendpoint (the TSPM policy enforcement point installed on the WebSphere Application server instance) from the Available Policy Distribution Targets drop-down menu. Click Add.
   f. In Available Policy Decision Points drop-down menu, select IBM Tivoli Runtime Security Services for both WSRR and prodendpoint.
   g. Click Next.
   h. Click Next.
   i. Click Finish.

2. Distribute the policy.
   b. Click Web Service → http://jkhle.itso.ibm.com/AccountCreationV1/service}AccountCreationV1_0.
   c. Select Policy → Distribute Policy.
   d. Click Distribute the latest effective policy.
   e. Click OK.

Common points for both scenarios

The policy has now been distributed to WSRR and, in the case of scenario 2, to the Policy Enforcement Point (PEP). TSPM attaches the policy to the logical object structure in WSRR.
These scenarios require the generation of a client certificate that the client then presents to the PEP upon connection, TSPM will not generate these certificates, so they have to be generated by the PEP. In the case of a PEP deployed in WebSphere Application Server, this would involve installing a Certificate Authority (CA), configuring the WebSphere Application Server to use that CA, and then generating a client certificate from the CA that can then be distributed to the client.

In the case where WebSphere DataPower is the PEP, the SSL profile in the front-end handler of the WS-proxy must be configured to require client certificates. The client certificates that are allowed will then have to be added by either adding certificates to the SSL profile or by adding a trust chain.

When the policy enforcement point is a WebSphere Application Server instance, and a policy evaluation returns a denial, the WebSphere Application Server instance will output two exceptions:


   faultCode: {http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-sec ext-1.0.xsd} FailedAuthentication
   faultString: CTGVS8046E Access denied. Please consult the authorization policy for this service.
   faultActor: com.ibm.tscc.enforce.websphere.WebSpherePEP

Caused by: javax.xml.rpc.soap.SOAPFaultException: CTGVS8046E Access denied.
Please consult the authorization policy for this service.

These exceptions are not errors, but are statements regarding denial of access; each time access is denied, two WebSphere Application Server ffdc files are also created.
Other considerations

TSPM attaches policies to services in WSRR using policy attachments conforming to the WSDL identifier specification. Take care when attaching policies in the WSRR, as the WSDL identifier may not be unique and could possible lead to the policy being attached to objects to which it was not intended to be attached.

The team who wrote this IBM Redpapers publication

This paper was produced by a team of specialists from around the world working at the International Technical Support Organization, Raleigh Center.

Andrew White is a software developer from the United Kingdom. He has 3 years of experience in middleware development at IBM. Andrew holds a degree in Computer Science from The University of Nottingham. His areas of expertise include WebSphere Application Server, WebSphere Service Registry and Repository (WSRR), WebSphere DataPower, WebSphere Process Server, Tivoli Composite Application Manager for Service Oriented Architecture (ITCAM4SOA), Tivoli Security Policy Manager (TSPM), service-oriented Architecture (SOA), and Microsoft® .NET.

Thanks to the following people for their contributions to the paper:

- Martin Keen
- Nicole Hargrove
- Ian Heritage
- Prasad Imandi
- Wendy Neave
- Laura Olson
- Bhargav Perepa
This document REDP-4561-00 was created or updated on November 3, 2009.

Send us your comments in one of the following ways:
- Use the online Contact us review Redbooks form found at:
  ibm.com/redbooks
- Send your comments in an email to:
  redbook@us.ibm.com
- Mail your comments to:
  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099, 2455 South Road
  Poughkeepsie, NY 12601-5400 U.S.A.

**Trademarks**

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

- DataPower®
- IBM®
- Redpaper™
- Redpapers™
- Redbooks (logo) ®
- Tivoli®
- WebSphere®

The following terms are trademarks of other companies:

Microsoft, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.