WebSphere® Service Registry and Repository

IBM

Version 6.2

SA14: SupportPac for policy set and JAX-WS services

WebSphere® Service Registry and Repository

SA14: SupportPac for policy set and JAX-WS services

December 2008

Contents

SA14: IBM® WebSphere Service Registry and Repository SupportPac for policy sets and JAX-WS services

WebSphere® Service Registry and Repository SupportPac™, SA14, provides support for policy sets and JAX-WS services.

You can use WSRR to discover and publish policy sets to and from WebSphere Application Server and WebSphere Message Broker; and to discover JAX-WS services available from WebSphere Application Server.

- You can discover and publish policy sets to and from the following applications:
  - WebSphere Application Server version 6.1. with Fix Pack 17 or later, with the Web Services Feature Pack 17 or later installed.
  - WebSphere Message Broker 6.1.
- You can discover JAX-WS services from WebSphere Application Server version 6.1. with Fix Pack 17 or later.

Prerequisite software

The minimum software requirement for configuring WebSphere Service Registry and Repository for SupportPac SA14 is WebSphere Service Registry and Repository version 6.2. with Fix Pack 2 or later.

WSRR SupportPac Web site

You can download the SupportPac file, sa14.zip from the WSRR SupportPac Web site. Download the file to a directory on your local system, and extract the contents of the compressed file.

License details

For terms and conditions of the license associated with SupportPac SA14, see the license files contained in the license directory of the SupportPac compressed file.

Related information

WSRR SupportPac Web site
http://www.ibm.com/support/docview.wss?rs=171&uid=swg27008751

Configuring WebSphere Service Registry and Repository for SupportPac SA14

You must configure WebSphere Service Registry and Repository to use the policy set and JAX-WS service SupportPac functions.

About this task

Perform the following tasks to configure WebSphere Service Registry and Repository to discover and publish policy sets, to and from, WebSphere Application Server and WebSphere Message Broker; and to discover JAX-WS services available from WebSphere Application Server.

1. Load the taxonomy.owl file into WebSphere Service Registry and Repository.
   - "Loading the taxonomy file" on page 2

2. Load the scheduler_config.xml file into WebSphere Service Registry and Repository.
   - "Loading the scheduler configuration file" on page 3
3. Enable the PolicySet validator in WebSphere Service Registry and Repository.
   - "Enabling the PolicySet validator" on page 3
4. Configure the discovery and publishing of policy sets for Websphere Application Server
   - "Configuring policy set discovery and publishing to and from WebSphere Application Server" on page 4
5. For WebSphere Message Broker only, add the ConfigManagerProxy.jar file as a shared library and associate it with the ServiceRegistry application in WebSphere Application Server.
   - "Adding the ConfigManagerProxy.jar file" on page 6
6. For WebSphere Message Broker only, configure the discovery and publishing of policy sets to and from WebSphere Message Broker
   - "Configuring policy set discovery and publishing to and from WebSphere Message Broker" on page 6

Loading the taxonomy file

You must configure WebSphere Service Registry and Repository to load the taxonomy file to implement the policy set and JAX-WS service SupportPac functions.

About this task

Perform the following steps to load the taxonomy file into WSRR:
- Switch to the **Configuration** Perspective.
- Expand **Active Configuration Profile**.
- Click **Classification Systems**.
- Click **Load Classifications System** in the main window.
- Click **Browse** and browse to the directory you extracted the contents of the compressed file to. Select the file taxonomy.owl and click **Open**.
- Click **OK**.

PolicySet SupportPac classifications

Loading the taxonomy.owl file into WebSphere Service Registry and Repository loads the following classifications:
- PolicySet SupportPac Classifications
- Policy
- WebSphere Message Broker 6.1
- WebSphere Application Server 6.1
- PolicySet

These classifications are used to classify the discovered policy sets and associated policy files.

Each policy set is classified as a PolicySet and is also classified with the system it was discovered from, for example WebSphere Application Server 6.1 or WebSphere

Message Broker 6.1. The associated policies are classified with the system they are discovered from.

Loading the scheduler configuration file

You must configure WebSphere Service Registry and Repository to load the scheduler configuration file to implement the policy set and JAX-WS service SupportPac functions.

About this task

Perform the following steps to load the scheduler configuration file into WSRR:
- Switch to the **Configuration** Perspective.
- Expand **Active Configuration Profile**.
- Click **Plug-ins** ▸ **Scheduler**.
- Click **Load Scheduler Configuration** in the main window.
- Click **Browse** and browse to the directory you extracted the contents of the compressed file to. Select the scheduler_config.xml file and click **Open**.
- Enter a name for the **Scheduler Configuration**, for example, *PolicySetSchedules*.
- Click **OK**.

The tasks can be run the manually or they can scheduled to run automatically. See the related tasks for further information about discovering services using the service discovery scheduler, and starting JAX-WS and policy set discovery manually.

Related tasks

"Discovering JAX-WS services and policy sets using the service discovery scheduler" on page 13
You can discover JAX-WS services and policy sets automatically at a configurable time interval, by configuring and enabling the service discovery scheduler.

"Starting JAX-WS and policy set discovery manually" on page 13
You can start service discovery at any time by running a script.

Enabling the PolicySet validator

You must configure WebSphere Service Registry and Repository to enable the PolicySet validator to implement the policy set and JAX-WS service SupportPac functions.

About this task

Perform the following steps to enable the PolicySet validator in WSRR:
- Switch to the **Configuration** Perspective.
- Click **Active Configuration Profile** ▸ **Plug-ins** ▸ **Validation Properties**.
- Click **Validation properties plug-in** (ValidationProperties) link in the main window.
- At the end of the line that starts with 'governanceValidators=' add *com.ibm.sr.policyset.validators.PolicySetValidator* using a comma to separate items in the line.
- Click **OK**.

Configuring policy set discovery and publishing to and from WebSphere Application Server

You configure policy set discovery and publishing by defining a <discovery-task> element specific to WebSphere Application Server policy sets in the main Service Discovery configuration file.

About this task

The <discovery-task> element for Policy Set discovery and publishing has the following structure:

```
<discovery-task name="WASPolicySetDiscoveryTask">
  <discoverer type="WASPolicySet" />
      <discovererClass>com.ibm.sr.policyset.was.WASPolicyDiscoverer</discovererClass>
      <parserClass>com.ibm.sr.policyset.was.WASPolicyConfigParser</parserClass>
      <validatorClass>com.ibm.sr.policyset.was.WASPolicyConfigValidator</validatorClass>
  </discoverer>
  <configuration>
    <instance>
    ... XML elements specifying configuration property values ...
    </instance>
            .
    <instance>
    ... XML elements specifying configuration property values ...
    </instance>
  </configuration>
</discovery-task>
```

The <instance> element

You specify one <instance> element for each WebSphere Application Server from which you want to discover JAX-WS services.

Table 1. The <instance> element has the name attribute

name	The name you want to assign to the WebSphere Application Server instance.

Table 2. The XML elements that you specify in the <instance> element

Element	Description
host	The host name of the WebSphere Application Server system.
port	The number of the SOAP connector port for the WebSphere Application Server.
conn-type	The mechanism used to connect to the WebSphere Application Server. The value of this element must be one of the following: • SOAP • RMI
security-enabled	Specifies whether security is enabled for the WebSphere Application Server. The value of this element must be one of the following: • true: security is enabled. • false: security is disabled.
username	The WebSphere Application Server administration user. This element is required if the value of the security-enabled element is set to true.
password	The WebSphere Application Server administration password. This element is required if the value of the security-enabled element is set to true. The password is converted to DES to hide its value.
was-version	The version of WebSphere Application Server. This element is required. It must be in the format 6.1.0.17 or 6.1.

Table 2. The XML elements that you specify in the <instance> element (continued)

Element	Description
publish-transitionURI	The WSRR lifecycle transition URI that is used to trigger the publishing of the policy set to this instance.

Note: The configuration properties point to the administrative service on the application server for a stand alone server environment and on the deployment manager for a distributed environment.

Example of a WebSphere Application Server policy set <discovery-task> element

The following example shows a <discovery-task> element that configures the discovery and publishing of policy sets from a WebSphere Application Server instance:

```
<discovery-task name="WASPolicySetDiscoveryTask">
   <discoverer type="WASPolicySet">
      <discovererClass>com.ibm.sr.policyset.was.WASPolicyDiscoverer</discovererClass>
      <parserClass>com.ibm.sr.policyset.was.WASPolicyConfigParser</parserClass>
      <validatorClass>com.ibm.sr.policyset.was.WASPolicyConfigValidator</validatorClass>
   </discoverer>
   <configuration>
      <instance name="WASFPInst1">
         <host>Server1</host>
         <port>8880</port>
         <conn-type>SOAP</conn-type>
         <security-enabled>false</security-enabled>
         <was-version>6.1.0.17</was-version>
         <publish-transitionURI>
             http://www.ibm.com/xmlns/prod/serviceregistry/6/0/governance/DefaultLifecycle#Certify
         </publish-transitionURI>
      </instance>
      <instance name="WASFPInst2">
         <host>Server2</host>
         <port>8880</port>
         <conn-type>SOAP</conn-type>
         <security-enabled>true</security-enabled>
         <username>user1</username>
         <password>(DES)PASSWORD1==</password>
         <was-version>6.1.0.17</was-version>
         <publish-transitionURI>
             http://www.ibm.com/xmlns/prod/serviceregistry/6/0/governance/DefaultLifecycle#Certify
         </publish-transitionURI>
      </instance>
   </configuration>
</discovery-task>
```

Modifying the service discovery configuration

You must add the <discovery-task> element before the closing </service-discovery> element at the end of the Service Discovery configuration file substituting the relevant values for accessing your system.

For instructions about modifying the Service Discovery configuration file, see the related links for the following sections in the WebSphere Service Registry and Repository Information Centre:
- Modifying the service discovery configuration XML file using the Web UI.
- Loading the service discovery configuration XML file.

➥ Modifying the service discovery configuration XML file using the Web UI
http://publib.boulder.ibm.com/infocenter/sr/v6r2/topic/com.ibm.sr.doc/
twsr_service_discovery_modify.html

➥ Loading the service discovery configuration XML file
http://publib.boulder.ibm.com/infocenter/sr/v6r2/topic/com.ibm.sr.doc/
twsr_service_discovery_load.html

Adding the ConfigManagerProxy.jar file

You must configure WebSphere Message Broker to add the ConfigManagerProxy.jar
file to implement the WebSphere Service Registry and Repository policy set and
JAX-WS service SupportPac functions.

About this task

The file ConfigManagerProxy.jar, is found in the Message Broker install directory
structure. For example, in a Microsoft® Windows® installation the file is located in
the C:\Program Files\IBM\MQSI\classes subdirectory.

Perform the following steps to add the ConfigManagerProxy.jar as a Shared library
and associate it with the ServiceRegistry application in WebSphere Application
Server:

1. Create a WAS Shared Library which includes the ConfigManagerproxy.jar by
   following the instructions in the WebSphere Application Server Information
   Center:
   - http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/topic/
     com.ibm.websphere.wsfep.multiplatform.doc/info/ae/ae/
     tcws_sharedlib_create.html
2. Associate the Shared Library with the Service Registry Application by
   following the instructions in the WebSphere Application Server Information
   Center:
   - http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/topic/
     com.ibm.websphere.wsfep.multiplatform.doc/info/ae/ae/
     tcws_sharedlib_app.html

Configuring policy set discovery and publishing to and from WebSphere Message Broker

You configure policy set discovery and publishing by defining a <discovery-task>
element specific to WebSphere Message Broker policy sets in the main Service
Discovery configuration file.

About this task

The <discovery-task> element for Policy Set discovery and publishing has the
following structure:

```
<discovery-task name="MBPolicySetDiscoveryTask">
  <discoverer type="MBPolicySet" />
      <discovererClass>com.ibm.sr.policyset.mb.MBPolicyDiscoverer</discovererClass>
      <parserClass>com.ibm.sr.policyset.mb.MBPolicyConfigParser</parserClass>
      <validatorClass>com.ibm.sr.policyset.mb.MBPolicyConfigValidator</validatorClass>
  </discoverer>
  <configuration>
    <instance>
    ... XML elements specifying configuration property values ...
    </instance>
```

```
          .
   <instance>
   ... XML elements specifying configuration property values ...
   </instance>
  </configuration>
</discovery-task>
```

The <instance> element

You specify one <instance> element for each WebSphere Message Broker from which you want to discover or publish policy sets.

Table 3. The <instance> element has the name attribute

name	The name you want to assign to the WebSphere Message Broker instance.

Table 4. The XML elements that you specify in the <instance> element

Element	Description
host	The host name of the WebSphere Message Broker system.
port	The number of the connector port for the WebSphere Message Broker Configuration Manager.
qmgr	The name of the Queue Manager of the WebSphere Message Broker system.
brokername	The name of the Broker on the WebSphere Message Broker system.
broker-version	The version of WebSphere Message Broker. This element is required. It must be in the format 6.1.
publish-transitionURI	The WSRR lifecycle transition URI that is used to trigger the publishing of the policy set to this instance.

Example of a WebSphere Message Broker policy set <discovery-task> element

The following example shows a <discovery-task> element that configures the discovery and publishing of policy sets from a WebSphere Message Broker instance:

```
<discovery-task name="MBPolicySetDiscoveryTask">
   <discoverer type="MBPolicySet">
      <discovererClass>com.ibm.sr.policyset.mb.MBPolicyDiscoverer</discovererClass>
      <parserClass>com.ibm.sr.policyset.mb.MBPolicyConfigParser</parserClass>
      <validatorClass>com.ibm.sr.policyset.mb.MBPolicyConfigValidator</validatorClass>
   </discoverer>
   <configuration>
      <instance name="MBInst1">
         <host>Server1</host>
         <port>2414</port>
         <qmgr>WBRK61_DEFAULT_QUEUE_MANAGER </qmgr>
         <brokername> WBRK61_DEFAULT_BROKER </brokername>
         <broker-version>6.1</broker-version>
         <publish-transitionURI>
             http://www.ibm.com/xmlns/prod/serviceregistry/6/0/governance/DefaultLifecycle#Certify
         </publish-transitionURI>
       </instance>
     </configuration>
  </discovery-task>
```

Modifying the service discovery configuration

You must add the <discovery-task> element before the closing
</service-discovery> element at the end of the Service Discovery configuration file
substituting the relevant values for accessing your system.

For instructions about modifying the Service Discovery configuration file, see the
related links for the following sections in the WebSphere Service Registry and
Repository Information Centre:
- Modifying the service discovery configuration XML file using the Web UI.
- Loading the service discovery configuration XML file.

> Modifying the service discovery configuration XML file using the Web UI
  http://publib.boulder.ibm.com/infocenter/sr/v6r2/topic/com.ibm.sr.doc/
  twsr_service_discovery_modify.html

> Loading the service discovery configuration XML file
  http://publib.boulder.ibm.com/infocenter/sr/v6r2/topic/com.ibm.sr.doc/
  twsr_service_discovery_load.html

Running policy set discovery

When the Service Discovery and Scheduler configurations have been set up, policy
sets can be discovered automatically by using the scheduled task, or manually by
running a scheduled task immediately.

About this task

See the related tasks for further information about discovering services using the
service discovery scheduler and starting JAX-WS and policy set discovery
manually.

Note: When discovering policy sets, if a policy set exists in WebSphere Service
Registry and Repository with the same name as one that is being
discovered, the existing policy set and associated policy files are not
overwritten. The policy set and associated policy files are classified only
with the type of system that they were originally discovered from, for
example, WebSphere Application Server 6.1.

Related tasks

"Discovering JAX-WS services and policy sets using the service discovery
scheduler" on page 13
You can discover JAX-WS services and policy sets automatically at a configurable
time interval, by configuring and enabling the service discovery scheduler.

"Starting JAX-WS and policy set discovery manually" on page 13
You can start service discovery at any time by running a script.

Viewing a discovered policy set and associated policy files

Policy sets and policy files can be viewed in WebSphere Service Registry and
Repository by using the policy authoring user interface.

About this task

Perform the following steps to view policy sets and policy files:
- In the navigation tree, select **Service Documents** → **Policy Documents**. All the
  polices and policy sets within WebSphere Service Registry and Repository are
  displayed.

- Click on the a policy or policy set to view the content.

Note: Discovered polices and policy sets are classified with the system they were discovered from, for example WebSphere Application Server version 6.1 or WebSphere Message Broker version 6.1. A policy set is also classified with the PolicySet classification. See the related task, Loading the taxonomy file, for further details of PolicySet SupportPac classifications.

Related tasks

"Loading the taxonomy file" on page 2
You must configure WebSphere Service Registry and Repository to load the taxonomy file to implement the policy set and JAX-WS service SupportPac functions.

Publishing a policy set

A policy set and its referenced policy files can be published to either WebSphere Application Server or WebSphere Message Broker by governing the policy set file and taking the file through a lifecycle.

About this task

The transition that will trigger the publish of the policy set is defined in the ServiceDiscovery configuration files within the <publish-transitionURI> element.

When a policy set is put in to a state in its lifecycle by the transition URI defined in the <publish-transitionURI>, the policy set is published to the instances defined in the discovery configuration that have the <publish-transitionURI>.

Example

```
<service-discovery xmlns="http://www.ibm.com/xmlns/prod/serviceregistry/6/2/servicediscovery">
<discovery-task name="WASPolicySetDiscoveryTask">
   <discoverer type="WASPolicySet">
      <discovererClass>com.ibm.sr.policyset.was.WASPolicyDiscoverer</discovererClass>
      <parserClass>com.ibm.sr.policyset.was.WASPolicyConfigParser</parserClass>
      <validatorClass>com.ibm.sr.policyset.was.WASPolicyConfigValidator</validatorClass>
   </discoverer>
   <configuration>
      <instance name="WASFPInst1">
         <host>Server1</host>
         <port>8880</port>
         <conn-type>SOAP</conn-type>
         <security-enabled>false</security-enabled>
         <was-version>6.1.0.17</was-version>
         <publish-transitionURI>
             http://www.ibm.com/xmlns/prod/serviceregistry/6/0/governance/DefaultLifecycle#Certify
         </publish-transitionURI>
      </instance>
   </configuration>
 </discovery-task>
<discovery-task name="MBPolicySetDiscoveryTask">
   <discoverer type="MBPolicySet">
      <discovererClass>com.ibm.sr.policyset.mb.MBPolicyDiscoverer</discovererClass>
      <parserClass>com.ibm.sr.policyset.mb.MBPolicyConfigParser</parserClass>
      <validatorClass>com.ibm.sr.policyset.mb.MBPolicyConfigValidator</validatorClass>
   </discoverer>
   <configuration>
      <instance name="MBInst1">
         <host>Server1</host>
         <port>2414</port>
         <qmgr>WBRK61_DEFAULT_QUEUE_MANAGER </qmgr>
```

```
        <brokername> WBRK61_DEFAULT_BROKER </brokername>
        <broker-version>6.1</broker-version>
        <publish-transitionURI>
            http://www.ibm.com/xmlns/prod/serviceregistry/6/0/governance/DefaultLifecycle#Certify
        </publish-transitionURI>
      </instance>
    </configuration>
  </discovery-task>
</service-discovery>
```

In the Service Discovery configuration above, a policy set moved to a state using the default lifecycle transition URI provided in WebSphere Service Registry and Repository, http://www.ibm.com/xmlns/prod/serviceregistry/6/0/governance/ DefaultLifecycle#Certify, is published to both the "WASFPInst1" and "MBInst1" systems.

Note: The policy set policy file must be classified with both the PolicySet classification and also the classification of the system it is to be published to, for example WebSphere Application Server 6.1 or WebSphere Message Broker 6.1. If the policy set and its associated policy files are valid for multiple systems, the policy set can be classified with all the systems it is valid for. You must ensure that the policy set and its associated policy files are valid for the systems you classify them for. If the policy set and its associated policy files are not valid for these systems, then publishing these policy sets might cause issues in the systems you are publishing to.

Configuring JAX-WS service discovery

Configure JAX-WS Service discovery by defining a <discovery-task> element specific to JAX-WS service discovery in the main Service Discovery configuration file.

About this task

The <discovery-task> element for JAX_WS Service discovery has the following structure:

```
<discovery-task name="JAXWSDiscoveryTask">
  <discoverer type="JAXWS" />
      <discovererClass>com.ibm.sr.servicediscovery.jaxws.JAXWSServiceDiscoverer</discovererClass>
      <parserClass>com.ibm.sr.servicediscovery.jaxws.JAXWSConfigurationParser</parserClass>
      <validatorClass>com.ibm.sr.servicediscovery.jaxws.JAXWSConfigurationValidator</validatorClass>
  </discoverer>
  <configuration>
    <instance>
    ... XML elements specifying configuration property values ...
    </instance>
            .
    <instance>
    ... XML elements specifying configuration property values ...
    </instance>
  </configuration>
</discovery-task>
```

The <instance> element

You specify one <instance> element for each WebSphere Application Server from which you want to discover JAX-WS services.

Table 5. The <instance> element has the name attribute

name	The name you want to assign to the WebSphere Application Server instance

Table 6. The XML elements that you specify in the <instance> element

Element	Description
host	The host name of the WebSphere Application Server system.
port	The number of the SOAP connector port for the WebSphere Application Server.
conn-type	The mechanism used to connect to the WebSphere Application Server. The value of this element must be one of the following: • SOAP • RMI
security-enabled	Specifies whether security is enabled for the WebSphere Application Server. The value of this element must be one of the following: • true: security is enabled. • false: security is disabled.
username	The WebSphere Application Server administration user. This element is required if the value of the security-enabled element is set to true.
password	The WebSphere Application Server administration password. This element is required if the value of the security-enabled element is set to true. The password is converted to DES to hide its value.

> **Note:** The configuration properties point to the administrative service on the application server for a stand alone server environment and on the deployment manager for a distributed environment.

Example of a JAX-WS <discovery-task> element

The following example shows a <discovery-task> element that configures the discovery of services from a WebSphere Application Server instance:

```
<discovery-task name="JAXWSDiscoveryTask">
   <discoverer type="JAXWS">
      <discovererClass>com.ibm.sr.servicediscovery.jaxws.JAXWSServiceDiscoverer</discovererClass>
      <parserClass>com.ibm.sr.servicediscovery.jaxws.JAXWSConfigurationParser</parserClass>
      <validatorClass>com.ibm.sr.servicediscovery.jaxws.JAXWSConfigurationValidator</validatorClass>
   </discoverer>
   <configuration>
      <instance name="WASFPInst1">
         <host>Server1</host>
         <port>8880</port>
         <conn-type>SOAP</conn-type>
         <security-enabled>false</security-enabled>
      </instance>
      <instance name="WASFPInst2">
         <host>Server2</host>
         <port>8880</port>
         <conn-type>SOAP</conn-type>
         <security-enabled>true</security-enabled>
         <username>user1</username>
```

```
     <password>(DES)PASSWORD1==</password>
   </instance>
  </configuration>
</discovery-task>
```

Modifying the service discovery configuration

You must add the <discovery-task> element before the closing
</service-discovery> element at the end of the service discovery configuration file
substituting the relevant values for accessing your system.

For instructions about modifying the Service Discovery configuration file, see the
related links for the following sections in the WebSphere Service Registry and
Repository Information Centre:
- Modifying the service discovery configuration XML file using the Web UI.
- Loading the service discovery configuration XML file.

   ⤷ Modifying the service discovery configuration XML file using the Web UI
   http://publib.boulder.ibm.com/infocenter/sr/v6r2/topic/com.ibm.sr.doc/
   twsr_service_discovery_modify.html

   ⤷ Loading the service discovery configuration XML file
   http://publib.boulder.ibm.com/infocenter/sr/v6r2/topic/com.ibm.sr.doc/
   twsr_service_discovery_load.html

Connecting to a secure WebSphere Application Server environment

You must configure SSL certificates in the client and server if the target WebSphere
Application Server environment is secured with a self-signed certificate.

About this task

Client is the application server where WebSphere Service Registry and Repository
is deployed. Server is the target application server.

To configure SSL certificates, you must perform one of the following two actions:
- Import the public certificate from the target application server into the default
  trust store of the application server where WebSphere Service Registry and
  Repository is deployed.
- Create a new SSL configuration with a keystore using the keyfile from the target
  application server, and create a dynamic outbound endpoint configuration. The
  format of the connection information of the dynamic outbound endpoint
  configuration you specify depends on the connection type, as shown in the
  following table:

Table 7. Format of the connection information of the dynamic outbound endpoint

Connection type	Format
SOAP	ADMIN_SOAP,<host>,<port> or *,<host>,<port>
RMI	IIOP,<host>,<port> or *,<host>,<port>

The values of <host> and <port> must match the values you specified in the
<host> and <port> elements.

Note: If you are using client authentication, you must also import the client
certificate from the application server on which WebSphere Service Registry
and Repository is deployed into the keyfile of the target application server.

For further details about configuring SSL certificates, see the related information.

Related information

➨ Associating a Secure Sockets Layer configuration dynamically with an outbound protocol and remote secure endpoint
http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/topic/
com.ibm.websphere.nd.multiplatform.doc/info/ae/ae/tsec_sslassocconfigout.html

Discovering JAX-WS services and policy sets using the service discovery scheduler

You can discover JAX-WS services and policy sets automatically at a configurable time interval, by configuring and enabling the service discovery scheduler.

About this task

By default, the service discovery scheduler is not enabled. You can configure and enable the service discovery scheduler by defining XML elements in a configuration file. You can either create a new configuration file, or modify the default configuration file which is preinstalled in WebSphere Service Registry and Repository.

To configure the service discovery scheduler from the default configuration file, use the Web UI to modify the XML elements in the configuration file. See the related information for further details about discovering services according to a schedule.

Related information

➨ Discovering services according to a schedule
http://publib.boulder.ibm.com/infocenter/sr/v6r2/topic/com.ibm.sr.doc/
twsr_service_discovery_scheduler.html

Starting JAX-WS and policy set discovery manually

You can start service discovery at any time by running a script.

About this task

To start service discovery manually, run the executeSchedulerTaskImmediate.jacl script by using the `wsadmin` command. You run the `wsadmin` command with different parameters depending on whether WebSphere Service Registry and Repository is deployed in a cluster configuration, or a stand alone or federated node configuration. Run the command from the <WSRR_INSTALL_ROOT>\ admin\scripts_cell directory. You must enter the command and parameters on one line.

<TASKNAME> must be either JAXWSDiscoveryTask, WASPolicSetDiscoveryTask or MBPolicySetDiscoveryTask, and must correspond to the name attribute of the <scheduler-task> element in the service discovery scheduler configuration XML file.

- In a cluster configuration, enter the command in the following format:
  - o `<WAS_INSTALL_ROOT>\bin\wsadmin  -f executeSchedulerTaskImmediate.jacl -cluster <CLUSTERNAME>  -taskname <TASKNAME>`
- **For example:**

```
c:\WebSphere\AppServer\bin\wsadmin -f executeSchedulerTaskImmediate.jacl
-cluster cluster1 -taskname WASDiscoveryTask
```

- In a stand alone or federated node configuration, enter the command in the following format:
  - o `<WAS_INSTALL_ROOT>\bin\wsadmin -f executeSchedulerTaskImmediate.jacl -cell <CELLNAME>  -node <NODENAME> -server <SERVERNAME> -taskname <TASKNAME>`

Note: If you are discovering a large number of services, you might have to increase the value of the `wsadmin` client SOAP timeout parameter, to prevent the client timing out before the service discovery task completes. See the related link about Java™ Management Extensions connector properties in the WebSphere® Application Server Information Center for details.

Note: If the WebSphere Application Server running the WebSphere Service Registry and Repository application has security enabled you must add the following parameters to the `wsadmin` command before the -cell parameter, `-username <WAS Username> - password <WAS Password>` or enter the WebSphere Application Server username and password when prompted by WebSphere Application Server.

Related information

↪ Java Management Extensions connector properties
http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/topic/
com.ibm.websphere.nd.multiplatform.doc/info/ae/ae/
ragt_rconnector_customp.html

Appendix. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Trademarks

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

IBM
SupportPac
WebSphere

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

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

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

IBM ®

Program Number: 5724-N72